HKUST SPD - INSTITUTIONAL REPOSITORY

Channel Estimation and Secret Key Rate Analysis of MIMO Terahertz Quantum Key Distribution

Neel Kanth Kundu [ID] , *Graduate Student Member, IEEE*, Soumya P. Dash [ID] , *Member, IEEE*,
Matthew R. McKay [ID] , *Fellow, IEEE*, and Ranjan K. Mallik [ID] , *Fellow, IEEE*

Abstract—We study the secret key rate (SKR) of a multiple-input multiple-output (MIMO) continuous variable quantum key distribution (CVQKD) system operating at terahertz (THz) frequencies, accounting for the effects of channel estimation. We propose a practical channel estimation scheme for the THz MIMO CVQKD system which is necessary to realize transmit-receive beamforming between Alice and Bob. We characterize the input-output relation between Alice and Bob during the key generation phase, by incorporating the effects of additional noise terms arising due to the channel estimation error and detector noise. Furthermore, we analyze the SKR of the system and study the effect of channel estimation error and overhead. Our simulation results reveal that the SKR may degrade significantly as compared to the SKR upper bound that assumes perfect channel state information, particularly at large transmission distances.

Index Terms— Channel estimation, continuous variable quantum key distribution (CVQKD), multiple-input multiple-output (MIMO), terahertz (THz) communications, quantum communications, secret key rate.

I. INTRODUCTION

With the widespread deployment of fifth-generation (5G) wireless communication systems, researchers have started to conceptualize new use cases and the required technological solutions for beyond fifth generation (B5G) or sixth generation (6G) communication systems [1]. The future B5G/6G networks aim to support a peak data rate of 1 Tbps, an air latency of 0.1 ms, and twice the spectral and energy efficiency of current 5G standards [1]–[5]. Different physical layer solutions have been proposed to meet the demands of B5G wireless applications spanning holographic telepresence,

tactile internet, internet of everything, and augmented and virtual reality [4]. These include multiple-input multiple-output (MIMO) systems [6], reconfigurable intelligent surfaces [7]–[12], novel modulation schemes [13]–[16], and harnessing of the terahertz (THz) frequency spectrum [17]–[21].

Apart from high data-rate requirements, security and privacy of the data are also considered to be of great importance in B5G/6G applications. With the rapid advancement in quantum computing, standard higher layer encryption schemes based on the Rivest-Shamir-Adleman (RSA) algorithm can be broken by Shor's factoring algorithm [22], [23]. Similarly, physical layer encryption based on classical key distribution algorithms like Diffie-Hellman [24] are also not secure, since its security is based on the assumption that the computationally hard problem of discrete logarithm cannot be solved in reasonable time by classical computers. Hence, current computationally secure encryption algorithms can be broken with the rapid development in practical quantum computing. Quantum key distribution (QKD) can be used to distribute secure keys between two parties, say Alice and Bob, which can then be used for one-time-pad (OTP) based physical layer encryption for 6G applications [25]–[28]. Alternatively, the key generated from a QKD protocol can also be used by the higher layers for symmetric key encryption. QKD offers unconditional security guaranteed by the laws of quantum physics.

Broadly speaking, there are two main classes of QKD which have been proposed in the literature. The first is discrete variable QKD (DVQKD) that encodes the key information in the polarization or the phase of single photon light pulses, whose security is guaranteed by the no-cloning theorem of quantum physics [29]–[36]. The second one is continuous variable QKD (CVQKD) that encodes the key information in the quadratures of Gaussian coherent states, and its security is based on the Heisenberg's uncertainty principle [37]–[42]. The implementation of DVQKD is difficult in practice since it requires single photon sources and detectors. On the other hand, it is relatively easy to implement CVQKD since it requires standard off-the-shelf telecommunication equipment. Thus, it is easier to integrate CVQKD into future wireless communication networks.

Most current wireless QKD systems are point-to-point links (e.g., satellite-to-earth links, satellite-to-satellite links, inter-building links, and free-space maritime links) implemented by using optical frequencies [43]–[55]. This requires high precision tracking of the receiver and does not support mobility required for terrestrial B5G/6G applications. Therefore, THz QKD systems have recently been proposed for mobile devices

N. K. Kundu is with the Department of Electronic and Computer Engineering (ECE), The Hong Kong University of Science and Technology (HKUST), Clear Water Bay, Kowloon, Hong Kong (e-mail: nkkundu@connect.ust.hk).
M. R. McKay was with the Department of ECE, HKUST. He is now with the Department of Electrical and Electronic Engineering, University of Melbourne, Melbourne, Australia (e-mail: m.mckay@ust.hk, matthew.mckay@unimelb.edu.au).
S. P. Dash is with the School of Electrical Sciences, Indian Institute of Technology Bhubaneswar, Odisha, India (e-mail: soumyapdashiitbbs@gmail.com).
R. K. Mallik is with the Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi, India (e-mail: rk-mallik@ee.iitd.ernet.in).

[20], [21], [56]–[58], since THz offers numerous advantages over optical frequencies such as less delicate pointing, acquisition and tracking, and being less affected by ambient light, atmospheric turbulence, scintillation, cloud, and dust [5], [17]–[19], [59]. Microwave frequency is not a feasible frequency spectrum for QKD, since the preparation vacuum thermal noise is much larger at room temperature at lower frequency spectrum. Therefore, THz frequency is a potential frequency spectrum for QKD applications since positive secret key rate (SKR) is achievable at room temperature due to lower thermal noise at THz frequencies [56], [58], [60].

Some recent studies have investigated the viability of THz CVQKD for both terrestrial [56], [58], [60]–[62], and inter-satellite links [62], [63]. One limiting factor of THz QKD is the low SKR and maximum transmission distance due to the high free-space path loss and atmospheric absorption loss at THz frequency spectrum. We recently proposed a MIMO THz CVQKD system that achieves a high SKR and large transmission distances by using multiple transmit and receive antennas [60]. Our initial work demonstrated the feasibility of MIMO transmission for CVQKD applications, assuming the availability of perfect channel knowledge at Alice and Bob. However, the estimation of the MIMO wireless channel between Alice and Bob, and analyzing the effect of channel estimation errors on the SKR of the system are important open questions which need to be addressed for practical implementation of the MIMO CVQKD system. This motivates us for the current work where we propose a practical channel estimation protocol for the MIMO THz CVQKD system, and incorporate the effect of channel estimation errors in the input-output model during the key generation phase. The main contributions of the paper can be summarized as follows:

- We propose a practical channel estimation protocol for the MIMO THz CVQKD system of [60]. This is necessary for realizing singular value decomposition (SVD)-based transmit-receive beamforming during the key generation protocol.
- We characterize the input-output relation between Alice and Bob during the key generation phase by incorporating the additional noise terms arising due to channel estimation errors and detector noise. We also characterize the variance of these additional noise terms, which is important for analyzing the SKR of the CVQKD system.
- In contrast to our previous work [60], where we considered only the Gaussian collective attack, here we consider two types of attacks implementable by Eve: individual and collective attacks. In the former case, the maximum key information that Eve can steal is given by Shannon's mutual information while in the latter stronger attack the maximum key information that Eve can steal is bounded by the Holevo information between Bob's output state and Eve's ancilla state. The type of attack that Eve can implement depends on the quantum resources available to her.
- We analyze the SKR for both types of attacks by incorporating the effects of channel estimation overhead, the additional noise terms due to imperfect channel

estimation, and the detector noise at Bob. We also derive simplified expansions for the SKR in order to intuitively understand the effect of different system parameters on the SKR of the MIMO CVQKD system.
- We carry out extensive numerical simulations to study the effect of channel estimation error on the SKR, and analyze the effect of key parameters such as pilot length and pilot power on the SKR of the MIMO CVQKD system. We also study the maximum threshold on the noise variance (arising due to channel estimation error) that the MIMO CVQKD system can tolerate in order to attain positive SKRs.

The rest of the paper is organized as follows. Section II presents the system model of the MIMO CVQKD system, the channel estimation protocol, and the input-output relation between Alice and Bob obtained from SVD based transmit-receive beamforming with imperfect channel state information. The SKR analysis for both the individual and collective attacks are presented in Section III. Simulation results are shown in Section IV and finally some concluding remarks are made in Section V.

Notation: Boldface ($\mathbf{A}$) letters are used for representing matrices. $\mathbf{A}^\dagger$ and $\mathbf{A}^T$ denote the conjugate transpose and transpose of a matrix $\mathbf{A}$, respectively. A matrix of all ones and all zeros is represented by $\mathbf{1}_{M \times N}, \mathbf{0}_{M \times N} \in \mathbb{C}^{M \times N}$, respectively, an $M \times M$ identity matrix is denoted by $\boldsymbol{I}_M$, and $\mathrm{diag}(\boldsymbol{a})$ with $\boldsymbol{a} \in \mathbb{C}^M$ returns an $M \times M$ diagonal matrix with the elements of $\boldsymbol{a}$ on its diagonals. A real multivariate Gaussian distribution with mean vector $\boldsymbol{\mu} \in \mathbb{R}^N$ and covariance matrix $\boldsymbol{\Sigma} \in \mathbb{R}^{N \times N}$ is denoted by $\mathcal{N}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$, and a multivariate complex Gaussian distribution is denoted by $\mathcal{CN}(\boldsymbol{\theta}, \boldsymbol{\Gamma})$ where $\boldsymbol{\theta} \in \mathbb{C}^N$ is the mean vector and $\boldsymbol{\Gamma} \in \mathbb{C}^{N \times N}$ is the covariance matrix. Finally, $\det(\mathbf{A})$ denotes the determinant of the square matrix $\mathbf{A}$.

II. System Model

A. MIMO CVQKD

We consider a beyond 5G/6G communication system where Alice and Bob have multiple antennas and operate in the THz frequency range for achieving high-rate data communications. Along with high-rate communications, they also wish to generate quantum secure keys for encrypting the sensitive data transmission. Alice and Bob use a CVQKD protocol to generate quantum secure keys which can then be used for OTP-based physical layer security or higher layer symmetric key encryption such as advanced encryption standards (AES) and digital encryption standards (DES).

In order to generate the quantum secure keys, Alice and Bob first estimate the wireless channel between them and then carry out the CVQKD key generation protocol as detailed in the subsections below. Alice and Bob use Gaussian coherent states as the quantum information carriers during channel estimation and key generation phases. Since generation and homodyne/heterodyne detection of Gaussian coherent states at optical frequencies is a mature technology, Alice and Bob can implement the THz CVQKD protocol by using optical-to-THz converters at the transmitter and THz-to-optical converters at

the receiver [56]. With the recent advancements in optical-to-THz conversion technologies [64]–[68], Alice can use an optical-THz converter before transmitting the THz signals using the MIMO antennas, whereas Bob can use a THz-optical converter for homodyne/heterodyne detection of the received THz signals at the MIMO antennas. Alternatively, THz CVQKD can be implemented by using signal generators and homodyne/heterodyne detectors that operate directly at THz frequencies, as proposed in [58]. Recently, significant experimental progress has been made in THz signal generation by using femtosecond lasers and semiconductor crystals [69]–[71], along with direct homodyne/heterodyne detection of THz frequencies by using electronic/opto-electronic mixers, and plasmonic contact electrodes [72]–[74].

B. Channel Model

We assume that Alice and Bob have N_t and N_r antennas, respectively. The MIMO wireless channel $\mathbf{H} \in \mathbb{C}^{N_r \times N_t}$ between Alice and Bob can be modeled as [21], [75]

$$\mathbf{H} = \sum_{l=1}^{L} \sqrt{\gamma_l} e^{j2\pi f_c \tau_l} \boldsymbol{\psi}_R\left(\phi_l^r\right) \boldsymbol{\psi}_T^{\dagger}\left(\phi_l^t\right) , \qquad (1)$$

where f_c and L denote the frequency of the carrier signal and total number of multipaths, respectively. Furthermore, γ_l and τ_l denote the the path loss and propagation delay of the l-th multipath, respectively. Moreover, ϕ_l^r denotes the angle of arrival for Bob's uniform linear array (ULA) at its l-th multipath component, and ϕ_l^t denotes the angle of departure from Alice's ULA at its l-th multipath component. For the ULAs, the array response vectors $\boldsymbol{\psi}_R\left(\phi_l^r\right)$ and $\boldsymbol{\psi}_T\left(\phi_l^t\right)$ are given by

$$\boldsymbol{\psi}_R\left(\phi_l^r\right) = \frac{1}{\sqrt{N_r}}[1, e^{j\frac{2\pi}{\lambda}d_r \sin\phi_l^r}, \ldots, e^{j\frac{2\pi}{\lambda}d_r(N_r-1)\sin\phi_l^r}]^T ,$$

$$\boldsymbol{\psi}_T\left(\phi_l^t\right) = \frac{1}{\sqrt{N_t}}[1, e^{j\frac{2\pi}{\lambda}d_t \sin\phi_l^t}, \ldots, e^{j\frac{2\pi}{\lambda}d_t(N_t-1)\sin\phi_l^t}]^T ,$$

$$(2)$$

where d_t, d_r are the inter-antenna spacings at Alice's and Bob's ULAs, respectively, and λ denotes the wavelength of the carrier signal. In the channel model (1), γ_l denotes the path loss which can be modelled as [61]

$$\gamma_l = \begin{cases} \left(\frac{\lambda}{4\pi d_l}\right)^2 G_t G_r 10^{-0.1\delta d_l}, & l = 1 \text{ (LoS)} \\ \beta r_l \left(\frac{\lambda}{4\pi d_l}\right)^2 G_t G_r 10^{-0.1\delta d_l}, & l = 2, 3, \ldots, L \text{ (NLoS)} \end{cases}$$

$$(3)$$

where LoS and NLoS denote line-of-sight and non-line-of-sight path, respectively, d_l denotes the corresponding path length, and δ denotes the atmospheric absorption coefficient in dB/km. Furthermore, β denotes the Rayleigh roughness factor of the scattering objects, r_l denotes the Fresnel reflection coefficient of the surface encountered by the l-th multipath component. The array gains of Bob's and Alice's ULAs are denoted by G_r and G_t, respectively which depend on the antennas gain of each element G_a as [76]

$$G_r = N_r G_a , \ G_t = N_t G_a . \qquad (4)$$

Similar to our initial work on THz MIMO CVQKD [60], *we incorporate the effects of both free-space path loss along with the atmospheric attenuation loss*, in contrast to the earlier works on THz CVQKD [56], [58] which did not consider the free-space path loss component in the channel model.

C. Channel Estimation

We consider a MIMO CVQKD system where the wireless channel between Alice and Bob is estimated by Bob prior to the deployment of the actual key distribution protocol. We assume a perfect feedback link between Bob and Alice such that the estimated channel parameters are fed back to Alice by Bob via a public authenticated channel. Furthermore, we consider that Eve does not have the knowledge of the wireless channel initially, and she tries to gain knowledge of the MIMO channel matrix by intercepting the feedback link. Additionally, we assume that the best channel estimate that Eve can attain is the channel estimated by Bob during the channel estimation phase. A schematic diagram of the channel estimation protocol with the classical feedback channel is shown in Fig. 1.
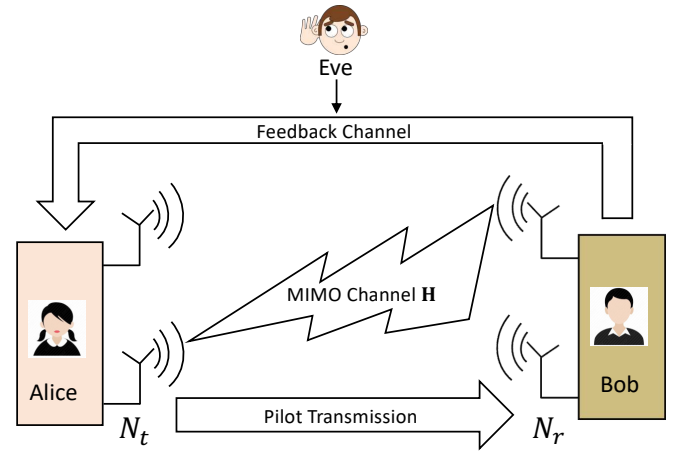
Fig. 1. A schematic diagram of channel estimation protocol in which Eve gains the channel knowledge by intercepting the classical feedback channel.

During the channel estimation phase Alice transmits pilot signals to Bob. During the t-th pilot transmission phase, Alice prepares N_t Gaussian coherent states $\left|\alpha_{p,i}^t\right\rangle$ with $\alpha_{p,i}^t = q_{p,i}^t + jp_{p,i}^t, \forall i = 1, \ldots, N_t$, which are then transmitted them from the N_t antennas. The signal power during the pilot transmission phase is V_p such that $\mathbb{E}[(q_{p,i}^t)^2] = \mathbb{E}[(p_{p,i}^t)^2] = V_p$, with $\mathbb{E}[\cdot]$ denoting the expectation operator. The transmitted pilot signal modes from Alice during the t-th pilot transmission phase is denoted as $\mathbf{x}_p^t = \mathbf{q}_p^t + j\mathbf{p}_p^t$, where $\mathbf{q}_p^t = [q_{p,1}^t, \ldots, q_{p,N_t}^t]^T$ and $\mathbf{p}_p^t = [p_{p,1}^t, \ldots, p_{p,N_t}^t]^T$. After receiving the signal modes, Bob performs heterodyne measurement to measure both quadratures of the received mode. This results in the following input-output relation for the t-th pilot transmission phase given by

$$\mathbf{y}^t = \mathbf{H}\mathbf{x}_p^t + \mathbf{H}\mathbf{x}_0^t + \mathbf{n}_{\text{het}}^t , \qquad (5)$$

where $\text{Re}\{\mathbf{y}^t\} = \hat{\mathbf{X}}_{B,I}^t$, $\text{Im}\{\mathbf{y}^t\} = \hat{\mathbf{X}}_{B,Q}^t$ are the in-phase and quadrature phase components, respectively, of the re-

ceived mode at Bob after performing the heterodyne measurement, and $\mathbf{n}_{\text{het}}^t = \mathbf{n}_{\text{het},I}^t + j\mathbf{n}_{\text{het},Q}^t$ is the additive receiver noise due to heterodyne measurement with $\mathbf{n}_{\text{het},I}^t, \mathbf{n}_{\text{het},Q}^t \sim \mathcal{N}\left(\mathbf{0}_{N_r \times 1}, (2v_{\text{el}} + 1)\boldsymbol{I}_{N_r}\right)$, where v_{el} is the variance of the electronic noise [77]. Furthermore, $\mathbf{x}_0^t = \mathbf{q}_0^t + j\mathbf{p}_0^t$ is the preparation thermal noise at Alice with $\mathbf{q}_0^t, \mathbf{p}_0^t \sim \mathcal{N}\left(\mathbf{0}_{N_t \times 1}, V_0 \boldsymbol{I}_{N_t}\right)$. Here V_0 is the thermal noise variance given by $V_0 = 2\bar{n} + 1$ with $\bar{n} = \left[\exp(hf_c/\kappa_B T_e) - 1\right]^{-1}$, where h and κ_B denote the Planck's and Boltzmann's constants, respectively and T_e is the environmental temperature in Kelvin.

We assume a quasi-static channel model where the channel matrix $\mathbf{H}$ remains constant over the coherence time of the channel T_c. Let $T_p < T_c$ be the pilot duration. Collecting all the received signal modes at Bob over $t = 1, 2, \ldots, T_p$, the equivalent signal model can be written as

$$\mathbf{Y}_p = \mathbf{H}\mathbf{X}_p + \mathbf{H}\mathbf{X}_0 + \mathbf{N}_{\text{het}}, \tag{6}$$

where $\mathbf{Y}_p = [\mathbf{y}^1, \ldots, \mathbf{y}^{T_p}] \in \mathbb{C}^{N_r \times T_p}$ is the matrix containing the received signals at Bob, $\mathbf{X}_p = [\mathbf{x}_p^1, \ldots, \mathbf{x}_p^{T_p}] \in \mathbb{C}^{N_t \times T_p}$ is the matrix containing the transmitted pilot signals from Alice, $\mathbf{X}_0 = [\mathbf{x}_0^1, \ldots, \mathbf{x}_0^{T_p}] \in \mathbb{C}^{N_t \times T_p}$ contains the unknown preparation thermal noise, and $\mathbf{N}_{\text{het}} = [\mathbf{n}_{\text{het}}^1, \ldots, \mathbf{n}_{\text{het}}^{T_p}] \in \mathbb{C}^{N_r \times T_p}$ contains the additive electronic noise at Bob. Alice and Bob agree upon a fixed pilot matrix $\mathbf{X}_p$ over a classical public channel for the purpose of channel estimation. As such, $\mathbf{X}_p$ is perfectly known to both Alice and Bob. The problem of channel estimation requires estimating the unknown matrix $\mathbf{H}$ from the equivalent linear measurement model

$$\mathbf{Y}_p = \mathbf{H}\mathbf{X}_p + \tilde{\mathbf{N}}, \tag{7}$$

where $\tilde{\mathbf{N}} = \mathbf{H}\mathbf{X}_0 + \mathbf{N}_{\text{het}}$ is the equivalent noise matrix. Note that the covariance matrix of $\tilde{\mathbf{N}}$ is unknown since $\mathbf{H}$ is unknown. To estimate $\mathbf{H}$, we employ a least squares (LS) scheme which leads to

$$\mathbf{H}_{\text{LS}} = \mathbf{Y}_p \mathbf{X}_p^+, \tag{8}$$

where $\mathbf{X}_p^+ = \mathbf{X}_p^\dagger \left(\mathbf{X}_p \mathbf{X}_p^\dagger\right)^{-1}$. Therefore, in order to estimate the MIMO channel, Bob first collects the heterodyne measurement outcomes $\mathbf{y}^t$, $t = 1, \ldots, T_p$ from (5) in the matrix $\mathbf{Y}_p$ given by (6), and then estimates the channel using (8) and the knowledge of the pilot matrix $\mathbf{X}_p$. After estimating the channel matrix, Bob feeds back the estimated channel to Alice using the classical public authenticated channel as shown in Fig. 1. Note that the knowledge of the estimated channel matrix is used for transmit beamforming by Alice during the key generation phase as detailed in Section II-D.

1) Optimal Pilot Matrix: We now find the optimal pilot matrix $\mathbf{X}_p$ that minimizes the channel estimation error. Substituting (7) in (8), we obtain

$$\mathbf{H}_{\text{LS}} = \mathbf{H} + \underbrace{\tilde{\mathbf{N}}\mathbf{X}_p^+}_{\Delta\mathbf{H}}. \tag{9}$$

The optimal pilot matrix that minimizes the mean squared error $\mathbb{E}\left[\|\Delta\mathbf{H}\|_F^2\right] = \mathbb{E}\left[\text{tr}\left(\Delta\mathbf{H}\Delta\mathbf{H}^\dagger\right)\right]$ can be obtained by solving the following optimization problem

$$\min_{\mathbf{X}_p} \quad \text{tr}\left(\mathbb{E}\left[\tilde{\mathbf{N}}\mathbf{X}_p^\dagger \left(\mathbf{X}_p\mathbf{X}_p^\dagger\right)^{-2}\mathbf{X}_p\tilde{\mathbf{N}}^\dagger\right]\right)$$
$$\text{s.t} \quad \text{tr}\left(\mathbf{X}_p^\dagger\mathbf{X}_p\right) = V_p N_t T_p. \tag{10}$$

We note that the columns of the noise matrix $\tilde{\mathbf{N}}$ are independent and identically distributed Gaussian random vectors. Let $\mathbf{C}_n$ be the covariance matrix of the columns of $\tilde{\mathbf{N}}$; we then have $\tilde{\mathbf{N}} \sim \mathcal{CN}_{N_r, T_p}\left(\mathbf{0}_{N_r \times T_p}, \mathbf{C}_n \otimes \mathbf{I}_{T_p}\right)$. Using the result from [78, Lemma 4] for the mean of a matrix-variate complex quadratic form, the equivalent optimization problem is given by

$$\min_{\mathbf{X}_p} \quad \text{tr}\left(\left(\mathbf{X}_p\mathbf{X}_p^\dagger\right)^{-3}\right)\text{tr}\left(\mathbf{C}_n\right)$$
$$\text{s.t} \quad \text{tr}\left(\mathbf{X}_p^\dagger\mathbf{X}_p\right) = V_p N_t T_p. \tag{11}$$

The optimal $\mathbf{X}_p$ that minimizes the objective satisfies $\mathbf{X}_p\mathbf{X}_p^\dagger = (V_p T_p)\mathbf{I}_{N_t}$ [79], [80]. Thus, $\mathbf{X}_p$ should contain orthogonal rows with the norm of each row being equal to $\sqrt{V_p T_p}$. One particular solution is constructed from the discrete Fourier transform (DFT) matrix, given by

$$\mathbf{X}_p = \sqrt{V_p}\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & W_{T_p} & \cdots & W_{T_p}^{T_p-1} \\ \vdots & \vdots & & \vdots \\ 1 & W_{T_p}^{N_t-1} & \cdots & W_{T_p}^{(N_t-1)(T_p-1)} \end{bmatrix}, \tag{12}$$

where $W_{T_p} = e^{j2\pi/T_p}$. This will be applied throughout the rest of the paper.

D. Key Generation

In this subsection we characterize the input-output relation between Alice and Bob during the key generation phase obtained from SVD-based transmit-receive beamforming. In contrast to our previous work [60] that assumed perfect channel knowledge, here we incorporate the effects of channel estimation error in the input-output model.

During the key generation phase, Alice employs Gaussian modulation for encoding the key information. She generates two statistically independent random vectors, $\boldsymbol{p}_A$ and $\boldsymbol{q}_A$, that follow a Gaussian distribution, i.e., $\boldsymbol{p}_A, \boldsymbol{q}_A \sim \mathcal{N}\left(\mathbf{0}_{N_t \times 1}, V_s\mathbf{I}_{N_t}\right)$, where V_s denotes the power utilized for encoding the initial key information. She then generates N_t displaced Gaussian coherent states denoted as $|\alpha_i\rangle$ with $\alpha_i = q_{A,i} + jp_{A,i}, \forall i = 1, \ldots, N_t$, and radiates them from her transmit antennas. We assume that during the key generation phase, Eve has the knowledge of $\mathbf{H}_{\text{LS}}$ and uses it to inject her Gaussian mode. Let $\mathbf{H}_{\text{LS}} = \mathbf{U}_{\text{LS}}\boldsymbol{\Sigma}_{\text{LS}}\mathbf{V}_{\text{LS}}^\dagger$ be the SVD of $\mathbf{H}_{\text{LS}}$. Analogous to [60], Alice uses $\mathbf{V}_{\text{LS}}$ for transmit beamforming and Bob uses $\mathbf{U}_{\text{LS}}$ for receive combining. The effective input-output relation during the key generation phase is then given by

$$\hat{\boldsymbol{a}}_B = \mathbf{U}_{\text{LS}}^\dagger \mathbf{H}\mathbf{V}_{\text{LS}}\hat{\boldsymbol{a}}_A + \mathbf{U}_{\text{LS}}^\dagger\mathbf{U}_{\text{LS}}\mathbf{S}_{\text{LS}}\hat{\boldsymbol{a}}_E, \tag{13}$$

where $\hat{\boldsymbol{a}}_A = [\hat{a}_{A,1}, \ldots, \hat{a}_{A,N_t}]^T$ represents the vector of transmitted mode from Alice, $\hat{\boldsymbol{a}}_B = [\hat{a}_{B,1}, \ldots, \hat{a}_{B,N_r}]^T$

represents the received mode vector at Bob, and $\hat{\boldsymbol{a}}_E = [\hat{a}_{E,1}, \ldots, \hat{a}_{E,N_t}]^T$ represents the Gaussian noise vector introduced by Eve to extract the key information. Further, $\boldsymbol{\Sigma}_{\text{LS}}$ and $\mathbf{S}_{\text{LS}}$ are diagonal matrices with entries

$$\boldsymbol{\Sigma}_{\text{LS}} = \text{diag}\left\{\sqrt{\hat{T}_1}, \ldots, \sqrt{\hat{T}_r}, \mathbf{0}_{(m-r)\times 1}\right\},$$
$$\mathbf{S}_{\text{LS}} = \text{diag}\left\{\sqrt{1-\hat{T}_1}, \ldots, \sqrt{1-\hat{T}_r}, \mathbf{1}_{(m-r)\times 1}\right\}, \quad (14)$$

where $m = \min(N_t, N_r)$, and $\hat{T}_1, \ldots, \hat{T}_r$ denote the r non-zero eigenvalues of $\mathbf{H}_{\text{LS}}^\dagger \mathbf{H}_{\text{LS}}$. Using (9) in (13), the equivalent input-output model admits

$$\hat{\boldsymbol{a}}_B = \boldsymbol{\Sigma}\hat{\boldsymbol{a}}_A \underbrace{- \mathbf{U}_{\text{LS}}^\dagger \Delta \mathbf{H} \mathbf{V}_{\text{LS}} \hat{\boldsymbol{a}}_A}_{\mathbf{n}_h} + \mathbf{S}_{\text{LS}} \hat{\boldsymbol{a}}_E, \quad (15)$$

where $\mathbf{n}_h$ represents the additional noise term arising due to channel estimation error.

Bob performs measurement on the received signal mode in order to extract the secret key information. Note that during the channel estimation phase, Bob performs heterodyne measurement since both quadratures of the received signal should be measured in order to estimate the complex valued channel matrix $\mathbf{H}$. On the other hand, during the key generation phase, Bob can perform either homodyne or heterodyne measurement since the secret key can be extracted from the real-valued measurement outcome of one of the quadratures or both. Upon performing the measurement, the input-output relation between Alice and Bob in terms of the quadratures is given by

$$\hat{X}_{B,i} = \sqrt{\hat{T}_i}\hat{X}_{A,i} + \sqrt{1-\hat{T}_i}\hat{X}_{E,i} - n_{h,i} + n_{\text{det},i},$$
$$i = 1, 2, \ldots, r, \quad (16)$$

where $\hat{X}_{B,i}$ represents Bob's quadrature measurement outcome, $\hat{X}_{A,i}$ represents Alice's transmitted quadrature of the i-th coherent state, and $\hat{X}_{E,i}$ denotes the Gaussian noise's quadrature injected by Eve to extract the key information. Here $\hat{X}$ denotes one of the two quadratures $\{\hat{q}, \hat{p}\}$, i.e., $\hat{X}_{A,i} = \{\hat{q}_{A,i}, \hat{p}_{A,i}\}$, and a same notation applies for the quadratures of Bob and Eve, $\hat{X}_{B,i}, \hat{X}_{E,i}$. Due to the presence of preparation thermal noise of variance V_0, Alice's transmitted mode has a variance of $V(\hat{X}_{A,i}) = V_a = V_s + V_0$. The Gaussian noise introduced by Eve has a power of $V(\hat{X}_{E,i}) = W$. The distribution of $n_{h,i}$ arising from channel estimation error is given by $n_{h,i} \sim \mathcal{N}(0, \sigma_{h,i}^2)$, with $\sigma_{h,i}^2 = 0.5\mathbf{C}_h(i,i)$, where $\mathbf{C}_h$ denotes the covariance matrix of the additional noise vector $\mathbf{n}_h$ in (15). Furthermore, $n_{\text{det},i} \sim \mathcal{N}(0, \sigma_{\text{det}}^2)$ is the detector noise with $\sigma_{\text{det}}^2 = d(1 + v_{el}) - 1$, where d is the measurement parameter which takes the value $d = 1$ for homodyne measurement and $d = 2$ for heterodyne measurement.

1) Estimation of Noise Covariance Matrix: Alice and Bob estimate the SKR based on the input-output model in (16), and decide to use the secret key for encryption only if the estimated SKR is above a threshold. In order to estimate the SKR, Alice and Bob need to estimate the variance of the noise terms in (16). We assume that Bob's detector noise variance σ_{det}^2 is perfectly known to Bob and he only needs to estimate

$\sigma_{h,i}^2$, which depends on $\mathbf{C}_h$. Therefore, in this subsection we find an estimator of $\mathbf{C}_h$. Using (15), the covariance matrix $\mathbf{C}_h$ can be expressed as

$$\begin{aligned}
\mathbf{C}_h = \mathbb{E}\left[\mathbf{n}_h \mathbf{n}_h^\dagger\right] &= \mathbb{E}\left[\mathbf{U}_{\text{LS}}^\dagger \tilde{\mathbf{N}} \mathbf{X}_p^+ \mathbf{V}_{\text{LS}} \hat{\boldsymbol{a}}_A \hat{\boldsymbol{a}}_A^\dagger \mathbf{V}_{\text{LS}}^\dagger (\mathbf{X}_p^+)^\dagger \tilde{\mathbf{N}}^\dagger \mathbf{U}_{\text{LS}}\right] \\
&\overset{(a)}{=} 2V_a \mathbb{E}\left[\mathbf{U}_{\text{LS}}^\dagger \tilde{\mathbf{N}} \mathbf{X}_p^+ (\mathbf{X}_p^+)^\dagger \tilde{\mathbf{N}}^\dagger \mathbf{U}_{\text{LS}}\right] \\
&\overset{(b)}{=} \frac{2V_a}{V_p^2 T_p^2} \mathbb{E}\left[\mathbf{U}_{\text{LS}}^\dagger \tilde{\mathbf{N}} \mathbf{X}_p^\dagger \mathbf{X}_p \tilde{\mathbf{N}}^\dagger \mathbf{U}_{\text{LS}}\right] \\
&\overset{(c)}{=} \frac{2V_a \text{tr}\left(\mathbf{X}_p^\dagger \mathbf{X}_p\right)}{V_p^2 T_p^2} \mathbf{U}_{\text{LS}}^\dagger \mathbf{C}_n \mathbf{U}_{\text{LS}} \\
&\overset{(d)}{=} \frac{2V_a N_t}{V_p T_p} \mathbf{U}_{\text{LS}}^\dagger \mathbf{C}_n \mathbf{U}_{\text{LS}}, \quad (17)
\end{aligned}$$

where we have used $\mathbb{E}\left[\hat{\boldsymbol{a}}_A \hat{\boldsymbol{a}}_A^\dagger\right] = 2V_a \mathbf{I}_{N_t}$ in equality (a), and $\mathbf{X}_p \mathbf{X}_p^\dagger = V_p T_p \mathbf{I}_{N_t}$ in equality (b). Furthermore, equality (c) follows from [78, Lemma 4], and we use $\text{tr}\left(\mathbf{X}_p^\dagger \mathbf{X}_p\right) = V_p N_t T_p$ in equality (d).

Since the noise covariance matrix $\mathbf{C}_n$ is unknown, we first find a maximum likelihood (ML) estimate of $\mathbf{C}_n$, which is then used to estimate $\mathbf{C}_h$. Given the estimate of the channel matrix $\mathbf{H}_{\text{LS}}$ and the knowledge of the pilot matrix $\mathbf{X}_p$, the ML estimate of $\mathbf{C}_n$ is given by

$$\begin{aligned}
\hat{\mathbf{C}}_n &= \underset{\mathbf{C}_n}{\text{argmax}} \; p\left(\mathbf{Y}_p | \mathbf{H}_{\text{LS}}, \mathbf{X}_p\right) \\
&= \underset{\mathbf{C}_n}{\text{argmax}} \prod_{t=1}^{T_p} \frac{\exp\left\{-(\mathbf{y}^t - \mathbf{H}_{\text{LS}}\mathbf{x}_p^t)^\dagger \mathbf{C}_n^{-1}(\mathbf{y}^t - \mathbf{H}_{\text{LS}}\mathbf{x}_p^t)\right\}}{\pi^{N_r}\det(\mathbf{C}_n)}.
\end{aligned}$$
$$(18)$$

Taking the log of the likelihood, the equivalent optimization problem is given by

$$\begin{aligned}
\hat{\mathbf{C}}_n = \underset{\mathbf{C}_n}{\text{argmin}} \Bigg(&T_p \log \det(\mathbf{C}_n) \\
&+ \sum_{t=1}^{T_p} (\mathbf{y}^t - \mathbf{H}_{\text{LS}}\mathbf{x}_p^t)^\dagger \mathbf{C}_n^{-1}(\mathbf{y}^t - \mathbf{H}_{\text{LS}}\mathbf{x}_p^t)\Bigg).
\end{aligned}$$
$$(19)$$

Taking the matrix variate derivative of the objective function of (19) with respect to $\mathbf{C}_n$ and setting it to zero, the ML estimate of $\mathbf{C}_n$ is given by

$$\hat{\mathbf{C}}_n = \frac{1}{T_p}\sum_{t=1}^{T_p}\left(\mathbf{y}^t - \mathbf{H}_{\text{LS}}\mathbf{x}_p^t\right)\left(\mathbf{y}^t - \mathbf{H}_{\text{LS}}\mathbf{x}_p^t\right)^\dagger. \quad (20)$$

Using the ML estimate of $\mathbf{C}_n$ in (17), the estimated value of $\mathbf{C}_h$ is given by

$$\hat{\mathbf{C}}_h = \frac{2V_a N_t}{V_p T_p}\mathbf{U}_{\text{LS}}^\dagger \hat{\mathbf{C}}_n \mathbf{U}_{\text{LS}}, \quad (21)$$

which may be used for estimating $\sigma_{h,i}^2 = 0.5\mathbf{C}_h(i,i)$, as required for estimating the SKR.

III. SECRET KEY RATE ANALYSIS

In this section we present the SKR of the MIMO CVQKD system by incorporating the channel estimation errors and the involved overhead. We assume that the entire coherence block is used to generate the secret keys which can then be used for OTP based encryption for data transmission in the subsequent coherence blocks. For generating the secret keys, Alice and Bob begin by generating a correlated random vectors' string $\{\hat{X}_{A,n}, \hat{X}_{B,n}\}_{n=1}^{N}$ by repeating the quantum key distribution protocol described in section II-D, N times. Given that T_c is the coherence time and T_p is the pilot overhead, N may be selected as $N = T_c - T_p$. For extracting the final keys, a reconciliation or sifting protocol is carried out by Alice and Bob over a classical authenticated channel, followed by error correction on the raw keys [81]. There are two types of reconciliation protocols: direct reconciliation (DR), where Alice declares which of the two quadratures should be used for the secret key generation, and reverse reconciliation (RR), where Bob declares which of the two quadratures were measured by him and should be used for the secret key generation on a classical public channel. It has been previously shown that RR has a higher SKR than the DR strategy since Eve (who has full control over the channel) can extract larger information if Alice declares which of the quadratures should be used for the secret key [56], [81]. The reason is that in DR, the signals sent by Alice are accessible to Eve via the ancilla modes that she injects and are stored in her quantum memory. However, in RR the measurement outcomes of Bob are not accessible by Eve. Similar to our initial work [60], here we focus only on RR since positive SKR can be achieved by this scheme for any channel transmittance $\hat{T}_i \in [0, 1]$. On the other hand, for DR we require $\hat{T}_i > 0.5$ in order to achieve positive SKRs [81], which is practically challenging owing to significantly higher path loss (see (3)) at THz frequencies [56].

In addition to the reconciliation protocol, the SKR also depends on the type of attack that Eve can perform. The general assumptions under which the SKRs are evaluated are [82]: (i) Eve has unlimited computational power, (ii) Eve has full access to the quantum channel, (iii) Alice and Bob use an authenticated classical channel for error correction and information reconciliation, and (iv) Eve cannot access the apparatuses used by Alice and Bob in their respective laboratories. There are two types of attacks which Eve can implement and these are ranked in terms of the increasing amount of information that Eve can extract. These attacks depend on how Eve interacts with the individual signals sent by Alice and when she measures the ancilla mode stored in her quantum memory. Here, for both types of attacks, we generalize the SKRs of the SISO system carried out in [77], [82] for our proposed MIMO system.

A. Eve Attack Mode I: Individual Attack

Individual attack is the weakest attack which Eve can implement. Here, she individually measures each incoming signal from Alice and the ancilla output is stored in a quantum memory. In order to extract the key information she measures the ancilla mode before the error correction step but after the reconciliation protocol carried out by Alice and Bob. For individual attack, the maximum key information accessible to Eve is given by the Shannon's mutual information between Eve's and Bob's measurement outcomes. The optimal individual attack is given by the Gaussian individual attack [82]. When Eve implements an individual attack, the SKR of the i-th parallel channel (in RR) is expressed as

$$R_i^I = \left(1 - \frac{T_p}{T_c}\right)\left(\beta I\left(X_{A,i} : X_{B,i}\right) - I\left(X_{B,i} : E_i\right)\right),$$
$$i = 1, \ldots, r, \quad (22)$$

where $I\left(X_{A,i} : X_{B,i}\right)$ denotes the Shannon's mutual information of Alice's and Bob's measurement outcomes, $I\left(X_{B,i} : E_i\right)$ denotes the Shannon's mutual information of Eve's and Bob's measurement for the i-th parallel channel, and β is the reconciliation efficiency. Note that the factor $(1 - T_p/T_c)$ arises in (22) due to the channel estimation overhead. The Shannon's mutual information of Alice's and Bob's measurement outcomes for the i-th parallel channel is thus given as

$$I\left(X_{A,i} : X_{B,i}\right) = \frac{d}{2}\log_2\left(1 + \frac{\hat{T}_i V_s}{\Lambda_i\left(V_0, W\right) + \sigma_{\det}^2 + \sigma_{h,i}^2}\right),$$
$$(23)$$

where $\Lambda_i(x, y) \triangleq \hat{T}_i x + (1 - \hat{T}_i)y$, and d is the measurement parameter which takes the value $d = 1$ for homodyne measurement and $d = 2$ for heterodyne measurement. Since in the individual attack Eve measures the ancilla just after Bob reveals the quadratures measured by him and before the error correction, the maximum accessible information to Eve is restricted by the Shannon's information obtained from her ancilla. Eve's information in RR is given by

$$I\left(X_{B,i} : E_i\right) = \frac{d}{2}\log_2\left(\frac{V_B^i}{V_{B|E}^i}\right), \quad (24)$$

where $V_B^i = \Lambda_i\left(V_a, W\right) + \sigma_{h,i}^2 + \sigma_{\det}^2$ is the variance of the Bob's received string and $V_{B|E}^i = \frac{1}{\Lambda_i(1/V_a, W) + \sigma_{h,i}^2} + \sigma_{\det}^2$ is the conditional variance of Bob's received string given Eve's measurement for the i-th parallel channel [82], [83]. The overall SKR of the MIMO QKD system when Eve implements an individual attack is given by (25) at the top of the next page.

For a better understanding of the effect of the various important system parameters on the SKR, we find the first order Taylor Series expansion of the SKR with individual attack. In the low channel transmittance limit (i.e., $\hat{T}_i \to 0$), the SKR can be approximated as expressed by (26) at the top of the next page. The simplified expression (26) reveals that the presence of the additional noise terms due to channel estimation error $\sigma_{h,i}^2$ and detector noise $\sigma_{\det}^2$ degrades the overall SKR of the system. Further, it reveals that the SKRs are almost the same for both homodyne ($d = 1$) and heterodyne detection scheme ($d = 2$), since the detector noise $\sigma_{\det}^2$ increase by a factor of d that balances out the factor of d in the numerator of (26). This observation is also confirmed in our simulation results shown in Section IV.

$$R_{\mathrm{MIMO}}^I = \sum_{i=1}^r R_i^I = \left(1 - \frac{T_p}{T_c}\right) \sum_{i=1}^r \left(\beta \frac{d}{2} \log_2 \left(1 + \frac{\hat{T}_i V_s}{\Lambda_i(V_0, W) + \sigma_{\mathrm{det}}^2 + \sigma_{h,i}^2}\right) - \frac{d}{2} \log_2 \left(\frac{\Lambda_i(V_a, W) + \sigma_{h,i}^2 + \sigma_{\mathrm{det}}^2}{\frac{1}{\Lambda_i(1/V_a, W) + \sigma_{h,i}^2} + \sigma_{\mathrm{det}}^2}\right)\right) \tag{25}$$

$$R_{\mathrm{MIMO}}^I \approx \left(1 - \frac{T_p}{T_c}\right) \frac{d}{2\ln(2)} \sum_{i=1}^r \left(\left(\frac{\beta V_s + W - V_a}{\sigma_{\mathrm{det}}^2 + \sigma_{h,i}^2 + W} + \frac{V_a W - 1}{V_a(\sigma_{h,i}^2 + W)(1 + \sigma_{\mathrm{det}}^2(\sigma_{h,i}^2 + W))}\right) \hat{T}_i \right.$$
$$\left. - \ln\left(\frac{(\sigma_{\mathrm{det}}^2 + \sigma_{h,i}^2 + W)(\sigma_{h,i}^2 + W)}{1 + \sigma_{\mathrm{det}}^2(\sigma_{h,i}^2 + W)}\right)\right) \tag{26}$$

An asymptotic upper bound on the SKR with individual attack that assumes perfect channel knowledge and no detector noise can be found by setting $\sigma_{h,i}^2 = \sigma_{\mathrm{det}}^2 = 0$ in the SKR expression of (25). This SKR upper bound is given by

$$R_{\mathrm{MIMO}}^{I,\mathrm{UB}} = \sum_{i=1}^r \frac{1}{2}\left(\log_2\left(1 + \frac{T_i V_s}{T_i V_0 + (1 - T_i)W}\right) \right.$$
$$\left. - \log_2\left((T_i V_a + (1 - T_i)W)\left(\frac{T_i}{V_a} + (1 - T_i)W\right)\right)\right). \tag{27}$$

For a rank-1 MIMO channel, the SKR expression in (27) is the same as that of a SISO system derived in [84, Eq. 6.124]. We study the effect of channel estimation error and pilot overhead on the SKR performance by comparing the SKR obtained from (25) with the upper bound (27) in the simulation results section.

B. Eve Attack Mode II: Collective Attack

Collective attack is the next strongest attack implementable by Eve in order to extract the maximum key information. Here Eve individually measures each incoming signal from Alice, but she performs an optimal collective measurement on the collection of stored ancilla after the key distillation procedure. For this attack, the maximum key information that Eve can extract is given by the Holevo's information between Eve's and Bob's states. When Eve implements a Gaussian collective attack, the SKR of the i-th parallel channel (in RR) is obtained as

$$R_i^C = \left(1 - \frac{T_p}{T_c}\right)\left(\beta I(X_{A,i} : X_{B,i}) - \chi(X_{B,i} : E_i)\right),$$
$$i = 1, \ldots, r, \quad (28)$$

where $I(X_{A,i} : X_{B,i})$ is given in (23). Further, $\chi(X_{B,i} : E_i)$ is the Holevo information between Eve and Bob's quantum state for the i-th parallel channel, that admits

$$\chi(X_{B,i} : E_i) = S(E_i) - S(E_i | X_{B,i}), \tag{29}$$

where $S(E_i)$ is the von Neumann entropy of Eve's state and $S(E_i | X_{B,i})$ is the von Neumann entropy of Eve's state given Bob's measurement, which can be either homodyne or heterodyne.

Let $\hat{\rho}_{E,i}$ and $\hat{\rho}_{AB,i}$ be the density matrices of Eve's state and Alice-Bob's joint state, respectively, for the i-th parallel channel. Similar to the analysis carried out in [77, Sec.8.2], we assume that Eve has access to the purification of Alice-Bob's joint state $\hat{\rho}_{AB,i}$ such that the density matrix of the resulting state is given by $\hat{\rho}_{ABE,i} = |\psi\rangle\langle\psi|$. The density matrix of Eve's state can be obtained by carrying out the partial trace with respect to (w.r.t) the Alice-Bob subspace, i.e., $\hat{\rho}_{E,i} = \mathrm{tr}_{AB}(\hat{\rho}_{ABE,i}) = \mathrm{tr}_{AB}(|\psi\rangle\langle\psi|)$. Similarly, the joint Alice-Bob state can be obtained by carrying out the partial trace w.r.t Eve's subspace, i.e., $\hat{\rho}_{AB,i} = \mathrm{tr}_E(\hat{\rho}_{ABE,i}) = \mathrm{tr}_E(|\psi\rangle\langle\psi|)$. Thus, Eve's density operator $\hat{\rho}_{E,i}$ and Alice-Bob's density matrix $\hat{\rho}_{AB,i}$ have the same eigenvalues, which implies that both have the same von Neumann entropy. Thus, in order to evaluate the von Neumann entropy of Eve's state, it is sufficient to compute the von Neumann entropy of the Alice-Bob subsystem which does not depend on the measurement outcome of Bob. Further, the covariance matrix of the Alice-Bob Gaussian state for the i-th correlated string is given as

$$\boldsymbol{\Sigma}_{AB}^i = \begin{bmatrix} V_a \mathbf{I}_2 & \mathbf{C}_i \\ \mathbf{C}_i^T & b_i \mathbf{I}_2 \end{bmatrix}, \tag{30}$$

where

$$\mathbf{C}_i = \sqrt{\hat{T}_i(V_a^2 - 1)} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{31}$$

and

$$b_i = \Lambda_i(V_a, W) + \sigma_{h,i}^2. \tag{32}$$

The von Neumann entropy of a Gaussian quantum system can be evaluated by determining the symplectic eigenvalues of the covariance matrix. The symplectic eigenvalues λ_1^i, λ_2^i of $\boldsymbol{\Sigma}_{AB}^i$ can be determined by evaluating the eigenvalues of the matrix $|i\boldsymbol{\Omega}\boldsymbol{\Sigma}_{AB}^i|$, where the modulus is in the operatorial sense [23]. Here, $\boldsymbol{\Omega}$ is the symplectic matrix that admits [23]

$$\boldsymbol{\Omega} = \bigoplus_{k=1}^2 \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \tag{33}$$

where $\bigoplus$ denotes the matrix direct sum operation. For a general covariance matrix of the form

$$\boldsymbol{\Upsilon} = \begin{bmatrix} \boldsymbol{\alpha} & \boldsymbol{\gamma} \\ \boldsymbol{\gamma}^T & \boldsymbol{\rho} \end{bmatrix}, \tag{34}$$

the symplectic eigenvalues admit

$$\nu_{1,2} = \sqrt{\frac{1}{2}\left(\Delta \pm \sqrt{\Delta^2 - 4\det\Upsilon}\right)} , \qquad (35)$$

where $\Delta = \det\alpha + \det\rho + 2\det\gamma$ [23]. Using similar calculation for our case, the symplectic eigenvalues λ_1^i, λ_2^i admit

$$\lambda_{1,2}^i = \sqrt{\frac{1}{2}\left(A^i \pm \sqrt{(A^i)^2 - 4B^i}\right)} , \qquad (36)$$

where

$$A^i = V_a^2\left(1 - 2\hat{T}_i\right) + 2\hat{T}_i + \left(\Lambda_i\left(V_a, W\right) + \sigma_{h,i}^2\right)^2 ,$$
$$B^i = \left(\Lambda_i\left(1, V_a W\right) + V_a\sigma_{h,i}^2\right)^2 . \qquad (37)$$

Finally, the von Neumann entropy of Eve's state $S\left(E_i\right)$ is given by

$$S\left(E_i\right) = h\left(\lambda_1^i\right) + h\left(\lambda_2^i\right) , \qquad (38)$$

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

$$h(x) = \frac{(x+1)}{2}\log_2\frac{(x+1)}{2} - \frac{(x-1)}{2}\log_2\frac{(x-1)}{2} . \qquad (39)$$

The von Neumann entropy of Eve's state given Bob's measurement $S\left(E_i\big|X_{B,i}\right)$ depends on the type of measurement used by Bob which can be either homodyne or heterodyne. Since homodyne and heterodyne measurements are rank-1 projections, the conditional state of Alice and Eve given Bob's measurement outcome $\rho_{AE|X_{B,i}}$ is a pure state [48]. Therefore the conditional von Neumann entropy Eve's state given Bob's measurement is equal to the conditional von Neumann entropy Alice's state given Bob's measurement, i.e., $S\left(E_i\big|X_{B,i}\right) = S\left(A_i\big|X_{B,i}\right)$. Therefore, the the symplectic eigenvalues of the conditional covariance matrix of Alice's state given Bob's measurement outcome need to be evaluated in order to evaluate $S\left(E_i\big|X_{B,i}\right)$. Using the analysis from [23] for general Gaussian measurements, Alice's conditional covariance matrix when Bob performs homodyne measurement is given by

$$\Sigma_{A|X_{B,i}}^{\mathrm{hom}} = V_a\mathbf{I}_2 - (b_i + v_{el})^{-1}\mathbf{C}_i\mathbf{\Pi}\mathbf{C}_i^T , \qquad (40)$$

where $\mathbf{\Pi} := \mathrm{diag}\left(1, 0\right)$. The symplectic eigenvalue of $\Sigma_{A|X_{B,i}}^{\mathrm{hom}}$ is given by

$$\lambda_{\mathrm{hom}}^i = \sqrt{\det\Sigma_{A|X_{B,i}}^{\mathrm{hom}}} = \sqrt{V_a^2 - \frac{V_a\hat{T}_i(V_a^2 - 1)}{b_i + v_{el}}} . \qquad (41)$$

When Bob performs heterodyne measurement, the conditional covariance matrix of Alice is given by

$$\Sigma_{A|X_{B,i}}^{\mathrm{het}} = V_a\mathbf{I}_2 - (b_i + 2v_{el} + 1)^{-1}\mathbf{C}_i\mathbf{C}_i^T , \qquad (42)$$

which upon simplification gives

$$\Sigma_{A|X_{B,i}}^{\mathrm{het}} = \left(V_a - \frac{\hat{T}_i(V_a^2 - 1)}{b_i + 2v_{el} + 1}\right)\mathbf{I}_2 . \qquad (43)$$

The symplectic eigenvalue of $\Sigma_{A|X_{B,i}}^{\mathrm{het}}$ admits

$$\lambda_{\mathrm{het}}^i = V_a - \frac{\hat{T}_i(V_a^2 - 1)}{b_i + 2v_{el} + 1} . \qquad (44)$$

Therefore the conditional von Neumann entropy of Eve's state admits

$$S\left(E_i\big|X_{B,i}\right) = h\left(\lambda_{\mathrm{hom/het}}^i\right) , \qquad (45)$$

where $h(x)$ is the function defined in (39) and λ_{hom}^i, λ_{het}^i are given by (41) and (44), respectively. Finally, using (28) and (29), the overall SKR of the MIMO QKD system is given by (46) at the top of the next page.

Similar to the individual attack, we find a Taylor series expansion of the SKR of collective attack to more explicitly understand the effect of different system parameters on the SKR. In the low channel transmittance limit (i.e., $\hat{T}_i \to 0$), the SKR can be approximated as expressed by (47) at the top of the next page. The simplified expression of the SKR with collective attack in (47) reveals that in a practical MIMO CVQKD system, the SKR decreases due to the noise arising from channel estimation error $\sigma_{h,i}^2$ and detector noise σ_{det}^2. Similar to the individual attack case, the simplified expression in (47) reveals that the SKRs are almost the same for both homodyne ($d = 1$) and heterodyne detection schemes ($d = 2$) since the detector noise σ_{det}^2 increase by a factor of d that balances out the factor of d in the numerator of the two terms of (47) that depends on σ_{det}^2. This observation is also confirmed in our simulation results shown in Section IV. Furthermore, it is easy to verify that in the limit of perfect channel estimation ($\sigma_{h,i}^2 \to 0$, $T_p \to 0$), no detector noise ($\sigma_{\mathrm{det}}^2 \to 0$), and perfect reconciliation efficiency ($\beta \to 1$), the SKR expression in (47) is the same as that of the SKR upperbound presented in [60].

IV. SIMULATION RESULTS

Similar to [60], a simulation scenario with a dominant LoS path is considered with $L = 1$. As shown in [60], $10 - 30$ THz is a feasible frequency range that can be utilized to obtain a positive SKR. Here, we show the performance results at $f_c = 15$ THz, since the atmospheric absorption coefficient ($\delta = 50$ dB/Km) and the free space path loss are lower at $f_c = 15$ THz.

We first study the performance of the proposed channel estimation protocol by plotting the SKR of the MIMO CVQKD system using the ML estimate of the noise covariance matrix $\hat{\mathbf{C}}_n$. Fig. 2 shows the plot of the SKR (in bits/channel use) versus distance (m) for two MIMO configurations at $f_c = 15$ THz with homodyne detection. The plots show the SKR with individual and collective attacks obtained from (25) and (46), respectively. The ML estimate uses $\hat{\mathbf{C}}_n$ from (20) in (21), and the 'Genie Aided' one uses the true knowledge of $\mathbf{C}_n$ in (17) for evaluating the noise variance due to channel estimation error $\sigma_{h,i}^2$. It can be observed that at lower transmission distances, the SKR obtained from the 'Genie Aided' scheme is very close to that of the estimated SKR that uses the ML estimate $\hat{\mathbf{C}}_n$. However, at a large transmission distance for the (256×256) MIMO architecture, the estimated SKR is slightly higher than the true SKR (i.e., 'Genie Aided'). This is due to the fact that at high transmission distance the received pilot power is low (due to high path loss) that leads to a high channel estimation error. Furthermore, the estimation error of $\hat{\mathbf{C}}_n$ is high for the (256×256) MIMO configuration due to

This article has been accepted for publication in IEEE Transactions on Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2022.3161008

9

$$R_{\text{MIMO}}^{C} = \sum_{i=1}^{r} R_i^C = \left(1 - \frac{T_p}{T_c}\right) \sum_{i=1}^{r} \left(\beta \frac{d}{2} \log_2 \left(1 + \frac{\hat{T}_i V_s}{\Lambda_i(V_0, W) + \sigma_{\text{det}}^2 + \sigma_{h,i}^2}\right) - h(\lambda_1^i) - h(\lambda_2^i) + h(\lambda_{\text{hom/het}}^i)\right) \quad (46)$$

$$R_{\text{MIMO}}^{C} \approx \left(1 - \frac{T_p}{T_c}\right) \frac{1}{2\ln(2)} \sum_{i=1}^{r} \left(\left(\frac{\beta d V_s}{\sigma_{\text{det}}^2 + \sigma_{h,i}^2 + W} + \frac{(V_a^2 - 1)\ln\left(\frac{V_a+1}{V_a-1}\right)}{(V_a + W + \sigma_{h,i}^2)} - \frac{\sigma_{h,i}^2(WV_a - 2W^2 + 1)\ln\left(\frac{W+\sigma_{h,i}^2+1}{W+\sigma_{h,i}^2-1}\right)}{(W + \sigma_{h,i}^2)(V_a + W + \sigma_{h,i}^2)}\right.\right.$$
$$\left.\left. - \frac{d(V_a^2 - 1)\ln\left(\frac{V_a+1}{V_a-1}\right)}{2(W + \sigma_{h,i}^2 + \sigma_{\text{det}}^2)}\right)\hat{T}_i - h(W + \sigma_{h,i}^2)\right) \quad (47)$$

the large dimension of the noise covariance matrix that needs to be estimated. This estimation error leads to a mismatch between the true SKR and the estimated SKR, particularly at large transmission distances. This over-estimate of the SKRs can be mitigated by increasing the pilot power V_p or the pilot duration T_p at large transmission distances.
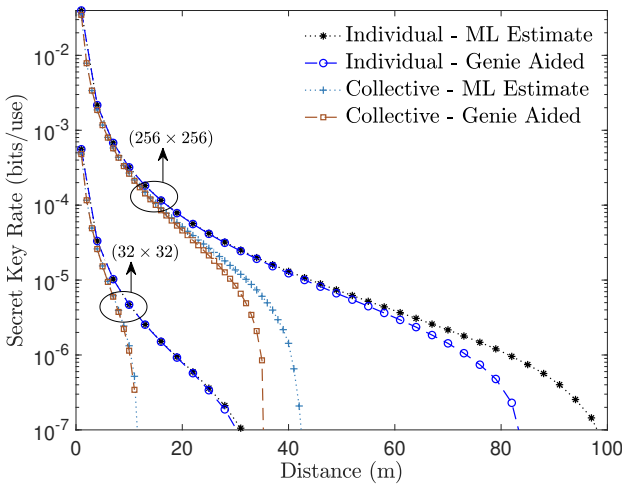

Fig. 2. The plots show the SKR (in bits/channel use) versus distance (m) for two MIMO architectures ($N_t \times N_r$) at $f_c = 15$ THz. Results are shown for individual and collective attacks with homodyne measurement using the ML estimate $\hat{\mathbf{C}}_n$, and the 'Genie Aided' one that uses true knowledge of $\mathbf{C}_n$ for evaluating $\sigma_{h,i}^2$. The other simulation parameters are $V_p = 60$ dB, $W = 1$, $T_e = 296$ K, $V_s = 1$, $v_{el} = 0.01$ and $\beta = 0.95$ [81]. The antenna gain of each of the elements at the transmitter and receiver arrays is $G_a = 30$ dBi [85], [86], $T_p = N_t + 500$, and $T_c = 5 \times 10^5$ [87].

Fig. 3 shows the SKR versus transmission distance for different MIMO configurations and $f_c = 15$ THz. It is observed that the practically achievable SKRs with homodyne and heterodyne measurements for the two different types of attacks that Eve can implement. For comparison, we also show the asymptotic SKR upper bound from [60, Eq. (20)] and (27) for collective and individual attacks respectively. It can be observed that there is a significant gap in the performance of the SKR upper bound and the practically achievable SKR, particularly at large transmission distances. This performance gap arises due additional noise terms due to channel estimation error, homodyne/heterodyne detector noise, imperfect reconciliation, and channel estimation overhead.

Furthermore, it can be observed that the performance of the homodyne and heterodyne detection schemes is almost the same for both individual and collective attacks. With the heterodyne scheme, the mutual information between Alice and Bob increases by a factor of two; however, the higher detection noise compensates this gain and the overall performance of homodyne and heterodyne schemes are virtually the same. This observation can also be understood from the approximate SKR expressions derived in (26), (47) for individual and collective attacks, respectively.

The plots in Fig. 3 reveal that although the SKR upper bound is only slightly better for the individual attack than the collective attack, the practical SKR performance is significantly better for the individual attack. Therefore, the practically achievable SKRs and the maximum transmission distances can be significantly reduced if Eve has the resources to implement the stronger Gaussian collective attack.

We now check the accuracy of the approximate SKR expressions derived in (26) and (47) for individual and collective attacks, respectively. Fig. 4 shows the plots of SKR in bits/channel use) versus transmission distance (m) obtained from the exact (25), (46) and approximate expressions (26), (47) for individual and collective attacks. Results are shown for two different MIMO configurations with homodyne measurement. We observe that the approximate expressions are accurate for practical transmission distances.

We next study the effect of pilot duration on the SKRs. Since the simulation results of Fig. 3 suggest that for practical transmission distances at THz frequencies, the SKRs are very similar for both homodyne detection and heterodyne detection schemes, here we present only the results for the homodyne case. Fig. 5(a) shows the plot of the SKR for individual and collective attacks as a function of the pilot duration T_p for different MIMO configurations at a fixed transmission distance of 20 m. From (17) it can be verified that as T_p increases the noise due to channel estimation error decreases, which suggests that the SKR should improve as T_p increases. The simulation results in Fig. 5(a) reveal that when Eve uses an individual attack, the SKR remains almost the same as T_p increases. On the other hand, the effect of increasing T_p on the SKR is more pronounced for the case of a collective attack where the SKR first increases as T_p increases and then saturates to a constant value. Therefore, the effect of channel estimation error on the SKR is more pronounced for
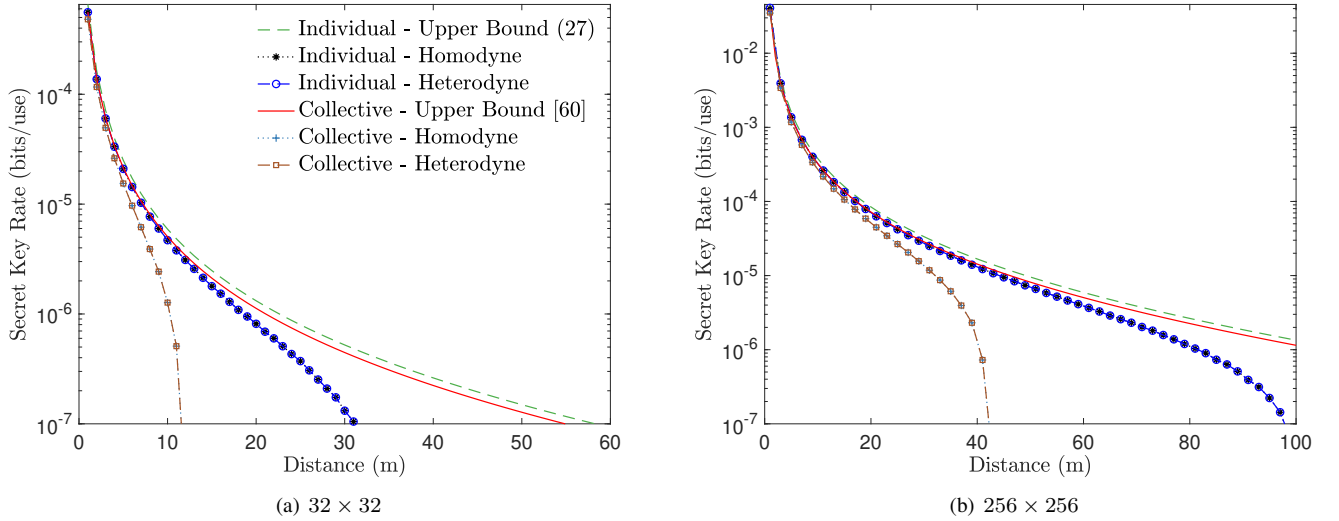
Fig. 3. The plots show the SKRs (bits/use) versus distance (m) for two MIMO architectures $(N_t \times N_r)$ at $f_c = 15$ THz. Results are shown for both individual and collective attacks with homodyne and heterodyne detection. For comparison we also show the asymptotic SKR upper bound from [60, eq. (20)] and (27) for collective and individual attacks, respectively. The other simulation parameters are the same as those of Fig. 2.
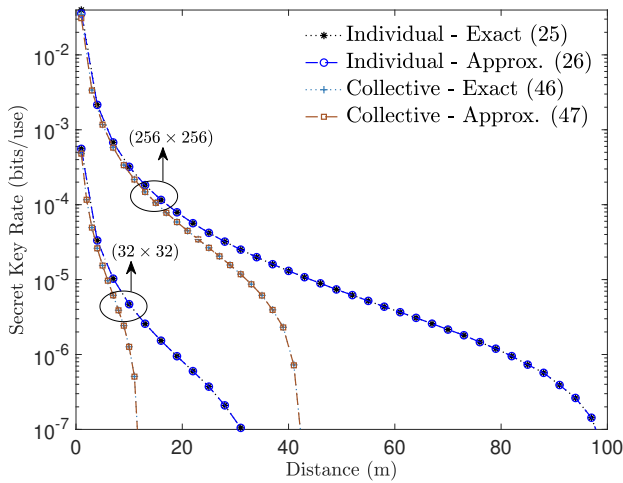

Fig. 4. The plots compare the SKRs (in bits/channel use) versus distance (m) obtained from the exact and approximate expressions. Results are shown for both individual and collective attacks for two different MIMO configurations with homodyne measurement. The simulation parameters are the same as those of Fig. 2.

the collective attack scenario than for the individual attack scenario. In a practical setting, it is desirable to have a smaller pilot duration since the computational complexity of channel estimation in (8) is $O(T_p N_r N_t)$ with the optimized choice of X_p in (12). Therefore, in practice, the pilot duration should be chosen as the minimum value of T_p at which the SKR saturates.

We also study the effect of the pilot power V_p on the SKRs. Fig. 5(b) shows the SKR as a function of V_p for different MIMO architectures at a fixed transmission distance of $d = 20$ m with homodyne detection. We observe that below a threshold V_p (that depends on the MIMO configuration), the

SKR is zero since the noise variance due to channel estimation error is too high. In this region, the SKR is limited by the pilot power. As V_p increases the SKR increases, and then above a threshold V_p (that again depends on the MIMO configuration), the SKR saturates. In this regime, the SKR is limited by the channel gain $\hat{T}_i$ that is constant at fixed $d = 20$ m. As before, we observe that the noise due to channel estimation error has a more pronounced effect on the SKR with collective attack as compared to individual attack. Similar to the pilot duration, in practice, the pilot power should be chosen as the minimum value of V_p at which the SKR saturates.

We now numerically study the simplified expressions of the SKRs in (26) and (47) in order to intuitively understand the effect of the noise from channel estimation error $\sigma_{h,i}^2$ on the SKRs. We want to find the maximum tolerable $\sigma_{h,i}^2$ such that positive SKRs can be achieved. Since the SKRs obtained from homodyne and heterodyne detection schemes are almost the same, here we consider only homodyne detection. Using the simplified SKR expressions from (26), (47), a necessary condition for achieving positive SKR on the i-th parallel channel is given by $\zeta_{I/C}^i > \alpha_{I/C}^i$, where I, C denote individual and collective attacks, respectively. The constants $\zeta_{I/C}^i, \alpha_{I/C}^i$ admit

$$\zeta_I^i = \frac{\beta V_s + W - V_a}{\sigma_{\text{det}}^2 + \delta_i} + \frac{V_a W - 1}{V_a \delta_i (1 + \delta_i \sigma_{\text{det}}^2)} , \qquad (48)$$

$$\zeta_C^i = \frac{\beta V_s - 0.5(V_a^2 - 1) \ln\left(\frac{V_a+1}{V_a-1}\right)}{\sigma_{\text{det}}^2 + \delta_i} + \frac{(V_a^2 - 1) \ln\left(\frac{V_a+1}{V_a-1}\right)}{(V_a + \delta_i)}$$
$$- \frac{\sigma_{h,i}^2 (WV_a - 2W^2 + 1) \ln\left(\frac{\delta_i+1}{\delta_i-1}\right)}{\delta_i(V_a + \delta_i)} , \quad (49)$$

(a) Secret Key Rate vs Pilot Duration T_p

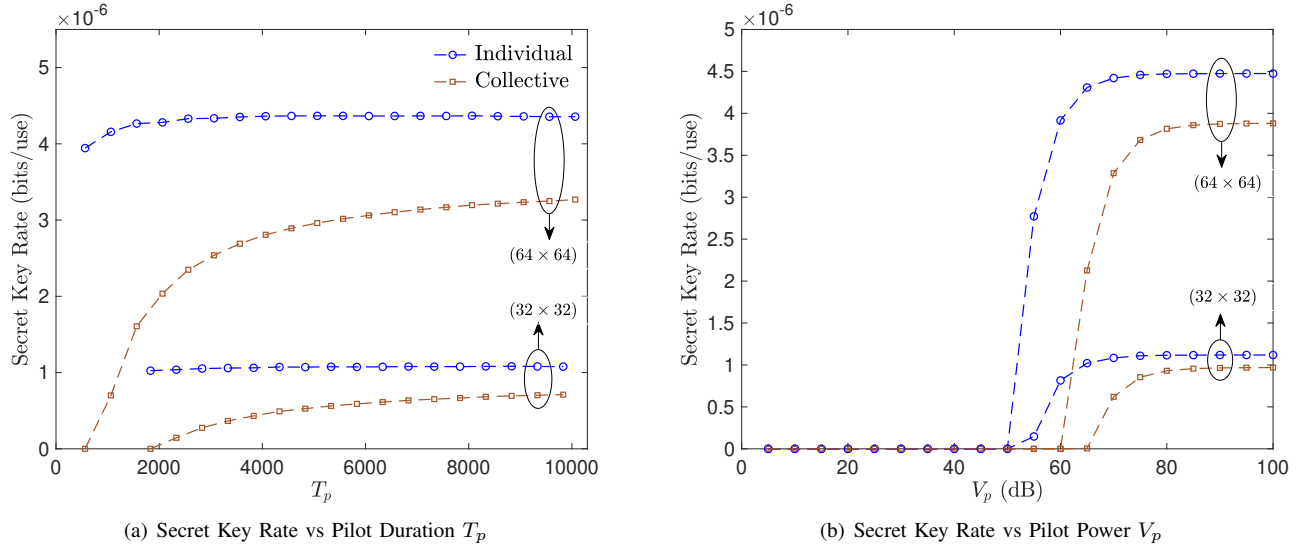(b) Secret Key Rate vs Pilot Power V_p

Fig. 5. The plots show the SKRs (bits/use) as a function of (a) pilot duration T_p, and (b) pilot power V_p for different MIMO architectures ($N_t \times N_r$). Results are shown for a fixed transmission distance of $d = 20$ m at $f_c = 15$ THz with homodyne detection. The rest of the simulation parameters are similar to those used in Fig. 2.

and

$$\alpha_I^i = \frac{\ln\left(\frac{\delta_i(\sigma_{\det}^2 + \delta_i)}{1 + \sigma_{\det}^2 \delta_i}\right)}{\hat{T}_i} , \quad \alpha_C = \frac{h(\delta_i)}{\hat{T}_i} , \quad (50)$$

where

$$\delta_i = \sigma_{h,i}^2 + W . \quad (51)$$

For the simulation scenario considered in Fig. 2 we have a rank-1 MIMO channel which leads to a single parallel channel. Therefore, here we study the effect of $\sigma_{h,i}^2$ on $\zeta_{C/I}^i, \zeta_{C/I}^i$ for $i = 1$ only. Fig. 6 plots $\zeta_{C/I}^1$, $\alpha_{C/I}^1$ from (48)-(50) versus $\sigma_{h,1}^2$ for various MIMO configurations. Results are shown for both the individual attack and collective attack case at a fixed transmission distance of $d = 20$ m. Here we treat $\sigma_{h,1}^2$ as a free variable since we want to study the effect of $\sigma_{h,1}^2$ on the SKR performance. It is easy to verify from (48)-(51) that $\zeta_{I/C}^1$ is independent of the MIMO configuration since it does not depend on $\hat{T}_1$, whereas $\alpha_{I/C}^1$ does depend on the MIMO configuration. From Fig. 6, we observe that $\zeta_{I/C}^1$ does not change much as $\sigma_{h,1}^2$ increases. However, $\alpha_{I/C}^1$ varies significantly as $\sigma_{h,1}^2$ and the MIMO configuration changes. The plots in Fig. 6 reveal that positive SKRs are achievable in the region where the solid line $\left(\zeta_{I/C}^1\right)$ is above the dashed line $\left(\alpha_{I/C}^1\right)$. We observe that there is a threshold noise variance $\sigma_{h,1}^2$ above which positive SKRs are not achievable. Furthermore, we observe that this threshold value of $\sigma_{h,1}^2$ increases as the number of antennas N_r, N_t increases, since the beamforming gain provided by multiple antennas increases, which, in turn, increases the magnitude of the effective channel transmittance $\hat{T}_1$. Hence, the MIMO CVQKD system can tolerate a much larger $\sigma_{h,1}^2$. Comparing the plots of Fig. 6(a) and Fig. 6(b), we observe that the threshold $\sigma_{h,1}^2$ is higher for the individual attack case. Therefore, the MIMO CVQKD system can tolerate a higher noise variance $\sigma_{h,1}^2$ when Eve implements an individual attack.

V. CONCLUSION

We have proposed a channel estimation protocol for a MIMO THz CVQKD scheme. The estimated channel matrix is used for SVD-based transmit-receive beamforming at Alice and Bob. We have characterized the input-output relation between Alice and Bob by incorporating the additional noise arising due to channel estimation error and detector noise. Furthermore, we have analyzed the SKR of the QKD system under two types of attacks that Eve can implement: an individual attack and a collective attack. We have incorporated the finite size effects arising from channel estimation overhead and imperfect information reconciliation in the SKR analysis. We have also derived simplified expansions for the SKRs which are shown to be quite accurate at practical transmission distances. The simplified expressions are used to intuitively understand the effect of different system parameters on the SKR performance of the MIMO CVQKD system. Our simulation results reveal that the SKR of a practical MIMO CVQKD system degrades significantly as compared to the asymptotic SKR upper bound, particularly at large transmission distances. At large transmission distances, the channel transmittance reduces and the additional noise variance due to channel estimation error increases; the combined effect of these two effects degrades the SKR. Furthermore, our simulation results show that the pilot duration T_p and pilot power V_p are important system parameters, since the SKR is zero below a threshold value of T_p, V_p and the SKR saturates above a threshold value of T_p, V_p. Therefore, the SKR results presented in our paper can be used to appropriately choose the values of T_p, V_p such that positive SKRs are achievable in practical THz MIMO CVQKD implementation.

It is to be noted that we proposed a least-squares based channel estimation scheme which requires the pilot length to be at least equal to the number of transmit antennas, i.e., $(T_p \geq N_t)$. Therefore, the pilot duration overhead can

This article has been accepted for publication in IEEE Transactions on Communications. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2022.3161008

12

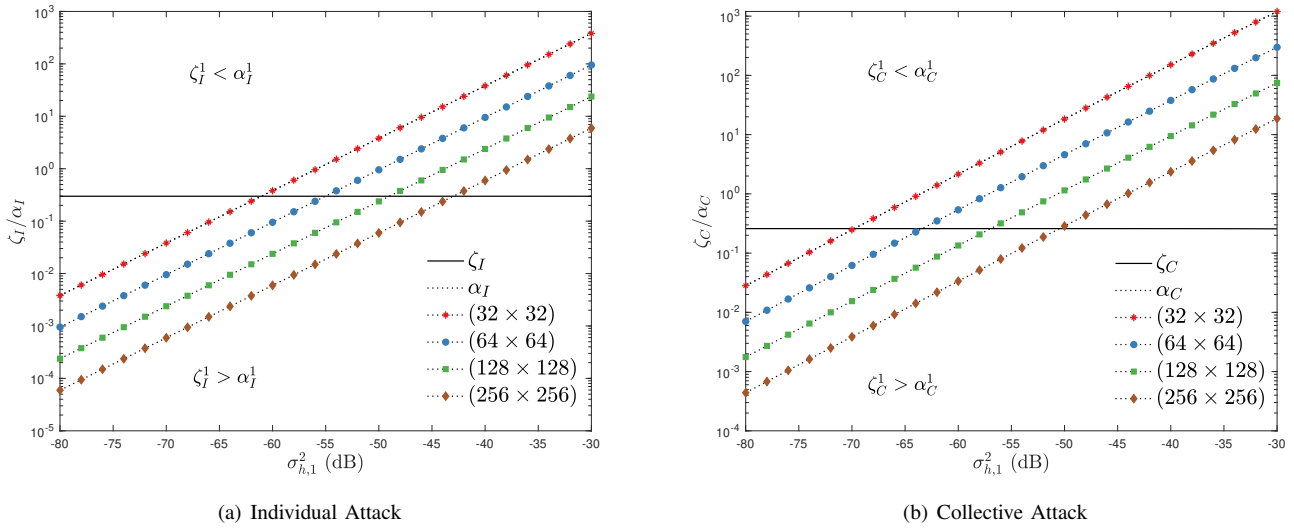(a) Individual Attack

(b) Collective Attack

Fig. 6. The plots show $\zeta_{C/I}^1$, $\alpha_{C/I}^1$ from (48)-(50) versus $\sigma_{h,1}^2$ for various MIMO configurations. Results are shown for both individual and collective attacks at a fixed transmission distance of $d = 20$ m. Positive SKRs are achievable in the region where the solid line $\left(\zeta_{I/C}^1\right)$ is above the dashed line $\left(\alpha_{I/C}^1\right)$. The rest of the simulation parameters are similar to those used in Fig. 2.

be high for large dimensional MIMO systems. The pilot overhead can be reduced and the estimation accuracy can be potentially increased by using compressive sensing based channel estimation schemes, since the THz MIMO channel is generally sparse in the angle domain due to a limited number of scatterers and fewer multi-path components [6], [88]. Therefore, the SKR analysis of the THz MIMO CVQKD system with compressive sensing based channel estimation schemes is an important direction to be studied in future extensions of this work.

We believe that by the time practical quantum computers pose a real threat on the current RSA cryptography algorithms ($\sim 5 - 10$ years) [89], THz signal generation and detection technology will be mature enough to practically realize the proposed MIMO THz CVQKD system. Moreover, by the time 6G communications along with QKD is standardized by 2030 [2], THz CVQKD can also become a potential candidate for wireless QKD in the access network.

References

[1] 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, Aug. 2019.

[2] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?" *Nature Electron.*, vol. 3, no. 1, pp. 20–29, Jan. 2020.

[3] K. David and H. Berndt, "6G vision and requirements: Is there any need for beyond 5G?" *IEEE Veh. Technol. Mag.*, vol. 13, no. 3, pp. 72–80, 2018.

[4] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G networks: Use cases and technologies," *IEEE Commun. Mag.*, vol. 58, no. 3, pp. 55–61, 2020.

[5] T. S. Rappaport, Y. Xing, O. Kanhere, S. Ju, A. Madanayake, S. Mandal, A. Alkhateeb, and G. C. Trichopoulos, "Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond," *IEEE Access*, vol. 7, pp. 78 729–78 757, 2019.

[6] A. Faisal, H. Sarieddeen, H. Dahrouj, T. Y. Al-Naffouri, and M.-S. Alouini, "Ultramassive MIMO systems at terahertz bands: Prospects and challenges," *IEEE Veh. Technol. Mag.*, vol. 15, no. 4, pp. 33–42, 2020.

[7] C. Pan, H. Ren, K. Wang, J. F. Kolb, M. Elkashlan, M. Chen, M. Di Renzo, Y. Hao, J. Wang, A. L. Swindlehurst *et al.*, "Reconfigurable intelligent surfaces for 6G systems: Principles, applications, and research directions," *IEEE Commun. Mag.*, vol. 59, no. 6, pp. 14–20, 2021.

[8] M. Di Renzo, A. Zappone, M. Debbah, M.-S. Alouini, C. Yuen, J. De Rosny, and S. Tretyakov, "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2450–2525, 2020.

[9] C. Huang, S. Hu, G. C. Alexandropoulos, A. Zappone, C. Yuen, R. Zhang, M. Di Renzo, and M. Debbah, "Holographic MIMO surfaces for 6G wireless networks: Opportunities, challenges, and trends," *IEEE Wireless Commun.*, vol. 27, no. 5, pp. 118–125, 2020.

[10] N. K. Kundu and M. R. McKay, "RIS-assisted MISO communication: Optimal beamformers and performance analysis," in *Proc. IEEE Globecom. Workshop. (GC Wkshps)*. IEEE, 2020, pp. 1–6.

[11] ——, "Channel estimation for reconfigurable intelligent surface aided MISO communications: From LMMSE to deep learning solutions," *IEEE Open J. of the Commun. Soc.*, vol. 2, pp. 471–487, 2021.

[12] ——, "Large intelligent surfaces with channel estimation overhead: Achievable rate and optimal configuration," *IEEE Wireless Commun. Lett.*, vol. 10, no. 5, pp. 986–990, 2021.

[13] E. Basar, "Reconfigurable intelligent surface-based index modulation: A new beyond MIMO paradigm for 6G," *IEEE Trans. Commun.*, vol. 68, no. 5, pp. 3187–3196, 2020.

[14] S. D. Tusha, A. Tusha, E. Basar, and H. Arslan, "Multidimensional index modulation for 5G and beyond wireless networks," *Proc. of the IEEE*, vol. 109, no. 2, pp. 170–199, 2020.

[15] C. Zhong, X. Hu, X. Chen, D. W. K. Ng, and Z. Zhang, "Spatial modulation assisted multi-antenna non-orthogonal multiple access," *IEEE Wireless Commun.*, vol. 25, no. 2, pp. 61–67, 2018.

[16] N. K. Kundu, R. K. Mallik, and M. R. McKay, "Signal design for frequency-phase keying," *IEEE Trans. Wireless Commun.*, vol. 19, no. 6, pp. 4067–4079, 2020.

[17] 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, 2020.

[18] I. F. Akyildiz, J. M. Jornet, and C. Han, "Terahertz band: Next frontier for wireless communications," *Phy. Commun.*, vol. 12, pp. 16–32, 2014.

[19] T. Kürner and S. Priebe, "Towards THz communications-status in research, standardization and regulation," *J. of Infrared, Millimeter, and Terahertz Waves*, vol. 35, no. 1, pp. 53–62, 2014.

[20] 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-

This article has been accepted for publication in IEEE Transactions on Communications. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2022.3161008

13

fast networks: A brief survey," *IEEE Netw.*, vol. 33, no. 4, pp. 89–95, Aug. 2019.

[21] 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. (ICC)*. Shanghai, China, May 2019, pp. 1–6.

[22] A. Manzalini, "Quantum communications in future networks and services," *Quantum Rep.*, vol. 2, no. 1, pp. 221–232, Mar. 2020.

[23] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Rev. Mod. Phy.*, vol. 84, no. 2, p. 621, May 2012.

[24] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[25] 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, p. 1261, 2020.

[26] 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. on Commun. Workshop. (ICC Wkshps)*. IEEE, 2021, pp. 1–6.

[27] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: New areas and new challenges," *Digital Commun. and Net.*, vol. 6, no. 3, pp. 281–291, 2020.

[28] C. Wang and A. Rahman, "Quantum-enabled 6G wireless networks: Opportunities and challenges," *TechRxiv*, 2021.

[29] C. H. Bennett and G. Brassard, "An update on quantum cryptography," in *Workshop on the Theory and Application of Cryptographic Techniques*. Springer, 1984, pp. 475–480.

[30] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phy. Rev. Lett.*, vol. 68, no. 21, p. 3121, 1992.

[31] C. H. Bennett and S. J. Wiesner, "Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states," *Phy. Rev. Lett.*, vol. 69, no. 20, p. 2881, 1992.

[32] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phy. Rev. Lett.*, vol. 67, no. 6, p. 661, 1991.

[33] J. D. Franson, "Two-photon interferometry over large distances," *Phy. Rev. A*, vol. 44, no. 7, p. 4552, 1991.

[34] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Phy. Rev. Lett.*, vol. 89, no. 3, p. 037902, 2002.

[35] W. T. Buttler, J. R. Torgerson, and S. K. Lamoreaux, "New, efficient and robust, fiber-based quantum key distribution schemes," *Phy. Lett. A*, vol. 299, no. 1, pp. 38–42, 2002.

[36] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *App. Phy. Lett.*, vol. 87, no. 19, p. 194108, 2005.

[37] T. C. Ralph, "Security of continuous-variable quantum cryptography," *Phy. Rev. A*, vol. 62, no. 6, p. 062306, 2000.

[38] M. Hillery, "Quantum cryptography with squeezed states," *Phy. Rev. A*, vol. 61, no. 2, p. 022309, 2000.

[39] N. J. Cerf, M. Levy, and G. Van Assche, "Quantum distribution of Gaussian keys using squeezed states," *Phys. Rev. A*, vol. 63, no. 5, p. 052311, 2001.

[40] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, no. 5, p. 057902, 2002.

[41] 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, 2003.

[42] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, "Continuous variable quantum cryptography: Beating the 3 dB loss limit," *Phys. Rev. Lett.*, vol. 89, no. 16, p. 167901, 2002.

[43] P. V. Trinh, A. T. Pham, A. Carrasco-Casado, and M. Toyoshima, "Quantum key distribution over FSO: Current development and future perspectives," in *Prog. in Electromagn. Res. Symp. (PIERS-Toyama)*. IEEE, 2018, pp. 1672–1679.

[44] P. V. Trinh, T. V. Pham, N. T. Dang, H. V. Nguyen, S. X. Ng, and A. T. Pham, "Design and security analysis of quantum key distribution protocol over free-space optics using dual-threshold direct-detection receiver," *IEEE Access*, vol. 6, pp. 4159–4175, 2018.

[45] Z. Qu and I. B. Djordjevic, "High-speed free-space optical continuous-variable quantum key distribution enabled by three-dimensional multiplexing," *Opt. Express*, vol. 25, no. 7, pp. 7919–7928, 2017.

[46] C. Erven, C. Couteau, R. Laflamme, and G. Weihs, "Entangled quantum key distribution over two free-space optical links," *Opt. Express*, vol. 16, no. 21, pp. 16 840–16 853, 2008.

[47] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, "Advances in quantum cryptography," *Adv. in Opt. and Photon.*, vol. 12, no. 4, pp. 1012–1236, 2020.

[48] S. Pirandola, "Limits and security of free-space quantum communications," *Phys. Rev. Res.*, vol. 3, no. 1, p. 013279, 2021.

[49] ——, "Satellite quantum communications: Fundamental bounds and practical security," *Phys. Rev. Res.*, vol. 3, no. 2, p. 023130, 2021.

[50] Z. Pan, K. P. Seshadreesan, W. Clark, M. R. Adcock, I. B. Djordjevic, J. H. Shapiro, and S. Guha, "Secret-key distillation across a quantum wiretap channel under restricted eavesdropping," *Phys. Rev. App.*, vol. 14, no. 2, p. 024044, 2020.

[51] Z. Pan and I. B. Djordjevic, "Secret key distillation over satellite-to-satellite free-space optics channel with a limited-sized aperture eavesdropper in the same plane of the legitimate receiver," *Opt. Express*, vol. 28, no. 25, pp. 37 129–37 148, 2020.

[52] ——, "Geometrical optics restricted eavesdropping analysis of satellite-to-satellite secret key distillation," *Entropy*, vol. 23, no. 8, p. 950, 2021.

[53] J. Gariano and I. B. Djordjevic, "Theoretical study of a submarine to submarine quantum key distribution systems," *Opt. Express*, vol. 27, no. 3, pp. 3055–3064, 2019.

[54] J. Gariano, M. Neifeld, and I. Djordjevic, "Engineering trade studies for a quantum key distribution system over a 30 Km free-space maritime channel," *App. Opt.*, vol. 56, no. 3, pp. 543–557, 2017.

[55] J. Gariano and I. B. Djordjevic, "Trade study of aperture size, adaptive optics and multiple spatial modes for a polarization entanglement QKD system over a 30 km maritime channel," *App. Opt.*, vol. 57, no. 28, pp. 8451–8459, 2018.

[56] C. Ottaviani, M. J. Woolley, M. Erementchouk, J. F. Federici, P. Mazumder, S. Pirandola, and C. Weedbrook, "Terahertz quantum cryptography," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 483–495, Mar. 2020.

[57] D. Zavitsanos, A. Ntanos, G. Giannoulis, and H. Avramopoulos, "On the QKD integration in converged fiber/wireless topologies for secured, low-latency 5G/B5G fronthaul," *Appl. Sci.*, vol. 10, no. 15, p. 5193, Jul. 2020.

[58] 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.

[59] 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. of the Commun. Soc.*, vol. 1, pp. 1–32, 2019.

[60] 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.

[61] Y. He, Y. Mao, D. Huang, Q. Liao, and Y. Guo, "Indoor channel modeling for continuous variable quantum key distribution in the terahertz band," *Optics Exp.*, vol. 28, no. 22, pp. 32 386–32 402, Oct. 2020.

[62] 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, pp. 1–13, 2021.

[63] Z. Wang, R. Malaney, and J. Green, "Inter-satellite quantum key distribution at terahertz frequencies," in *Proc. IEEE Int. Conf. Commun. (ICC)*. Shanghai, China, May 2019, pp. 1–7.

[64] S. Ummethala, T. Harter, K. Koehnle, Z. Li, S. Muehlbrandt, Y. Kutuvantavida, J. Kemal, P. Marin-Palomo, J. Schaefer, A. Tessmann *et al.*, "THz-to-optical conversion in wireless communications using an ultra-broadband plasmonic modulator," *Nature Photon.*, vol. 13, no. 8, pp. 519–524, 2019.

[65] I. Ilyakov, B. Shishkin, V. Malevich, D. Ponomarev, R. Galiev, A. Y. Pavlov, A. Yachmenev, S. Kovalev, M. Chen, R. Akhmedzhanov *et al.*, "Efficient optical-to-terahertz conversion in large-area ingaas photodember emitters with increased indium content," *Opt. Lett.*, vol. 46, no. 14, pp. 3360–3363, 2021.

[66] S. Ummethala, T. Harter, K. Köhnle, S. Muehlbrandt, Y. Kutuvantavida, J. Kemal, J. Schaefer, H. Massler, A. Tessmann, S. Garlapati *et al.*, "Terahertz-to-optical conversion using a plasmonic modulator," in *Proc. IEEE Conf. on Lasers and Electro-Opt. (CLEO)*. San Jose, CA, USA, May 2018, pp. 1–2.

[67] M. Bakunov, E. Efimenko, S. Gorelov, N. Abramovsky, and S. Bodrov, "Efficient Cherenkov-type optical-to-terahertz converter with terahertz beam combining," *Opt. Lett.*, vol. 45, no. 13, pp. 3533–3536, 2020.

[68] D. Turan, P. K. Lu, N. T. Yardimci, Z. Liu, L. Luo, J.-M. Park, U. Nandi, J. Wang, S. Preu, and M. Jarrahi, "Wavelength conversion through plasmon-coupled surface states," *Nature Commun.*, vol. 12, no. 1, pp. 1–8, 2021.

[69] D. Jang, J. H. Sung, S. K. Lee, C. Kang, and K.-Y. Kim, "Generation of 0.7 mj multicycle 15 thz radiation by phase-matched optical rectification in lithium niobate," *Opt. Lett.*, vol. 45, no. 13, pp. 3617–3620, 2020.

[70] T. Seifert, S. Jaiswal, U. Martens, J. Hannegan, L. Braun, P. Maldonado, F. Freimuth, A. Kronenberg, J. Henrizi, I. Radu *et al.*, "Efficient metallic spintronic emitters of ultrabroadband terahertz radiation," *Nature Photon.*, vol. 10, no. 7, pp. 483–488, 2016.

[71] U. Nandi, M. Abdelaziz, S. Jaiswal, G. Jakob, O. Gueckstock, S. M. Rouzegar, T. Seifert, M. Kläui, T. Kampfrath, and S. Preu, "Antenna-coupled spintronic terahertz emitters driven by a 1550 nm femtosecond laser oscillator," *Appl. Phys. Lett.*, vol. 115, no. 2, p. 022405, 2019.

[72] Y.-J. Lin and M. Jarrahi, "Heterodyne terahertz detection through electronic and optoelectronic mixers," *Rep. on Prog. in Phys.*, vol. 83, no. 6, p. 066101, 2020.

[73] K. Ikamas, D. B. But, and A. Lisauskas, "Homodyne spectroscopy with broadband terahertz power detector based on 90-nm silicon CMOS transistor," *App. Sci.*, vol. 11, no. 1, p. 412, 2021.

[74] C. W. Berry, N. Wang, M. R. Hashemi, M. Unlu, and M. Jarrahi, "Significant performance enhancement in photoconductive terahertz optoelectronics by incorporating plasmonic contact electrodes," *Nature Commun.*, vol. 4, no. 1, pp. 1–10, 2013.

[75] H. Deng and A. Sayeed, "Mm-wave MIMO channel modeling and user localization using sparse beamspace signatures," in *Proc. IEEE 15th Int. Wkshp. on Signal Process. Adv. in Wireless Commun. (SPAWC)*. Toronto, ON, Canada, Jun. 2014, pp. 130–134.

[76] S. Sun, T. S. Rappaport, M. Shafi, P. Tang, J. Zhang, and P. J. Smith, "Propagation models and performance evaluation for 5G millimeter-wave bands," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8422–8439, Sep. 2018.

[77] I. B. Djordjevic, *Physical-Layer Security and Quantum Key Distribution*. Springer, 2019.

[78] M. R. McKay and I. B. Collings, "General capacity bounds for spatially correlated Rician MIMO channels," *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3121–3145, 2005.

[79] J. H. Manton, "Optimal training sequences and pilot tones for OFDM systems," *IEEE Commun. Lett.*, vol. 5, no. 4, pp. 151–153, 2001.

[80] M. Biguesh and A. B. Gershman, "Training-based MIMO channel estimation: A study of estimator tradeoffs and optimal training signals," *IEEE Trans. on Signal Process.*, vol. 54, no. 3, pp. 884–893, 2006.

[81] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, "Quantum cryptography approaching the classical limit," *Phy. Rev. Lett.*, vol. 105, no. 11, p. 110501, Sep. 2010.

[82] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin *et al.*, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Phy. Rev. A*, vol. 76, no. 4, p. 042305, 2007.

[83] F. Grosshans and N. J. Cerf, "Continuous-variable quantum cryptography is secure against non-Gaussian attacks," *Physical Rev. Lett.*, vol. 92, no. 4, p. 047905, 2004.

[84] I. B. Djordjevic, *Physical-Layer Security and Quantum Key Distribution*. Springer, 2019.

[85] K. Rikkinen, P. Kyosti, M. E. Leinonen, M. Berg, and A. Parssinen, "THz radio communication: Link budget analysis toward 6G," *IEEE Commun. Mag.*, vol. 58, no. 11, pp. 22–27, Nov. 2020.

[86] S. U. Hwu, K. B. deSilva, and C. T. Jih, "Terahertz (THz) wireless systems for space applications," in *Proc. IEEE Sensors Appl. Symp.* Galveston, TX, USA, Feb. 2013, pp. 171–175.

[87] K. Tsujimura, K. Umebayashi, J. Kokkoniemi, J. Lehtomäki, and Y. Suzuki, "A causal channel model for the terahertz band," *IEEE Trans. on Terahertz Sc. and Technol.*, vol. 8, no. 1, pp. 52–62, 2017.

[88] H. Sarieddeen, M.-S. Alouini, and T. Y. Al-Naffouri, "An overview of signal processing techniques for terahertz communications," *Proc. of the IEEE*, pp. 1–38, 2021.

[89] M. Dyakonov, "When will useful quantum computers be constructed? Not in the foreseeable future, this physicist argues. Here's why: The case against: Quantum computing," *IEEE Spectrum*, vol. 56, no. 3, pp. 24–29, 2019.

Neel Kanth Kundu (S'19) received the B.Tech. degree in electrical engineering with specialization in communication systems and networking from the Indian Institute of Technology Delhi, New Delhi, India, in 2018. He is currently working toward the Ph.D. degree with the Department of Electronic and Computer Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Hong Kong.

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.

Mr. Kundu is the recipient of the Hong Kong Ph.D. Fellowship and the Overseas Research Award.

Soumya P. Dash (S'16–M'19) received the B.Tech. (H) degree in electrical engineering from the Indian Institute of Technology, Bhubaneswar, in 2014 and the Ph.D. degree in electrical engineering from the Indian Institute of Technology, Delhi, in 2019. From January 2019 to March 2019, he was an Early-Doctoral Research Fellow with the Department of Electrical Engineering, Indian Institute of Technology, Delhi. Since March 2019, he has been with the faculty of the School of Electrical Sciences, Indian Institute of Technology, Bhubaneswar, where he is currently an Assistant Professor. His research interests include communication theory for hybrid communication systems, power line communications, smart grid communications, next-generation wireless communication systems, and diversity combining.

He is a Member of the IEEE Communications and Vehicular Technology Societies. He was the recipient of the VDGOOD Young Scientist Award and the President of India Gold Medal for the academic year 2013-14 for obtaining highest CGPA amongst the students graduating with B.Tech. (H) degree from the Indian Institute of Technology Bhubaneswar.

Matthew R. McKay (S'03-M'07-SM'13-F'21) received the Ph.D. degree in Electrical Engineering from the University of Sydney, Australia. He is currently Professor in the Department of Electrical and Electronic Engineering at the University of Melbourne, and also as a Professorial Fellow (Honorary) in the Department of Microbiology and Immunology. Matthew has been awarded a Future Fellowship of the Australian Research Council. Prior to joining the University of Melbourne, Matthew was a Professor in the Department of Electronic and Computer Engineering at the Hong Kong University of Science and Technology (HKUST), and also in the Department of Chemical and Biological Engineering. He currently holds and Adjunct Professor title at HKUST. He was a Research Scientist with the Institute for Medical Engineering & Science (IMES) at the Massachusetts Institute of Technology in 2014, and with the Department of Statistics at Stanford University in 2015.

Matthew and his co-authors were awarded best paper awards at multiple conferences (ICASSP, ICC, Globecom, etc). He received a 2010 Young Author Best Paper Award by the IEEE Signal Processing Society, and the 2011 Stephen O. Rice Prize by the IEEE Communication Society. He has served as the Area Editor of Feature Articles for the IEEE SIGNAL PROCESSING MAGAZINE, and also on the editorial boards of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and 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. In 2021, he was awarded the Australia-China Alumni Award for Research and Science by the Australia-China Alumni Association. He is a Fellow of the IEEE.

Ranjan K. Mallik (S'88–M'93–SM'02–F'12) received the B.Tech. degree from the Indian Institute of Technology Kanpur, Kanpur, in 1987 and the M.S. and Ph.D. degrees from the University of Southern California, Los Angeles, 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. 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. Since December 1998, he has been with the faculty of the Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi, where he is currently a 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 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, and The Institution of Engineers (India); 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, and the J. C. Bose Fellowship. He has served as an Area Editor and an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, and as an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS.