Hybrid Beamforming Assisted OTFS-Based CV-QKD Systems for Doubly Selective THz Channels

Xin Liu, *Graduate Student Member, IEEE*, Chao Xu, *Senior Member, IEEE*, Stephen Wang, *Senior Member, IEEE*, Soon Xin Ng, *Senior Member, IEEE*, and Lajos Hanzo, *Life Fellow, IEEE*

***Abstract*—Continuous-variable quantum key distribution (CV-QKD) maps information onto the quadrature components of electromagnetic waves, so that off-the-shelf wireless transceivers can be utilized. This motivates the move from optical to Terahertz (THz) bands. However, wireless THz channels suffer from severe path loss, while the mobility of wireless users imposes doubly selective fading. Against this background, we propose a new CV-QKD regime that relies on hybrid beamforming (HBF) assisted multiple-input multiple-output (MIMO) orthogonal frequency division multiplexing (OFDM) and orthogonal time frequency space (OTFS) system, where the channel's transmissivity and robustness against double selectivity are overcome by HBF and OTFS, respectively. Secondly, in order to provide channel state information (CSI) for both the transmitter (CSI-T) and receiver (CSI-R), practical channel estimation methods are conceived. They operate in the time-frequency domain for OFDM and in the delay-Doppler domain for OTFS. Thirdly, soft-decision detection is devised for our MIMO OFDM/OTFS aided multi-dimensional reconciliation (MDR) scheme. Low-density parity-check (LDPC) coding is invoked for further improving secure CV-QKD transmission distance in the THz band. Our simulation results demonstrate that the proposed HBF MIMO OTFS-based CV-QKD system relying on realistic estimated CSI is capable of achieving an adequate secret key rate (SKR) and secure transmission distance in hostile doubly selective THz channels.**

***Index Terms*—Orthogonal frequency division multiplexing (OFDM), orthogonal time frequency space (OTFS), low-density parity check (LDPC), continuous variable quantum key distribution (CV-QKD), multiple-input multiple-out (MIMO), hybrid beamforming (HBF), Terahertz (THz), secret key rate (SKR).**

I. Introduction

Quantum key distribution (QKD) is capable of supporting ultimate information security in communication systems [1]–[7] thanks to the capability of eavesdropping detection based on the no-cloning theorem and Heisenberg's uncertainty principle. Continuous variable QKD (CV-QKD), leveraging either homodyne or heterodyne detection, has attracted substantial attention from both academia and industry due to its convenient compatibility with the operational optical and wireless network infrastructures [2], [8]. It is also capable of providing higher key rate than its discrete variable QKD (DV-QKD) based counterpart [9]–[12] Furthermore, to meet the explosive data-rate demand of next-generation communication systems, the Terahertz (THz) band has also been explored for CV-QKD [13]–[18]. As a further advance, multiple-input multiple-output (MIMO) techniques have been adopted in [19]–[22] for improving the secure transmission distance limited by the high path loss of the THz band. Furthermore, the classic orthogonal frequency division multiplexing (OFDM) waveform used in both 4G and 5G, has been utilized to support CV-QKD in the THz band in order to mitigate the detrimental multipath effect of wireless channels [23]–[32].

Table I summarizes the state-of-the-art of CV-QKD schemes, with a emphasis on harnessing OFDM to improve the secret key rate (SKR) in wireless THz channels. An OFDM-based CV-QKD scheme was proposed for a benign optical fibre channel and both its security level and the SKR were investigated in [23]–[27], [29], [31]. It was demonstrated that OFDM enhances both the maximum key rate at a given distance and the overall maximum secure transmission distance. Furthermore, an OFDM-based CV-QKD free-space optical (FSO) link was established in [28], [32], where its SKR was analysed. Additionally, the authors of [30] analyzed the SKR performance of an OFDM-based CV-QKD scheme operating in the THz band, considering both indoor environments and inter-satellite links. However, all these OFDM-aided CV-QKD schemes assume time-invariant fading channels in stationary scenarios, which is unrealistic. In practice, the user mobility induces Doppler effects, leading to time-varying frequency-selective fading channels, which is a typical high mobility scenario in space-air-ground integrated networks (SAGIN) [2]–[4], [33]. More specifically, the higher the mobility in the SAGIN scenarios, the more dominant the effect of Doppler spread, which will cause hostile doubly selective fading. This hostile channel destroys OFDM's subcarrier orthogonality and degrades its performance. To address this issue, orthogonal time frequency space (OTFS) modulation has been proposed for classical wireless communication in time-varying and frequency selective fading channels [33]–[41]. In light of this, an analog beamforming (ABF) MIMO OFDM/OTFS based and low-density parity-check (LDPC) coding assisted multidimensional reconciliation (MDR) CV-QKD system was conceived in [42] for transmission over doubly selective fading THz channels. It was demonstrated [42] that the OTFS-based system offers higher SKR and longer secure transmission distance than its OFDM-based counterpart in both stationary and mobile ($v = 30$ mph) scenarios.

Against this background, the following key questions arise

L. Hanzo would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council (EPSRC) projects under grant EP/Y037243/1, EP/W016605/1, EP/X01228X/1, EP/Y026721/1, EP/W032635/1, EP/Y037243/1 and EP/X04047X/1 as well as of the European Research Council's Advanced Fellow Grant QuantCom (Grant No. 789028).

TABLE I: Novel contributions of this work in comparison to the state-of-the-art THZ CV-QKD schemes.

Contributions	**This work**	[23]–[27], [29], [31]	[30]	[28], [32]	[15], [17]	[19]	[22]	[42]
Optical fibre		✓						
FSO				✓				
Terahertz	✓		✓		✓	✓	✓	✓
SISO	✓	✓	✓	✓	✓		✓	✓
MIMO	✓					✓	✓	✓
Analog beamforming	✓					✓	✓	✓
Frequency selective	✓	✓	✓	✓				✓
Time-invariant fading	✓	✓	✓	✓	✓	✓	✓	✓
Time-varying fading	✓							✓
OFDM	✓	✓	✓	✓				✓
OTFS	✓							✓
SVD	✓							
Channel estimation	✓							

for the multi-carrier based CV-QKD system design consider in the face of time-varying and frequency selective fading scenarios:

- ***(Q-1)*** ***System modeling:*** How to design the reconciliation scheme of a CV-QKD system facing doubly selective fading?
- ***(Q-2)*** ***Channel Estimation:*** How can we incorporate channel estimation techniques into the CV-QKD system considered?
- ***(Q-3)*** ***Reconciliation:*** How can we embed an LDPC-coded reconciliation scheme into a QKD system?

Against this background, as a further improvement of the ABF-assisted MIMO OFDM/OTFS CV-QKS system, hybrid beamforming (HBF) is proposed, which requires that full channel state information (CSI) is provided at both the transmitter (CSI-T) and the receiver (CSI-R). In light of this, a variety of channel estimation methods are conceived for MIMO OFDM/OTFS in order to provide CSI-T and CSI-R for HBF. As demonstrated by Table I, the novel contributions of this work are as follows:

- Firstly, in answer to ***(Q-1)*** multi-carrier OFDM and OTFS based LDPC assisted CV-QKD reconciliation schemes are designed and investigated in time-varying and frequency-selective THz fading channels, where a new HBF technique is conceived for improving the OFDM/OTFS based quantum transmission distance attained in the face of severe THz path loss.
- Secondly, with regard to ***(Q-2)*** MIMO-aided OFDM and OTFS channel estimation techniques have been conceived for both the time-frequency (TF) domain and for the delay-Doppler (DD) domain. It is demonstrated that under the idealistic simplifying conditions of perfect CSI, the beamforming gain provided by sufficiently large number of antennas allows OFDM and OTFS perform comparably, even in doubly selective fading environments. However, the OFDM-based system relying on realistic channel estimation only performs adequately in stationary scenarios, since it suffers from a high error-floor in mobile scenarios. By contrast, our proposed OTFS-based system is capable of performing well in both stationary and mobile scenarios.
- Finally, as to ***(Q-3)*** based on OFDM and OTFS modulation, soft-decision detection is devised for CV-QKD MDR and then LDPC decoding is invoked for further improving the secure CV-QKD THz transmission distance. Our analysis and simulation results demonstrate that the proposed HBF scheme is capable of improving secure CV-QKD transmission for both OTFS and OFDM in comparison to the existing ABF schemes. Furthermore, our performance results also evidence that the proposed HBF MIMO OTFS-based CV-QKD system relying on realistic estimated CSI is capable of outperforming its OFDM counterpart both in terms of SKR and secure transmission distance.

The rest of this paper is structured as follows. Our OFDM/OTFS CV-QKD system is presented in Section II, which introduces the CV-QKD system model, the OFDM and the OTFS quantum transmission. Then in Section III, the HBF MIMO OFDM/OTFS CV-QKD system is conceived as well as our improved soft-decision aided MDR decoding conceived for doubly selective THz channels and the relevant complexity analysis is detailed. The MIMO OFDM/OTFS channel estimation algorithms of our CV-QKD system are proposed in Section IV, which is followed by the SKR analysis in Section V. Our simulation results are presented in Section VI. Finally, our conclusions are offered in Section VII.

Notations: In this paper, bold uppercase $\mathbf{A}$ and lowercase $\mathbf{a}$ denote matrices and vectors, respectively. For a matrix $\mathbf{A}$, $\mathbf{A}[m,:]$ and $\mathbf{A}[:,n]$ represent its mth row and the nth column, while $\mathbf{A}[m,n]$ represents the element at the mth row and nth column. For a vector $\mathbf{a}$, $\mathbf{a}[m]$ represents its mth element. The operation $(\cdot)^*$ denotes the complex conjugate of a scalar or a vector. The operations $(\cdot)^{-1}$, $(\cdot)^T$ and $(\cdot)^H$ represent the matrix inverse, transpose and Hermitian transpose, respectively. $\|\cdot\|$ denotes the Frobenius norm. The functions $\mathfrak{Re}(\cdot)$ and $\mathfrak{Im}(\cdot)$ extract the real and imaginary part of a complex value, respectively. Additionally, $\mathrm{diag}\,(\mathbf{a})$ forms a square diagonal matrix from vector $\mathbf{a}$, and $\mathrm{rem}(a,b)$ returns the remainder of a divided by b.

II. System model of MIMO OFDM/OTFS Based CV-QKD

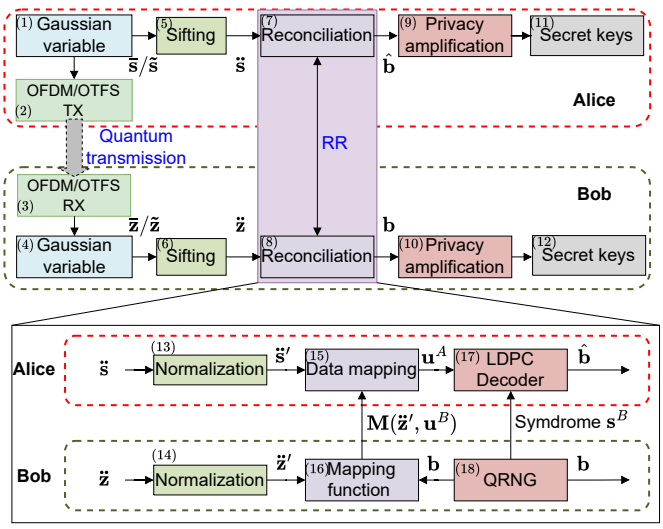


Fig. 1: CV-QKD protocol diagram of OFDM/OTFS LDPC-aided scheme [42], where the quantum transmission process is indicated by the dashed-line thick arrow, while the solid-line thin arrows represent the classical transmission process. The detailed reconciliation procedures can be found in [43].

In this section, the CV-QKD system model and the single-input single-output (SISO) OFDM/OTFS based quantum transmission process are briefly introduced [42].

A. CV-QKD System Model

The classic CV-QKD protocol [43] is portrayed in Fig. 1, which mainly contains the quantum transmission part relying on homodyne detection, and the classical reverse reconciliation (RR) process. Note that the simple symdrome-based RR scheme (System A) of [43] is considered in order to focus our discussions on the OFDM/OTFS quantum transmission. However, the other reconciliation schemes of [43] are also applicable to our proposed multi-carrier based CV-QKD system. More explicitly, the operational steps of Fig. 1 are detailed as follows:

(a) Alice prepares the Gaussian distributed random variables $\bar{\mathbf{s}}/\widetilde{\mathbf{s}}$ of block (1) and maps them to subcarriers. Then transmits them with the aid of the OFDM/OTFS TX of block (2) through wireless THz quantum channels (QuCs)[1], which is denoted by the dashed-line thick arrow in Fig. 1.

(b) Bob equalizes the received signals based on the OFDM/OTFS RX of block (3) for obtaining the noise-contaminated decision variables $\bar{\mathbf{z}}/\widetilde{\mathbf{z}}$ at the output of block (4).

[1]It is widely acknowledged that particle-like behaviour of photons is gradually eroded in the THz radio-frequency (RF) band, where predominantly wave-like behaviour prevails [18]. However, sufficient non-zero SKR was still heralded in [18]. Hence a RF THz channel is considered in our treatise. Furthermore, homodyne THz detectors [17], [18] are assumed to be used directly in our scenario, which is different from the THz-to-optical converter based homodyne detection of [15].

TABLE II: OFDM and OTFS notations.

	TD	FD	DD domain
Transmitter	$s_{n,m}$	$\bar{s}_{n,\overline{m}}$	$\widetilde{s}_{k,l}$
Channel	$h_{n,m,l}$	$\bar{h}_{n,\overline{m}}$	$\widetilde{h}_p\omega_{MN}^{k_p(nM+m-l_p)}$
Receiver	$y_{n,m}$	$\bar{y}_{n,\overline{m}}$	$\widetilde{y}_{k,l}$

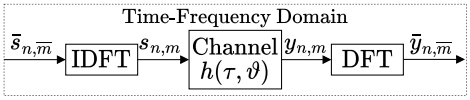


Fig. 2: System diagram of OFDM transmission scheme.

(c) In the sifting step, Alice and Bob synchronize their bases[2] in blocks (5) and (6) for MDR processing. Hence they only retain those reconstructed Gaussian variables, where the same bases were used.

(d) In the RR step, Bob first generates a random bit stream $\mathbf{b}$ based on the quantum random number generator (QRNG) of block (18). Then it maps the modulated binary data $\mathbf{u}^B$ to the normalized random variables $\ddot{\mathbf{z}}'$, seen at the output of block (14) based on the mapping function $\mathbf{M}(\ddot{\mathbf{z}}', \mathbf{u}^B)$ agreed by both Alice and Bob as seen at the output of block (16).

(e) Alice applies the agreed MDR function $\mathbf{M}(\ddot{\mathbf{z}}', \mathbf{u}^B)$ in block (15) for obtaining a noisy version $\mathbf{u}^A$ of Bob's modulated data based on the output $\ddot{\mathbf{s}}'$ from block (13) combined with the output $\mathbf{M}(\ddot{\mathbf{z}}', \mathbf{u}^B)$ of block (16).

(f) Then the LDPC syndrome $\mathbf{s}^B$ generated based on the key $\mathbf{b}$, is sent from Bob to Alice over the classical channel (ClC) for LDPC decoding in block (17) in order to obtain the reconciled binary key $\hat{\mathbf{b}}$.

(g) Then the privacy amplification of blocks (9) and (10) randomly drop some of the reconciled bits to reduce Eve's chances of perfectly guessing the key. After privacy amplification, both Alice and Bob obtain the negotiated keys, which are stored in blocks (11) and (12).

B. OFDM/OTFS based Quantum Transmission

In this section, the OFDM scheme of Fig. 2 and the OTFS scheme of Fig. 3 are briefly introduced for quantum transmission over wireless THz channels [42]. The OFDM and OTFS notations in the time-domain (TD), frequency-domain (FD) and DD domain are summarized in Table II.

1) OFDM based quantum transmission: As portrayed by Fig. 2, the OFDM transmitter maps the data-carrying symbols to the nth OFDM symbol in FD as $\bar{\mathbf{s}}_n \in \mathcal{C}^{M\times 1}$, and then they are transformed to the TD as $\mathbf{s}_n \in \mathcal{C}^{M\times 1}$ via the inverse discrete Fourier transform (IDFT). The received TD signal can be expressed as [42]:

$$y_{n,m} = \sqrt{T}\sum_{l=0}^{L-1} h_{n,m,l}\left(s_{n,<m-l>_M} + s_{0n,<m-l>_M}\right) + \sqrt{1-T}s_{En,m}, \tag{1}$$

[2]Note that homodyne detection is used in our proposed scheme, where either the in-phase or quadrature components is retained based on the bases they agreed.

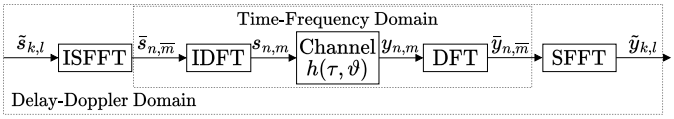


Fig. 3: System diagram of OTFS transmission scheme.

where T represents the channel transmissivity, $h_{n,m,l}$ models the faded channel impulse response (CIR) from the lth time delay line (TDL) tap, with L representing the maximum TDL tap, and s_{0n} and s_E represent the preparation thermal noise and the additive white Gaussian noise (AWGN) introduced by Eve to extract the key information [19], respectively. The received TD signal can be denoted as $\mathbf{y}_n = [y_{n,0}, y_{n,1}, \ldots, y_{n,M-1}]^T$ in matrix form and is transformed into the FD by discrete Fourier transform (DFT) as follows:

$$\overline{\mathbf{y}}_n = \mathbf{F}_M \mathbf{y}_n = \sqrt{T}\overline{\mathbf{H}}_n \bar{\mathbf{s}}_n + \overline{\mathbf{v}}_n, \tag{2}$$

where $\mathbf{F}_M \in \mathcal{C}^{M\times M}$ denotes the DFT matrix. Furthermore, $\overline{\mathbf{H}}_n$ represents the faded CIR in FD and can be expressed as $\overline{\mathbf{H}}_n = \mathbf{F}_M \mathbf{H}_n \mathbf{F}_M^H$, and $\overline{\mathbf{v}}_n = \sqrt{T}\overline{\mathbf{H}}_n \bar{\mathbf{s}}_{0n} + \sqrt{1-T}\bar{\mathbf{s}}_{En}$.

2) OTFS based quantum transmission: As portrayed by Fig. 3, the OTFS transmitter modulates a total number of NM symbols in the DD domain as $\left\{\{\widetilde{s}_{k,l}\}_{k=0}^{N-1}\right\}_{l=0}^{M-1}$, which is transformed into the FD as $\overline{s}_{n,\overline{m}}$ via the inverse symplectic finite Fourier transform (ISFFT), where n, $\overline{m}$, k and l refer to the symbol index, sample index, Doppler index and delay index, respectively. Then, an IDFT operation is applied to the FD signal $\overline{s}_{n,\overline{m}}$, hence the TD signal is generated as $s_{n,m}$. Accordingly, the received TD signal can be expressed as [42]

$$y_{n,m} = \sqrt{T}\sum_{p=0}^{P-1} \widetilde{h}_p \omega_{MN}^{k_p[n(M+M_{cp})+m-l_p]} s_{n,<m-l_p>_M} + v_{n,m}, \tag{3}$$

where we have $v_{n,m} = \sqrt{T}\sum_{p=0}^{P-1} \widetilde{h}_p \omega_{MN}^{k_p[n(M+M_{cp})+m-l_p]} \cdot s_{0,n,<m-l_p>_M} + \sqrt{1-T}s_{E_{n,m}}$ and $\omega_{MN}^{k_p[n(M+M_{cp})+m-l_p]} = \exp\{j\left[(2\pi k_p[n(M+M_{cp})+m-l_p])/(MN)\right]\}$. Upon comparing Eq. (1) and Eq. (3), we can see that a total number of P paths fall into L resolvable TDLs, i.e. $P = \sum_{l=0}^{L-1} P_l$, and there are P_l paths in the lth TDL tap given that each path has different Doppler spread. Furthermore, $\widetilde{h}_p$ and M_{cp} represent the fading gain and the length of the cyclic prefix (CP), respectively. To elaborate further, Fig. 4 demonstrates the relationship between the paths and the TDLs, given that $L = 4$. As seen from Fig. 4, there are 5 paths in total, with one path $\tilde{h}_0$ falling into the 0th TDL, two paths $\tilde{h}_1, \tilde{h}_2$ falling into the 1st TDL with different Doppler indices, and another two paths $\tilde{h}_3, \tilde{h}_4$ falling into the 3rd TDL with different Doppler indices. Following this, the received FD signal $\overline{y}_{n,\overline{m}}$ is obtained by the DFT, and thereafter the DD domain signal $\widetilde{y}_{k,l}$ can be generated by using the symplectic finite Fourier transform (SFFT) operation on $\overline{y}_{n,\overline{m}}$.

In summary, the input-output relationship of OTFS with a single CP added to the entire frame can be expressed in the following matrix form:

$$\widetilde{\mathbf{y}} = \sqrt{T}\widetilde{\mathbf{H}}\widetilde{\mathbf{s}} + \widetilde{\mathbf{v}}, \tag{4}$$

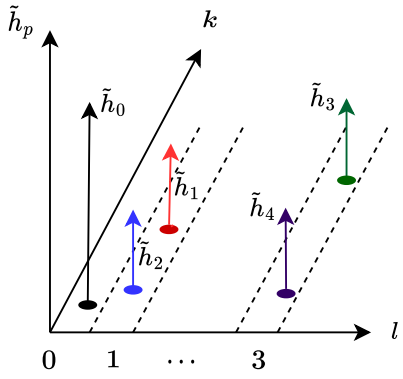


Fig. 4: The illustration of the relationship between the paths and TDLs, where $L = 4$, $P_0 = 1$, $P_1 = 2$, $P_2 = 0$, $P_3 = 2$.

where $\widetilde{\mathbf{y}} \in \mathcal{C}^{MN\times 1}$ and the κth element of $\widetilde{\mathbf{y}}$ is given by $\widetilde{\mathbf{y}}[\kappa] = \widetilde{y}_{k,l}$, where $k = \lfloor \frac{\kappa}{M} \rfloor$, $l = \kappa - kM$. Similarly, the κth elements of $\widetilde{\mathbf{s}} \in \mathcal{C}^{MN\times 1}$ and of $\widetilde{\mathbf{v}} \in \mathcal{C}^{MN\times 1}$ are given by $\widetilde{\mathbf{s}}[\kappa] = \widetilde{s}_{k,l}$, and $\widetilde{\mathbf{v}}[\kappa] = \widetilde{v}_{k,l}$, respectively, where $\widetilde{\mathbf{v}} = \sqrt{T}\widetilde{\mathbf{H}}\widetilde{\mathbf{s}}_0 + \sqrt{1-T}\widetilde{\mathbf{s}}_E$. Moreover, the DD domain fading matrix $\widetilde{\mathbf{H}} \in \mathcal{C}^{MN\times MN}$ is time-invariant and sparse, where the non-zero elements are given by $\widetilde{\mathbf{H}}_{\kappa,\iota} = \widetilde{h}_p \widetilde{T}(k,l,k_p,l_p)$, with $\widetilde{T}(\cdot)$ representing the DD index-based phase rotations [44].

III. Proposed Hybrid Beamforming-based MIMO OFDM/OTFS MDR-assisted CV-QKD

Instead of the ABF applied in [42], HBF is proposed in this paper, which requires that full CSI is provided, in order to improve the performances. Therefore, in this section, both the HBF-based MIMO OFDM and MIMO OTFS systems operating in doubly selective THz channels are proposed, which are followed by the proposed MDR decoding and complexity analysis of our MIMO OFDM/OTFS CV-QKD systems.

A. MIMO OFDM in Doubly Selective THz Channels using Hybrid Beamforming

For a MIMO THz scheme using N_{Tx} transmit antennas (TAs) and N_{Rx} receive antennas (RAs), the TD fading matrix is modelled by [33], [45]:

$$\mathbf{H}_{n,m,l} = \sqrt{N_{Tx}N_{Rx}} \cdot \sum_{p=0}^{P_l-1} \widetilde{h}_p \omega_{MN}^{k_p(nM+m-l_p)} \mathbf{a}_{Rx}(\theta_{Rx,p})\mathbf{a}_{Tx}^H(\theta_{Tx,p}), \quad l_p = l \tag{5}$$

where there are P_l paths falling into the lth TDL with the same delay, i.e. $l_p = l$, but different Doppler k_p. We use uniform linear arrays (ULAs) at both the transmitter and the receiver, where the antenna response vectors are given by:

$$\mathbf{a}_{Tx}(\theta_{Tx,p}) = \frac{1}{\sqrt{N_{Tx}}}\Big[1, e^{j\frac{2\pi d\sin(\theta_{Tx,p})}{\lambda}}, e^{j2\frac{2\pi d\sin(\theta_{Tx,p})}{\lambda}}, \cdots, e^{j\frac{(N_{Tx}-1)2\pi d\sin(\theta_{Tx,p})}{\lambda}}\Big]^T, \tag{6}$$

$$\mathbf{a}_{Rx}(\theta_{Rx,p}) = \frac{1}{\sqrt{N_{Rx}}}\Big[1, e^{j\frac{2\pi d\sin(\theta_{Rx,p})}{\lambda}}, e^{j2\frac{2\pi d\sin(\theta_{Rx,p})}{\lambda}}, \cdots, , e^{j\frac{(N_{Rx}-1)2\pi d\sin(\theta_{Rx,p})}{\lambda}}\Big]^T, \tag{7}$$

respectively. In Eq. (6) and Eq. (7) λ is the wavelength of the signal and $d = \lambda/2$ denotes the aperture domain sample spacing. Thereafter, we adopt HBF for our MIMO OFDM scheme operating in doubly selective THz channels under the assumption that the CSI is available at both Alice and Bob. In light of this, the analog beamformed fading channel is formulated as:

$$\mathbf{H}^{RF}_{n,m,l} = \left(\mathbf{W}^{Rx,RF}\right)^H \mathbf{H}_{n,m,l}\mathbf{W}^{Tx,RF}, \tag{8}$$

where $\mathbf{W}^{Tx,RF} \in \mathcal{C}^{N_{Tx}\times N_s}$ and $\mathbf{W}^{Rx,RF} \in \mathcal{C}^{N_{Rx}\times N_s}$ are constituted by N_s columns of $\mathbf{A}_{Tx}$ and $\mathbf{A}_{Rx}$ that correspond to the first N_s largest channel gain of $\widetilde{h}_p$, respectively, while N_s represents the number of the data streams conveyed by each subcarrier. Furthermore, $\mathbf{A}_{Tx}$ and $\mathbf{A}_{Rx}$ representing the antenna response in matrix form are given by $\mathbf{A}_{Tx} = [\mathbf{a}_{Tx}(\theta_{Tx,0}), \mathbf{a}_{Tx}(\theta_{Tx,1}), ..., \mathbf{a}_{Tx}(\theta_{Tx,P-1})]$ and $\mathbf{A}_{Rx} = [\mathbf{a}_{Rx}(\theta_{Rx,0}), \mathbf{a}_{Rx}(\theta_{Rx,1}), ..., \mathbf{a}_{Rx}(\theta_{Rx,P-1})]$, respectively. The analog transmit precoder (TPC) and receiver combiner (RC) matrices should satisfy $\left\{\left\{\left\|\mathbf{W}^{Tx,RF}[t,\mu]\right\| = \frac{1}{\sqrt{N_{Tx}}}\right\}_{t=1}^{N_{Tx}}\right\}_{\mu=1}^{N_s}$ and $\left\{\left\{\left\|\mathbf{w}^{Rx,RF}[r,\nu]\right\| = \frac{1}{\sqrt{N_{Tx}}}\right\}_{r=1}^{N_{Rx}}\right\}_{\nu=1}^{N_s}$.

Therefore, the signal obtained by the receiver's ν-th RF chain after analog combining is modelled as

$$y^{\nu}_{n,m} = \sqrt{T}\sum_{\mu=0}^{N_s-1}\sum_{l=0}^{L-1} h^{RF_{\nu,\mu}}_{n,m,l} s^{\mu}_{n,<m-l>_M} + v^{\nu}_{n,m}, \tag{9}$$

where we have $v_{n,m} = \sqrt{T}\sum_{\mu=0}^{N_s-1}\sum_{l=0}^{L-1} h^{RF_{\nu,\mu}}_{n,m,l} \cdot s_{0^{\mu}_{n,<m-l>_M}} + \sqrt{1-T}s_{E^{\nu}_{n,m}}$, and $h^{RF_{\nu,\mu}}_{n,m,l} = \mathbf{H}^{RF}_{n,m,l}[\nu,\mu]$. The TD matrix form is given by

$$\mathbf{y}^{\nu}_n = \sqrt{T}\sum_{\mu=0}^{N_s-1}\mathbf{H}^{RF_{\nu,\mu}}_n \mathbf{s}^{\mu}_n + \mathbf{v}^{\nu}_n, \tag{10}$$

where $\mathbf{y}^{\nu}_n = [y^{\nu}_{n,0}, y^{\nu}_{n,1}, \cdots, y^{\nu}_{n,M-1}]^T$, $\mathbf{H}^{RF_{\nu,\mu}}_n[r,c] = h^{RF_{\nu,\mu}}_{n,r,<r-c>_M}$, $\mathbf{s}^{\mu}_n = [s^{\mu}_{n,0}, s^{\mu}_{n,1}, \cdots, s^{\mu}_{n,M-1}]^T$ and $\mathbf{v}^{\nu}_n = [v^{\nu}_{n,0}, v^{\nu}_{n,1}, \cdots, v^{\nu}_{n,M-1}]^T$. Then the FD received signal at the ν-th RF chain can be obtained by applying the DFT, yielding:

$$\begin{aligned}\overline{y}^{\nu}_{n,\overline{m}} &= \frac{1}{\sqrt{M}}\sum_{m=0}^{M-1} y^{\nu}_{n,m}\omega_M^{-m\overline{m}} \\ &= \frac{\sqrt{T}}{\sqrt{M}}\sum_{m=0}^{M-1}\sum_{\mu=0}^{N_s-1}\sum_{l=0}^{L-1} h^{RF_{\nu,\mu}}_{n,m,l} s^{\mu}_{n,<m-l>_M}\omega_M^{-m\overline{m}} + \overline{v}^{\nu}_{n,\overline{m}}.\end{aligned} \tag{11}$$

The FD matrix form is given by

$$\overline{\mathbf{y}}^{\nu}_n = \mathbf{F}_M\mathbf{y}^{\nu}_n = \sqrt{T}\sum_{\mu=0}^{N_s-1}\overline{\mathbf{H}}^{RF_{\nu,\mu}}_n\overline{\mathbf{s}}^{\mu}_n + \overline{\mathbf{v}}^{\nu}_n, \tag{12}$$

where $\overline{\mathbf{y}}^{\nu}_n \in \mathcal{C}^{M\times 1}$, $\overline{\mathbf{s}}^{\mu}_n = \mathbf{F}_M\mathbf{s}^{\mu}_n \in \mathcal{C}^{M\times 1}$, $\overline{\mathbf{v}}^{\nu}_n = \mathbf{F}_M\mathbf{v}^{\nu}_n \in \mathcal{C}^{M\times 1}$, while $\overline{\mathbf{H}}^{RF_{\nu,\mu}}_n = \mathbf{F}_M\mathbf{H}^{RF_{\nu,\mu}}_n\mathbf{F}^H_M \in \mathcal{C}^{M\times M}$ is no longer diagonal in time-varying frequency-selective fading. Following this, the full matrix form is expressed as

$$\overline{\mathbf{y}}_n = \sqrt{T}\overline{\mathbf{H}}^{RF}_n\overline{\mathbf{s}}_n + \overline{\mathbf{v}}_n, \tag{13}$$

where $\overline{\mathbf{y}}_n \in \mathcal{C}^{N_sM\times 1}$, $\overline{\mathbf{H}}^{RF}_n \in \mathcal{C}^{N_sM\times N_sM}$, $\overline{\mathbf{s}}_n \in \mathcal{C}^{N_sM\times 1}$ and $\overline{\mathbf{v}}_n \in \mathcal{C}^{N_sM\times 1}$.

Based on Eq. (13), the ABF performance can be further improved by digital beamforming, which relies on the singular value decomposition (SVD) as follows:

$$\overline{\mathbf{H}}^{RF}_n = \overline{\mathbf{U}}^{RF}_n\overline{\mathbf{\Sigma}}^{RF}_n(\overline{\mathbf{V}}^{RF}_n)^H, \tag{14}$$

where both $\overline{\mathbf{U}}^{RF}_n \in \mathcal{C}^{N_sM\times N_sM}$ and $\overline{\mathbf{V}}^{RF}_n \in \mathcal{C}^{N_sM\times N_sM}$ are unitary matrices, and the r^{FD}_n non-zero singular values of the rank r^{FD}_n matrix $\overline{\mathbf{H}}^{RF}_n$ can be expressed as follows:

$$\overline{\mathbf{\Sigma}}^{RF}_n = \begin{bmatrix} \mathrm{diag}\left\{\varsigma_{n,1}, \varsigma_{n,2}, ..., \varsigma_{n,r^{FD}_n}\right\} & \mathbf{0}_{r^{FD}_n\times\left(N_sM-r^{FD}_n\right)} \\ \mathbf{0}_{\left(N_sM-r^{FD}_n\right)\times r^{FD}_n} & \mathbf{0}_{\left(N_sM-r^{FD}_n\right)\times\left(N_sM-r^{FD}_n\right)} \end{bmatrix}. \tag{15}$$

Based on the singular values in Eq. (15), we retain the first $N^{FD}_{s,n}$ singular values of $\overline{\mathbf{H}}^{RF}_n$, which are no less than 0.1, i.e. $\varsigma_{n,n^{FD}_s} \geq 0.1$ with $n^{FD}_s \in [1, N^{FD}_{s,n}], N^{FD}_{s,n} \leq r^{FD}_n \leq N_sM$. Then we apply water-filling (WF) to them. In light of this, firstly, the average beamforming gain based on the $N^{FD}_{s,n}$ retained singular values can be derived as

$$\overline{\varsigma}_n = \sqrt{\frac{1}{N^{FD}_{s,n}}\sum\nolimits_{n^{FD}_s=1}^{N^{FD}_{s,n}}\varsigma^2_{n,n^{FD}_s}}. \tag{16}$$

Secondly, the first $N^{FD}_{s,n}$ columns of $\overline{\mathbf{V}}^{RF}_n$ and $\overline{\mathbf{U}}^{RF}_n$ are exploited as the digital TPC matrix $\overline{\mathbf{W}}^{Tx,BB}_n$ and RC matrix $\overline{\mathbf{W}}^{Rx,BB}_n$, respectively, i.e. $\overline{\mathbf{W}}^{Tx,BB}_n = \overline{\mathbf{V}}^{RF}_n[:, 1 : N^{FD}_{s,n}] \in \mathcal{C}^{N_sM\times N^{FD}_{s,n}}$ and $\left\|\overline{\mathbf{W}}^{Tx,BB}\right\|^2 = N^{FD}_{s,n}$, while $\overline{\mathbf{W}}^{Rx,BB}_n = \overline{\mathbf{U}}^{RF}_n[:, 1 : N^{FD}_{s,n}] \in \mathcal{C}^{N_sM\times N^{FD}_{s,n}}$ and $\left\|\overline{\mathbf{W}}^{Rx,BB}\right\|^2 = N^{FD}_{s,n}$. Thirdly, the digital TPC matrices are updated based on the average beamforming gain in Eq. (16) for WF, which gives

$$\overline{\mathbf{W}}^{Tx,BB}_{\mathrm{WF},n} = \overline{\mathbf{W}}^{Tx,BB}_n\overline{\varsigma}_n\left[\mathrm{diag}\left\{\frac{1}{\varsigma_{n,1}}, \frac{1}{\varsigma_{n,2}}, ..., \frac{1}{\varsigma_{n,N^{FD}_{s,n}}}\right\}\right]. \tag{17}$$

Therefore, at the transmitter, the data-carrying symbols are modulated in the FD as $\overline{\mathbf{x}}_n \in \mathcal{C}^{N^{FD}_{s,n}\times 1}$ and then the subcarriers are precoded as

$$\overline{\mathbf{s}}_n = \overline{\mathbf{W}}^{Tx,BB}_{\mathrm{WF},n}\overline{\mathbf{x}}_n. \tag{18}$$

At the receiver, digital RC is applied to $\overline{\mathbf{y}}_n$ of Eq. (13), which gives

$$\overline{\mathbf{r}}_n = \left(\overline{\mathbf{W}}^{Rx,BB}_n\right)^H\overline{\mathbf{y}}_n = \sqrt{T}\overline{\varsigma}_n\overline{\mathbf{x}}_n + \left(\overline{\mathbf{W}}^{Rx,BB}_n\right)^H\overline{\mathbf{v}}_n. \tag{19}$$

Therefore, the data streams are equalized in the FD as follows:

$$\overline{\mathbf{z}}_n = \overline{\mathbf{r}}_n/\overline{\varsigma}_n, \tag{20}$$

which obtains raw key in the FD based on OFDM modulation.

B. MIMO OTFS in Doubly Selective THz Channel using Hybrid Beamforming

As for OTFS based on the OFDM frame-wise CP structure, the receiver's ν-th RF chain signal after the analog RC is expressed as follows:

$$y_{n,m}^{\nu}=\sqrt{T}\sum_{\mu=0}^{N_s-1}\sum_{l=0}^{L-1}h_{n,m,l}^{RF_{\nu,\mu}}s_{<nM+m-l>_{MN}}^{\mu}+v_{n,m}^{\nu}, \tag{21}$$

where $v_{n,m}^{\nu}=\sqrt{T}\sum_{\mu=0}^{N_s-1}\sum_{l=0}^{L-1}h_{n,m,l}^{RF_{\nu,\mu}}s_{0<nM+m-l>_{MN}}^{\mu}+\sqrt{1-T}s_{E_{n,m}^{\nu}}$. After carrying out the DFT and SFFT at the receiver's ν-th RF chain, the DD-domain signal is given by

$$\widetilde{y}_{k,l}^{\nu}=\sqrt{T}\sum_{\mu=0}^{N_s-1}\sum_{p=0}^{P-1}\widetilde{h}_p^{RF_{\nu,\mu}}\widetilde{T}(k,l,k_p,l_p)\widetilde{s}_{<k-k_p>_N,<l-l_p>_M}^{\mu}+\widetilde{v}_{k,l}^{\nu}, \tag{22}$$

where we have

$$\begin{aligned}\widetilde{h}_p^{RF_{\nu,\mu}}=\sqrt{N_{Tx}N_{Rx}}\widetilde{h}_p\cdot\Big[&\left(\mathbf{W}^{Rx,RF}\right)^H\mathbf{a}_{Rx}\left(\theta_{Rx},p\right)\cdot\\&\mathbf{a}_{Tx}^H\left(\theta_{Tx},p\right)\mathbf{W}^{Tx,RF}\Big][\nu,\mu].\end{aligned} \tag{23}$$

The DD-domain input-output relationship cast in matrix form is hence given by

$$\widetilde{\mathbf{y}}^{\nu}=\sqrt{T}\sum_{\mu=0}^{N_s-1}\widetilde{\mathbf{H}}^{RF_{\nu,\mu}}\widetilde{\mathbf{s}}^{\mu}+\widetilde{\mathbf{v}}^{\nu}, \tag{24}$$

where we have $\widetilde{\mathbf{y}}^{\nu}\in\mathcal{C}^{MN\times1}$, $\widetilde{\mathbf{y}}^{\nu}[\kappa]=\widetilde{y}_{k,l}$, $\widetilde{\mathbf{s}}^{\mu}\in\mathcal{C}^{MN\times1}$, $\widetilde{\mathbf{s}}^{\mu}[\kappa]=\widetilde{s}_{k,l}$, $\widetilde{\mathbf{v}}^{\nu}\in\mathcal{C}^{MN\times1}$, $\widetilde{\mathbf{v}}^{\nu}[\kappa]=\widetilde{v}_{k,l}$, $k=\lfloor\frac{\kappa}{M}\rfloor$, $l=\kappa-kM$, $\widetilde{\mathbf{H}}^{RF_{\nu,\mu}}\in\mathcal{C}^{MN\times MN}$, $\widetilde{\mathbf{H}}^{RF_{\nu,\mu}}[\kappa,\iota]=\widetilde{h}_p^{RF_{\nu,\mu}}\widetilde{T}(k,l,k_p,l_p)$. Furthermore, the full matrix form is given by

$$\widetilde{\mathbf{y}}=\sqrt{T}\widetilde{\mathbf{H}}^{RF}\widetilde{\mathbf{s}}+\widetilde{\mathbf{v}}, \tag{25}$$

where $\widetilde{\mathbf{y}}\in\mathcal{C}^{N_sMN\times1}$, $\widetilde{\mathbf{H}}^{RF}\in\mathcal{C}^{N_sMN\times N_sMN}$, $\widetilde{\mathbf{s}}\in\mathcal{C}^{N_sMN\times1}$ and $\widetilde{\mathbf{v}}\in\mathcal{C}^{N_sMN\times1}$. Similar to its use in OFDM, the SVD is applied to $\widetilde{\mathbf{H}}^{RF}$, which gives

$$\widetilde{\mathbf{H}}^{RF}=\widetilde{\mathbf{U}}^{RF}\widetilde{\mathbf{\Sigma}}^{RF}(\widetilde{\mathbf{V}}^{RF})^H, \tag{26}$$

where both $\widetilde{\mathbf{U}}^{RF}\in\mathcal{C}^{N_sMN\times N_sMN}$ and $\widetilde{\mathbf{V}}^{RF}\in\mathcal{C}^{N_sMN\times N_sMN}$ are unitary matrices, and the r^{DD} non-zero singular values of the rank r^{DD} matrix $\widetilde{\mathbf{H}}^{RF}$ can be expressed as follows:

$$\widetilde{\mathbf{\Sigma}}^{RF}=\begin{bmatrix}\mathrm{diag}\left\{\vartheta_1,\vartheta_2,...,\vartheta_{r^{DD}}\right\}&\mathbf{0}_{r^{DD}\times\left(N_sMN-r^{DD}\right)}\\\mathbf{0}_{\left(N_sMN-r^{DD}\right)\times r^{DD}}&\mathbf{0}_{\left(N_sMN-r^{DD}\right)\times\left(N_sMN-r^{DD}\right)}\end{bmatrix} \tag{27}$$

Based on the singular values in Eq. (27), we take the first N_s^{DD} singular values of $\widetilde{\mathbf{H}}^{RF}$, which are no less than 0.1, i.e. $\vartheta_{n_s^{DD}}\geq0.1$ with $n_s^{DD}\in[1,N_s^{DD}]$, $N_s^{DD}\leq r^{DD}\leq N_sMN$. Then we apply water-filling to them. In light of this, firstly, the average beamforming gain based on the N_s^{DD} singular values can be formulated as:

$$\overline{\vartheta}=\sqrt{\frac{1}{N_s^{DD}}\sum\nolimits_{n_s^{DD}=1}^{N_s^{DD}}\vartheta_{n_s^{DD}}^2}. \tag{28}$$

Secondly, the first N_s^{DD} columns of $\widetilde{\mathbf{V}}^{RF}$ and $\widetilde{\mathbf{U}}^{RF}$ are harnessed as the digital TPC matrix $\widetilde{\mathbf{W}}^{Tx,BB}$ and RC matrix $\widetilde{\mathbf{W}}^{Rx,BB}$, respectively, i.e. $\widetilde{\mathbf{W}}^{Tx,BB}=\widetilde{\mathbf{V}}^{RF}[:,1:N_s^{DD}]\in\mathcal{C}^{N_sMN\times N_s^{DD}}$ and $\left\|\widetilde{\mathbf{W}}^{Tx,BB}\right\|^2=N_s^{DD}$, while $\widetilde{\mathbf{W}}^{Rx,BB}=\widetilde{\mathbf{U}}^{RF}[:,1:N_s^{DD}]\in\mathcal{C}^{N_sMN\times N_s^{DD}}$ and $\left\|\widetilde{\mathbf{W}}^{Rx,BB}\right\|^2=N_s^{DD}$. Thirdly, the digital TPC matrices are updated based on the average beamforming gain in Eq. (28) of WF, which gives

$$\widetilde{\mathbf{W}}_{\mathrm{WF}}^{Tx,BB}=\widetilde{\mathbf{W}}^{Tx,BB}\overline{\vartheta}\left[\mathrm{diag}\left\{\frac{1}{\vartheta_1},\frac{1}{\vartheta_2},...,\frac{1}{\vartheta_{N_s^{DD}}}\right\}\right]. \tag{29}$$

Therefore, at the transmitter, the data-carrying symbols are modulated in the DD as $\widetilde{\mathbf{x}}\in\mathcal{C}^{N_s^{DD}\times1}$ and then the subcarriers are precoded as

$$\widetilde{\mathbf{s}}=\widetilde{\mathbf{W}}_{\mathrm{WF}}^{Tx,BB}\widetilde{\mathbf{x}}. \tag{30}$$

At the receiver, the digital RC is applied to $\widetilde{\mathbf{y}}$ of Eq. (25), which gives

$$\widetilde{\mathbf{r}}=\left(\widetilde{\mathbf{W}}^{Rx,BB}\right)^H\widetilde{\mathbf{y}}=\sqrt{T}\overline{\vartheta}\widetilde{\mathbf{x}}+\left(\widetilde{\mathbf{W}}^{Rx,BB}\right)^H\widetilde{\mathbf{v}}. \tag{31}$$

Hence, the DD-domain data-carrying symbols are normalized as

$$\widetilde{\mathbf{z}}=\widetilde{\mathbf{r}}/\overline{\vartheta}, \tag{32}$$

which obtains raw key in the DD based on OTFS modulation.

C. MDR Decoding for OFDM/OTFS in Doubly Selective THz Channels

As portrayed in Fig. 1, the MDR process [42], [43], [46] is employed for enhancing the CV-QKD performance in THz quantum channels after the OFDM- and OTFS- based quantum transmission and detection. However, the conventional MDR found in [47], [48] generally assumes a binary AWGN (BI-AWGN) channel, where the noise variance of log likelihood ratio (LLR) computation is uniform across all received Gaussian variables. By contrast, the OFDM FD-SVD decision variables $\overline{\mathbf{z}}_n$ in Eq. (20) exhibit different noise variances across different OFDM symbols for each sub-channel in the presence of doubly selective fading. By contrast, the OTFS DD-SVD decision variables $\widetilde{\mathbf{z}}$ in Eq. (32) have a noise variance that is always the same for each sub-channel in doubly selective fading. In light of this, the modified MDR scheme associated with a new mapping schemes [42] is adopted in order to provide reliable LLRs, which is elaborated on in Algorithm 1 of [42].

Therefore, the LLR calculation associated with FD-SVD detection of Eq. (20) in OFMD transmission can be obtained as

$$\mathcal{L}\left(\mathbf{u}_i^A[d]\right)=\frac{2\left\|\ddot{\mathbf{x}}_i\right\|\left\|\ddot{\mathbf{z}}_i\right\|}{\sqrt{D}}\frac{\left\|\overline{\varsigma}_n^{\varrho}\right\|^2}{\left\|\overline{\mathbf{W}}_{\varrho,n}^{Rx,BB}[:,n_s^{FD}]\right\|^2N_0/2}\mathbf{u}_i^A[d], \tag{33}$$

where the modulated/demodulated symbols of the ith segment can be denoted as $\ddot{\mathbf{x}}_i=\mathfrak{Re}\left[\bar{\mathbf{x}}_i^{\mathrm{MDR}}\right]=\mathfrak{Re}\left[\bar{x}_{i,0}^{\mathrm{MDR}},\cdots,\bar{x}_{i,d}^{\mathrm{MDR}},\cdots,\bar{x}_{i,D-1}^{\mathrm{MDR}}\right]^T$ and $\ddot{\mathbf{z}}_i=\mathfrak{Re}\left[\bar{\mathbf{z}}_i^{\mathrm{MDR}}\right]=\mathfrak{Re}\left[\bar{z}_{i,0}^{\mathrm{MDR}},\cdots,\bar{z}_{i,d}^{\mathrm{MDR}},\cdots,\bar{z}_{i,D-1}^{\mathrm{MDR}}\right]^T$ along with $i=\lfloor n/D\rfloor\cdot N_s^{FD}+n_s^{FD}+\varrho\left(N/D\cdot N_s^{FD}\right)$ and $d=\mathrm{rem}(n,D)$, while $n=0,1,...,N-1$, $n_s^{FD}=0,1,...,N_s^{FD}-1$ and $\varrho=0,1,...,N_{bl}-1$. Moreover, $\bar{x}_{i,d}^{\mathrm{MDR}}=\bar{x}_{n,n_s^{FD}}^{\varrho}$ and $\bar{z}_{i,d}^{\mathrm{MDR}}=$

$\bar{z}^{\varrho}_{n,n_s^{FD}}$ represent the dth element in the ith segment of $\bar{s}_i^{\text{MDR}}$ and $\bar{z}_i^{\text{MDR}}$, respectively. The ith segment of noise term can be denoted as $\ddot{\mathbf{v}}_i = \mathfrak{Re}\left[\bar{v}_{i,0}^{\text{MDR}}, \cdots, \bar{v}_{i,d}^{\text{MDR}}, \cdots, \bar{v}_{i,D-1}^{\text{MDR}}\right]^T$ with $\bar{v}_{i,d}^{\text{MDR}} = \bar{v}^{\varrho}_{n,n_s^{FD}}$. Therefore, the variance of each element of the noise becomes $\frac{\left\|\overline{\mathbf{W}}_{\varrho,n}^{Rx,BB}[:,n_s^{FD}]\right\|^2 N_0/2}{\|\bar{\varsigma}_n^{\varrho}\|^2}$, with N_0 representing the power of the original AWGN[3].

In OTFS transmission, similar to Eq. (33), the LLR calculation associated with the DD-SVD detection of Eq. (32) in OTFS transmission can be obtained as

$$\mathcal{L}\left(\mathbf{u}_i^A[d]\right) = \frac{2\|\ddot{\mathbf{x}}_i\|\|\ddot{\mathbf{z}}_i\|}{\sqrt{D}} \frac{\left\|\bar{\vartheta}^{\varrho}\right\|^2}{\left\|\widetilde{\mathbf{W}}_{\varrho}^{Rx,BB}[:,n_s^{DD}]\right\|^2 N_0/2} \mathbf{u}_i^A[d], \tag{34}$$

where the modulated/demodulated symbols for the ith segment can be denoted as $\ddot{\mathbf{x}}_i = \mathfrak{Re}\left[\widetilde{\mathbf{x}}_i^{\text{MDR}}\right] = \mathfrak{Re}\left[\widetilde{x}_{i,0}^{\text{MDR}}, \cdots, \widetilde{x}_{i,d}^{\text{MDR}}, \cdots, \widetilde{x}_{i,D-1}^{\text{MDR}}\right]^T$, and $\ddot{\mathbf{z}}_i = \mathfrak{Re}\left[\widetilde{\mathbf{z}}_i^{\text{MDR}}\right] = \mathfrak{Re}\left[\widetilde{z}_{i,0}^{\text{MDR}}, \cdots, \widetilde{z}_{i,d}^{\text{MDR}}, \cdots, \widetilde{z}_{i,D-1}^{\text{MDR}}\right]^T$ with $i = n_s^{DD} + \lfloor \varrho/D \rfloor \cdot N_s^{DD}$ and $d = \text{rem}(\varrho, D)$, where $\varrho = 0, 1, ..., N_{bl} - 1$. Moreover, $\widetilde{x}_{i,d}^{\text{MDR}} = \widetilde{x}^{\varrho}_{n_s^{DD}}$ and $\widetilde{z}_{i,d}^{\text{MDR}} = \widetilde{z}^{\varrho}_{n_s^{DD}}$ represent the dth element in the ith segment of $\widetilde{x}_i^{\text{MDR}}$ and $\widetilde{z}_i^{\text{MDR}}$, respectively. The ith segment of the noise term can be denoted as $\ddot{\mathbf{v}}_i = \mathfrak{Re}\left[\widetilde{v}_{i,0}^{\text{MDR}}, \cdots, \widetilde{v}_{i,d}^{\text{MDR}}, \cdots, \widetilde{v}_{i,D-1}^{\text{MDR}}\right]^T$ along with $\widetilde{v}_{i,d}^{\text{MDR}} = \widetilde{v}^{\varrho}_{n_s^{DD}}$. Therefore, the variance of each element of the noise $\ddot{\mathbf{v}}_i$ becomes $\frac{\left\|\widetilde{\mathbf{W}}_{\varrho}^{Rx,BB}[:,n_s^{DD}]\right\|^2 N_0/2}{\left\|\bar{\vartheta}^{\varrho}\right\|^2}$.

Note that the accuracy of the FD LLRs of Eq. (33) may be impacted by the MDR process in mobile scenarios, which will lead to degraded SKR performance. Specifically, the MDR process assumes identical fading gains for all elements within a segment, resulting in a uniform fading value during the LLR calculation for a segment. However, in time-variant channels, the FD channel $\overline{\mathbf{H}}_n^{RF}$ will fluctuate with time, therefore the average beamforming gain $\bar{\varsigma}_n^{\varrho}$ obtained for each element in a segment will differ from each other, which degrades the accuracy of the FD LLR calculation of Eq. (33). By contrast, the accuracy of DD LLR calculation of Eq. (34) remains unaffected by the MDR process in mobile scenarios, because the DD domain channel matrix $\widetilde{\mathbf{H}}^{RF}$ remains quasi-static even in doubly selective fading channels.

D. Complexity Analysis for OFDM/OTFS in Doubly Selective THz Channels

Clearly, the SVD calculations dominate the computational complexities of both the OFDM- and OTFS-based transceivers. To elaborate further, the complexity of FD-SVD in Eq. (14) for a single OFDM symbol associated with $\overline{\mathbf{H}}_n^{RF} \in \mathcal{C}^{M\times M}$ is $\mathcal{O}(M^3)$ [49]–[51]. Hence the complexity of a block is $\mathcal{O}(M^3N)$. By contrast, for an OTFS-based system associated with $\widetilde{\mathbf{H}}^{RF} \in \mathcal{C}^{MN\times MN}$, the complexity of a DD-SVD in Eq. (26) for a single OTFS block is $\mathcal{O}(M^3N^3)$.

[3]The value of N_0 is to evaluate the noise level as the signal power is normalized to 1 in simulation. But both the realistic signal and noise powers will be elaborated in Sec. V.

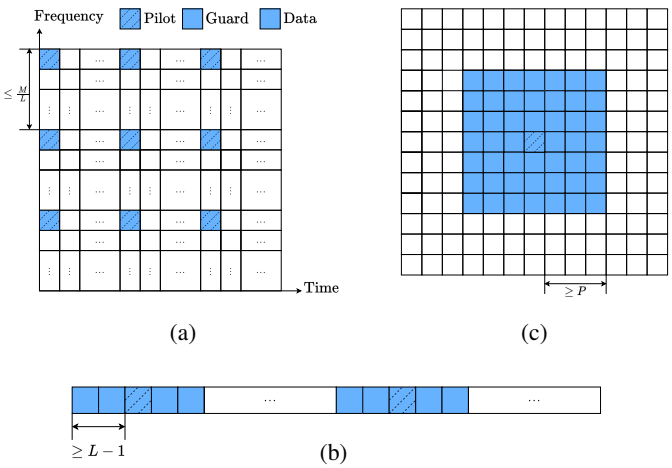


Fig. 5: Schematic illustration of (a) FD, (b) TD and (c) DD-domain channel estimation techniques.

Therefore, the complexity of the FD-SVD of OFDM is lower than that of DD-SVD of OTFS. Note that both detectors perform similarly in a stationary scenario. Hence, the FD-SVD of OFDM is the better choice in stationary scenarios.

However, in high-mobility scenarios, the total complexity for N_{bl} blocks of OFDM or OTFS symbols required for completing the MDR process with the aid of LDPC codes is $\mathcal{O}(M^3NN_{bl})$ and $\mathcal{O}(M^3N^3)$ for OFDM and OTFS, respectively. This is because in time-variant channels, the FD matrix $\overline{\mathbf{H}}_n^{RF}$ will change with time, which means that the digital beamforming of OFDM has to be updated for each OFDM symbol, where the SVD calculations required for updating the digital beamforming have to be repeated. By contrast, the digital beamforming of OTFS does not have to be updated, owing to the fact that the DD-domain fading representation is time-invariant. In this context, OTFS exhibits lower complexity than OFDM when $N_{bl} > N^2$. This condition arises when a large number of blocks are combined with powerful LDPC codes featuring long frame lengths, enabling near-capacity performance.

IV. Proposed MIMO OFDM/OTFS channel estimation in CV-QKD system

In contrast to the ABF MIMO OFDM/OTFS CV-QKD scheme proposed in [42], where perfect CSI is assumed, a realistic imperfect CSI is considered in this work. Therefore, in this section, MIMO OFDM/OTFS channel estimation algorithms are proposed for time-varying frequency-selective MIMO THz channels. Fig. 5 illustrates three different channel estimation techniques, namely FD, TD and DD-domain estimations, respectively. The FD estimation in Fig. 5(a) arranges the pilot symbols in both FD and TD with suitable spacings, which can be viewed as the "horizontal comb" and the "vertical comb". In contrast to FD estimation, Fig. 5(b) shows the TD estimation via placing the TD pilot symbols at the beginning of each transmitted frame. Moreover, as for the DD-domain estimation shown in Fig. 5(c), the pilot symbols are inserted into DD index grids. For OFDM channel estimation,

it was demonstrated in [44] that TD estimation performs better than FD estimation in the face of intercarrier interference (ICI), while the DD-domain channel estimation is the natural choice for OTFS systems.

A. MIMO OFDM Doubly Selective Channel Estimation

For MIMO OFDM, the subcarriers are assumed to be orthogonal to each other without ICI, which is only true in time-invariant fading channels. Hence the TF-domain channel estimation algorithm that assumes time-invariant fading for MIMO OFDM is detailed as follows. Firstly, the input-output relationship between the uth TA of the transmitter and the vth RA of the receiver in the TD is modelled as follows

$$\mathbf{y}^{CE_{v,u}} = \mathbf{H}^{CE_{v,u}}\mathbf{s}^{CE_{v,u}} + \mathbf{v}^{CE_{v,u}}, \tag{35}$$

where $\mathbf{y}^{CE_{v,u}} \in \mathcal{C}^{L\times 1}$ represents the received contaminated pilot symbols. Furthermore, $\mathbf{s}^{CE_{v,u}} \in \mathcal{C}^{L\times 1}$ represents the pilot symbols, which takes part of the Direc delta impulse-based CP inserted in the TD of Fig. 5(a). More specifically, the Direc delta pulse-based CP is expressed as [44]

$$s_{0,m} = \begin{cases} \rho_{\mathrm{p}}^{\mathrm{TD}}, & m = 0 \\ 0, & m = \pm 1, \pm 2, \ldots, \pm \mathcal{N}_{\mathrm{guard}}^{\mathrm{TD}} \end{cases}, \tag{36}$$

where the power of the pilot impulse $\rho_{\mathrm{p}}^{\mathrm{TD}}$ aims for ensuring that the transmission power obeys $\sum_{\forall m}\|s_{0,m}\|^2 = 2\mathcal{N}_{\mathrm{guard}}^{\mathrm{TD}} + 1$, while the zeros in Eq. (36) are referred to as guard intervals in Fig. 5(a). Based on Eq. (36), the first $L-1$ zeros provides CP, which are removed from Eq. (35). In this way, the CIR taps in the TD can be estimated one by one based on Eq. (35). Therefore, to make sure that there is no interference when carrying out TD convolution represented in the matrix form of Eq. (35), the number of guard intervals $\mathcal{N}_{\mathrm{guard}}^{\mathrm{TD}}$ should be no less than $L-1$, i.e. $\mathcal{N}_{\mathrm{guard}}^{\mathrm{TD}} \geq L-1$. In our work, we set $\mathcal{N}_{\mathrm{guard}}^{\mathrm{TD}} = L-1$. Moreover, $\mathbf{H}^{CE_{v,u}} \in \mathcal{C}^{L\times L}$ represents the $L \times L$ CIR matrix in TD, which is expressed as

$$\mathbf{H}^{CE_{v,u}} = \begin{bmatrix} h_{0,v,u} & h_{L-1,v,u} & \cdots & h_{2,v,u} & h_{1,v,u} \\ h_{1,v,u} & h_{0,v,u} & \cdots & h_{3,v,u} & h_{2,v,u} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ h_{L-2,v,u} & h_{L-3,v,u} & \cdots & h_{0,v,u} & h_{L-1,v,u} \\ h_{L-1,v,u} & h_{L-2,v,u} & \cdots & h_{1,v,u} & h_{0,v,u} \end{bmatrix}, \tag{37}$$

where $h_{l,v,u}, \forall l \in [0, L-1]$ are the L CIR taps and $h_{l,v,u} = \sqrt{N_{Tx}N_{Rx}} \cdot \sum_{\forall l_p = l} \widetilde{h}_p \Big[\sqrt{N_{Rx}}\, \mathbf{a}_{Rx}(\theta_{Rx}, p)\sqrt{N_{Rx}}\mathbf{a}_{Tx}^H(\theta_{Tx}, p)\Big][v,u]$. Secondly, based on Eq. (35), the L CIR taps can be estimated as $\widehat{h}_{l,v,u}$ that contains the angle of arrival (AoA) and angle of departure (AoD) information. More explicitly, since the TD CE pilot symbol is a Dirac Delta signal, $y^{CE_{v,u}}$ can be directly used as the noise-contaminated estimated CIR $\widehat{h}_{l,v,u}$. Thirdly, the full channel matrix containing all the $\widehat{h}_{l,v,u}$ values of the different antenna pairs for the lth delay tap is constructed as follows

$$\widehat{\mathbf{H}}_l = \begin{bmatrix} \widehat{h}_{l,1,1} & \widehat{h}_{l,1,2} & \cdots & \widehat{h}_{l,1,N_{Tx}} \\ \widehat{h}_{l,2,1} & \widehat{h}_{l,2,2} & \cdots & \widehat{h}_{l,2,N_{Tx}} \\ \vdots & \vdots & \ddots & \vdots \\ \widehat{h}_{l,N_{Rx},1} & \widehat{h}_{l,N_{Rx},2} & \cdots & \widehat{h}_{l,N_{Rx},N_{Tx}} \end{bmatrix}. \tag{38}$$

Based on Eq. (38), the dominant AoA $\widehat{\theta}_{Rx,p}$ and AoD $\widehat{\theta}_{Tx,p}$ and channel gain of $\widehat{\widetilde{h}}_p$ for the lth delay tap, i.e. $l_p = l$, can be obtained, as described in Algorithm 1. Therefore, the reconstructed channel in TD after channel estimation can be expressed as

$$\widehat{\mathbf{H}}_{n,m,l} = \sqrt{N_{Tx}N_{Rx}} \cdot \widehat{\widetilde{h}}_p \mathbf{a}_{Rx}(\widehat{\theta}_{Rx,p})\mathbf{a}_{Tx}^H(\widehat{\theta}_{Tx,p}),\ l_p = l. \tag{39}$$

Algorithm 1: MIMO OFDM channel estimation algorithm.

Input: $\mathbf{y}^{CE_{v,u}}$ for $u/v = 0, 1, ..., N_{Tx-1}/N_{Rx-1}$.

Output: AoA and AoD $\widehat{\theta}_{Rx,p}, \widehat{\theta}_{Tx,p}$, and channel gain $\widehat{\widetilde{h}}_p$ with $l_p = l$ for all the delay taps.

// Obtain channel gain $\widehat{h}_{l,v,u}$

for *All the* (v,u) *antenna pairs* **do**

  Get $\widehat{h}_{l,v,u}$ for L delay taps.

end

// Obtain $\widehat{\theta}_{Rx,p}$, $\widehat{\theta}_{Tx,p}$, and $\widehat{\widetilde{h}}_p$ with $l_p = l$

for *All the* L *delay taps* **do**

  Construct $\widehat{\mathbf{H}}_l$ based on Eq. (38) using $\widehat{h}_{l,v,u}$.

  Define the objective function:

$$J(\theta_{Rx,p}, \theta_{Tx,p}) = \mathbf{a}_{Rx}^H(\theta_{Rx,p}) \cdot \widehat{\mathbf{H}}_l \cdot \mathbf{a}_{Tx}(\theta_{Tx,p}). \tag{40}$$

  The estimation of AoA/AoD can be obtained by:

$$\left(\widehat{\theta}_{Rx,p}, \widehat{\theta}_{Tx,p}\right) = \arg \max_{\substack{\forall \theta_{Rx,p} = 0^\circ, 1^\circ, \ldots, 90^\circ \\ \forall \theta_{Tx,p} = 0^\circ, 1^\circ, \ldots, 90^\circ}} J(\theta_{Rx,p}, \theta_{Tx,p}) \tag{41}$$

  based on the orthogonality of two different steering vectors, which obey:

$$\mathbf{a}_{Rx}^H(\theta_{Rx,p})\,\mathbf{a}_{Rx}(\theta_{Rx,p}) = 1, \mathbf{a}_{Tx}^H(\theta_{Tx,p})\,\mathbf{a}_{Tx}(\theta_{Tx,p}) = 1. \tag{42}$$

  The channel gain can be obtained by:

$$\widehat{\widetilde{h}}_p = \frac{J_{\max}}{N_{Rx}N_{Tx}}. \tag{43}$$

end

// Reconstruct the channel in TD

Reconstruct the channel in TD after channel estimation, which is expressed as in Eq. (39).

// Update the analog beamformed fading channel

Update the analog beamformed fading channel $\widehat{\mathbf{H}}_{n,m,l}^{RF}$ based on Eq. (8).

B. MIMO OTFS Doubly Selective Channel Estimation

In this section, we conceive the DD-domain channel estimation for MIMO OTFS. The proposed method is based on the assumption of quasi-static DD-domain fading, which is true even in realistic doubly selective THz fading channels.

We perform the DD-domain channel estimation based on each single antenna pair in order to obtain the AoA/AoD, delay and Doppler indices and channel gain for each path. The detailed procedure is shown in Algorithm 2. Firstly, the input-output relationship between the uth TA of the transmitter and the vth RA of the receiver in the DD domain is modelled as follows:

$$\widetilde{\mathbf{y}}^{CE_{v,u}} = \widetilde{\mathbf{H}}^{CE_{v,u}} \widetilde{\mathbf{s}}^{CE_{v,u}} + \widetilde{\mathbf{v}}^{CE_{v,u}}, \tag{44}$$

where we have $\widetilde{\mathbf{y}}^{CE_{v,u}} \in \mathcal{C}^{MN\times 1}$, $\widetilde{\mathbf{H}}^{CE_{v,u}} \in \mathcal{C}^{MN\times MN}$, $\widetilde{\mathbf{s}}^{CE_{v,u}} \in \mathcal{C}^{MN\times 1}$ and $\widetilde{\mathbf{v}}^{CE_{v,u}} \in \mathcal{C}^{MN\times 1}$. Furthermore, $\widetilde{\mathbf{H}}^{CE_{v,u}}[\kappa,\iota] = \widetilde{h}_{p,v,u}\widetilde{T}(k,l,k_p,l_p)$ and $\widetilde{h}_{p,v,u} = \sqrt{N_{Tx}N_{Rx}}\widetilde{h}_p \cdot \left[\sqrt{N_{Rx}}\mathbf{a}_{Rx}(\theta_{Rx},p)\sqrt{N_{Tx}}\mathbf{a}_{Tx}^H(\theta_{Tx},p)\right][v,u]$, since neither analog beamforming nor digital beamforming is used during the channel estimation process. Moreover, $\widetilde{\mathbf{s}}^{CE_{v,u}}$ represents the DD-domain pilot symbol, which is a Dirac delta impulse transmitted in the DD-domain of Fig. 5(b). The elements of $\widetilde{\mathbf{s}}^{CE_{v,u}}$ are set as [44]

$$\widetilde{\mathbf{s}}^{CE_{v,u}}[\kappa] = \begin{cases} \rho_{\mathrm{p}}^{\mathrm{DD}}, & \kappa = \kappa_{\mathrm{p}} \\ 0, & \kappa = \kappa_{\mathrm{p}} \pm 1, \kappa_{\mathrm{p}} \pm 2, \ldots, \kappa_{\mathrm{p}} \pm \mathcal{N}_{\mathrm{guard}}^{\mathrm{DD}} \\ \widetilde{s}_{k,l}, & \text{otherwise} \end{cases} \tag{45}$$

where the power of the pilot impulse $\rho_{\mathrm{p}}^{\mathrm{DD}}$ is adjusted for maintaining the constant OTFS frame power of MN. The guard interval has to obey $\mathcal{N}_{\mathrm{guard}}^{\mathrm{DD}} \geq P$. Secondly, the estimated Delay and Doppler index $\widehat{l}_p, \widehat{k}_p$ and channel gain $\widehat{\widetilde{h}}_{p,v,u}$ that contains the AoA and AoD information are obtained based on the SISO OTFS channel estimation algorithm of [33]. Thirdly, a new channel matrix containing all the $\widehat{\widetilde{h}}_{p,v,u}$ values of the different antenna pairs for the pth path is constructed as follows

$$\widehat{\widetilde{\mathbf{H}}}_p = \begin{bmatrix} \widehat{\widetilde{h}}_{p,1,1} & \widehat{\widetilde{h}}_{p,1,2} & \cdots & \widehat{\widetilde{h}}_{p,1,N_{Tx}} \\ \widehat{\widetilde{h}}_{p,2,1} & \widehat{\widetilde{h}}_{p,2,2} & \cdots & \widehat{\widetilde{h}}_{p,2,N_{Tx}} \\ \vdots & \vdots & \ddots & \vdots \\ \widehat{\widetilde{h}}_{p,N_{Rx},1} & \widehat{\widetilde{h}}_{p,N_{Rx},2} & \cdots & \widehat{\widetilde{h}}_{p,N_{Rx},N_{Tx}} \end{bmatrix}. \tag{46}$$

Based on Eq. (46), the estimated AoA $\widehat{\theta}_{Rx,p}$ and AoD $\widehat{\theta}_{Tx,p}$ and channel gain $\widetilde{h}_p$ can be obtained, as detailed in Algorithm 2.

It is worth briefly mentioning that the overhead of the TD/DD-domain channel estimation, as shown in Fig. 4(b) and (c) applied for OFDM-based and OTFS-based systems, respectively, mainly relies on the numbers of TDLs L and paths P. More explicitly, the overhead of the TD channel estimation can be quantified by $\left(2\mathcal{N}_{\mathrm{guard}}^{\mathrm{TD}}+1\right)$ for an OFDM symbol. Therefore, the overhead for a block of OFDM symbols is $\left(2\mathcal{N}_{\mathrm{guard}}^{\mathrm{TD}}+1\right)\cdot N$, since pilot symbols are required for each OFDM symbol within each block. On the other hand, the overhead of the DD-domain channel estimation can be quantified by $\left(2\mathcal{N}_{\mathrm{guard}}^{\mathrm{DD}}+1\right)^2$ for the duration of an OTFS block corresponding to N OFDM symbols, thanks to the time-invariant nature of DD-domain fading. For example, consider $\mathcal{N}_{\mathrm{guard}}^{\mathrm{TD}} = 2$ and $\mathcal{N}_{\mathrm{guard}}^{\mathrm{DD}} = 3$ when $L = P = 3$, which coincides with the illustration in Fig. 4 of our manuscript, and $M = 64$, $N = 16$. Then the pilot overhead for an OFDM block is $\left(2\mathcal{N}_{\mathrm{guard}}^{\mathrm{TD}}+1\right)\cdot N = 80$, while the overhead for an OTFS block is $\left(2\mathcal{N}_{\mathrm{guard}}^{\mathrm{DD}}+1\right)^2 = 49$. Therefore, the overhead of OTFS is smaller than that of OFDM for most settings. As for the complexity of channel estimation, the complexities of Algorithm 1 and Algorithm 2 are approximately the same, since the sizes of the matrices involved in implementing the algorithms in Eq. (38) and in Eq. (46) are the same. However, the TD channel estimation Algorithm 1 has to be activated for each OFDM symbol, while the DD-domain channel estimation Algorithm 2 of OTFS only once. Therefore, the complexity of our channel estimator proposed for OTFS is approximately a factor of N lower than that of OFDM.

Algorithm 2: MIMO OTFS channel estimation algorithm.

Input: $\widetilde{\mathbf{y}}^{CE_{v,u}}$ for $u/v = 0, 1, ..., N_{Tx-1}/N_{Rx-1}$. **Output:** Delay and Doppler index $\widehat{l}_p, \widehat{k}_p$, AoA and AoD $\widehat{\theta}_{Rx,p}, \widehat{\theta}_{Tx,p}$, and channel gain $\widehat{\widetilde{h}}_p$ for all the paths.

`// Obtain` $\widehat{l}_p, \widehat{k}_p$ `and channel gain` $\widehat{\widetilde{h}}_{p,v,u}$

for *All the* (v,u) *antenna pairs* **do**

  Get $\widehat{l}_p, \widehat{k}_p, \widehat{\widetilde{h}}_{p,v,u}$ for $\widehat{P}$ paths based on SISO OTFS channel estimation in [33].

end

`// Obtain` $\widehat{\theta}_{Rx,p}, \widehat{\theta}_{Tx,p}$, `and` $\widehat{\widetilde{h}}_p$

for *All the* $\widehat{P}$ *paths* **do**

  Construct $\widehat{\widetilde{\mathbf{H}}}_p$ based on Eq. (46) using $\widehat{\widetilde{h}}_{p,v,u}$.

  Define the objective function:

$$J(\theta_{Rx,p},\theta_{Tx,p}) = \mathbf{a}_{Rx}^H(\theta_{Rx,p}) \cdot \widehat{\widetilde{\mathbf{H}}}_p \cdot \mathbf{a}_{Tx}(\theta_{Tx,p}). \tag{47}$$

  The estimation of AoA/AoD can be obtained by:

$$\left(\widehat{\theta}_{Rx,p}, \widehat{\theta}_{Tx,p}\right) = \arg \max_{\substack{\forall\theta_{Rx,p}=0^\circ,1^\circ,\ldots,90^\circ \\ \forall\theta_{Tx,p}=0^\circ,1^\circ,\ldots,90^\circ}} J(\theta_{Rx,p},\theta_{Tx,p}) \tag{48}$$

  based on the orthogonality of two different steering vectors, which obey:

$$\mathbf{a}_{Rx}^H(\theta_{Rx,p})\,\mathbf{a}_{Rx}(\theta_{Rx,p}) = 1, \mathbf{a}_{Tx}^H(\theta_{Tx,p})\,\mathbf{a}_{Tx}(\theta_{Tx,p}) = 1. \tag{49}$$

  The channel gain can be obtained by:

$$\widehat{\widetilde{h}}_p = \frac{J_{\max}}{N_{Rx}N_{Tx}}. \tag{50}$$

end

`// Reconstruct the analog beamformed fading gain for each path`

Reconstruct the analog beamformed fading gain $\widehat{\widetilde{h}}_p^{RF_{\nu,\mu}}$ for each path p based on Eq. (23).

V. Secret key rate analysis

It is assumed that the commonly used collective attack is adopted to analyze the SKR, hence the SKR is expressed as

follows [42], [52][4]

$$K_{\text{finite}} = \gamma\left(1-P_B\right)\left[\beta I_{AB} - \chi_{BE} - \triangle\left(N_{\text{privacy}}\right)\right], \quad (51)$$

where γ denotes the fraction of the key extractions relative to the total number of data exchanged by Alice and Bob, while P_B represents the block error rate (BLER) in the reconciliation step. Additionally, I_{AB} is the classical mutual information between Alice and Bob based on their shared correlated data, and χ_{BE} represents the Holevo information, quantifying the information Eve can extract from Bob. Furthermore, the reconciliation efficiency $\beta \in [0,1]$ is defined as [58], [59]

$$\begin{aligned}\beta = \frac{R^{\text{eff}}}{C} &= \frac{R^{\text{eff}}}{\mathbb{E}\left[0.5\log_2\left(1+\text{SNR}^{Rx}\right)\right]} \\ &= \frac{R^{\text{eff}}}{\mathbb{E}\left[0.5\log_2\left(1+1/N_0^{Rx}\right)\right]},\end{aligned} \quad (52)$$

where effective transmission rate R^{eff} is given by $R^{\text{eff}} = \left(1-\frac{M_{cp}}{M}\right)\cdot R$ for OFDM transmission and $R^{\text{eff}} = \left(1-\frac{M_{cp}}{MN}\right)\cdot R$ for OTFS, while R is the coding rate, and C is the one-dimensional Shannon capacity [60], [61]. Additionally, the receive SNR after equalization at the receivers is given by $\text{SNR}^{Rx} = 1/N_0^{Rx} = 1/N_0\Upsilon$. The noise variance N_0^{Rx} equals to $\frac{\left\|\overline{\mathbf{W}}_{\varrho,n}^{Rx,BB}[:,n_s^{FD}]\right\|^2 N_0}{\|\overline{\varsigma}_n^{\varrho}\|^2}$ and $\frac{\left\|\widetilde{\mathbf{W}}_{\varrho}^{Rx,BB}[:,n_s^{DD}]\right\|^2 N_0}{\left\|\overline{\vartheta}^{\varrho}\right\|^2}$ based on Eq. (33) and Eq. (34), when FD-SVD of OFDM and DD-SVD of OTFS receivers are used, respectively, and the corresponding coefficient Υ equals to $\frac{\|\overline{\varsigma}_n^{\varrho}\|^2}{\left\|\overline{\mathbf{W}}_{\varrho,n}^{Rx,BB}[:,n_s^{FD}]\right\|^2}$, and $\frac{\left\|\overline{\vartheta}^{\varrho}\right\|^2}{\left\|\widetilde{\mathbf{W}}_{\varrho}^{Rx,BB}[:,n_s^{DD}]\right\|^2}$.

Firstly, the mutual information between Alice and Bob can be obtained as follows [42]:

$$\begin{aligned}I_{AB} =& \frac{1}{2}\log_2\left[1+\frac{\eta T\Upsilon V_s}{\eta T V_0 + \eta\left(1-T\right)+\left(1-\eta\right)S}\right] \\ =& \frac{1}{2}\log_2\left[\frac{\eta T(\Upsilon V_s + V_0)+\eta\left(1-T\right)+\left(1-\eta\right)S}{\eta T V_0 + \eta\left(1-T\right)+\left(1-\eta\right)S}\right],\end{aligned} \quad (53)$$

where η represents the detection efficiency and S stands for the variance of the trusted detector's noise [15], while $T = 10^{-\alpha\mathfrak{L}/10}$ represents the distance-dependent path loss, where α and $\mathfrak{L}$ represent the attenuation and distance between Alice and Bob, respectively. Furthermore, V_s and V_0 represent the variance of the Gaussian signal and the thermal noise used in the modulator of CV-QKD. Note that we can rewrite $V_s' = \Upsilon V_s$ and $V_A' = V_s' + V_0$, since V_s is adjustable in order to match the required SNR at receiver's side by compensating the effect of fading channel gain Υ and loss T.

Secondly, the Holevo information between Bob and Eve can be calculated as follows [59], [62]

$$\chi_{BE} = S(\rho_{AB}) - S\big(\rho_{A|B}\big), \quad (54)$$

where $S(\cdot)$ is the von Neumann entropy defined in [59], [62]. Hence, the Holevo information can be calculated as

$$\chi_{BE} = G\left(\upsilon_1\right) + G\left(\upsilon_2\right) - G\left(\upsilon_3\right), \quad (55)$$

where υ_1, υ_2 and υ_3 are symplectic eigenvalues of ρ_{AB} and $\rho_{A|B}$ in Eq. (55), and $G(*) = \left(\frac{*+1}{2}\right)\cdot\log_2\left(\frac{*+1}{2}\right) - \left(\frac{*-1}{2}\right)\cdot\log_2\left(\frac{*-1}{2}\right)$. After substituting Eq. (53) and Eq. (55) into Eq. (51), the corresponding SKR can be obtained.

TABLE III: Simulation parameters.

Parameter	Symbol	Value
Parameters for OFDM/OTFS		
The number of subcarrier	M	64
The number of symbol	N	16
Subcarrier spacing	Δf	2 MHz
Carrier frequency	f_c	15 THz
Maximum delay	τ_{max}	20 ns
Speed	v	0,30 mph
Parameters for MIMO		
The number of transmitter antennas	N_{Tx}	1,4,8
The number of receiver antennas	N_{Rx}	1,4,8
The number of data stream	N_s	1
Parameters for LDPC		
Coding rate	R	0.5
Code length	N_{FEC}	1024
Parameters for the QuC		
Ricean factor	K	0 dB
Atmospheric loss	α	50 dB/km
Maximum TDL	$L = \lceil\tau_{max}M\Delta f\rceil$	3
CP length	M_{cp}	$L+1$
Total paths	P	L

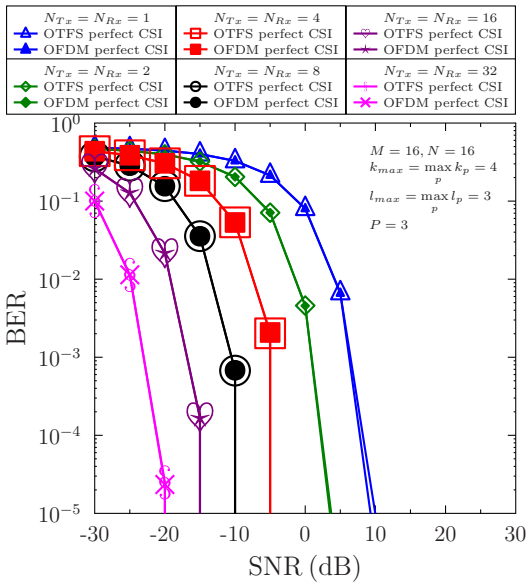
VI. Performance Analysis of Hybrid Beamforming-Assisted Systems

In this section, a comparison between HBF-assisted OFDM and OTFS systems in classical communications is conducted, followed by a comprehensive parametric study of both OFDM and OTFS based THz CV-QKD systems. Explicitly, firstly the bit error rate (BER) performance comparisons are presented for both OFDM and OTFS based multicarrier-based systems associated with a MIMO dimension of $N_{Tx}\times N_{Rx}$ in classical communications. Then, our BLER performance comparisons are presented for different multicarrier-based CV-QKD quantum transmission systems associated with a vehicle velocity v and MIMO dimension $N_{Tx}\times N_{Rx}$. Moreover, the SKR versus distance as a key performance indicator will be analyzed. The simulation parameters are summarized in Table III, which are determined based on key studies in the literature [15], [19], [42], [43], [63], [64].

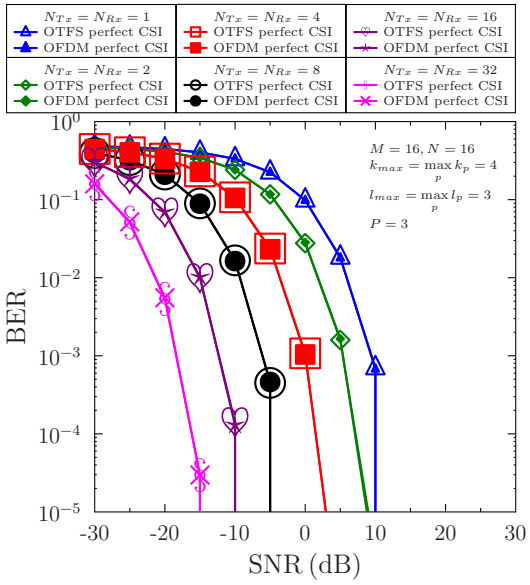
A. OFDM vs. OTFS in Classical Communication

Fig. 6 portrays our BER performance comparison between HBF assisted MIMO OFDM and OTFS systems in classical communications with perfect CSI under different MIMO sizes in mobile scenarios. To elaborate, firstly, it is demonstrated in Fig. 6 that the BER of OFDM is comparable to that of OTFS in general due to the idealistic dominating beamforming gain

[4]Note that the so-called collective attack represents the strongest possible attack [53], where Eve having an unlimited computational capability applies an optimal collective measurement to the entire set of stored ancilla after the key distribution procedure. However, it is also possible to consider the effect of eavesdropping on the SKR, where there is a realistic lossy quantum channel between Eve and the target of eavesdropping [21], [54]. Alternatively, the effect of imperfect quantum memory may also be considered [55], etc. On the other hand, the issue of beam misalignment would have a grave impact on the transmission performance [56], [57], thus may degrade the SKR.

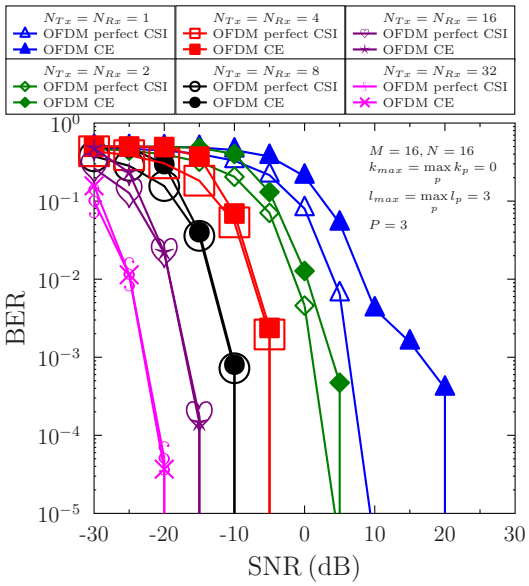


(a)

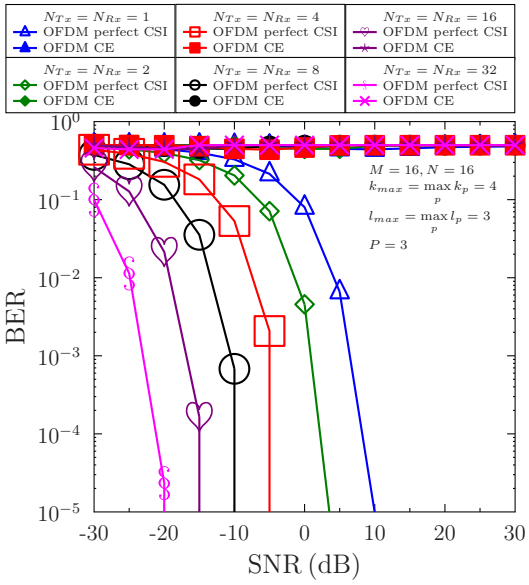


(b)

Fig. 6: Performance comparison between **HBF assisted MIMO OFDM and OTFS systems in classical communications with perfect CSI** and with different MIMO sizes in **mobile** scenario ($k_{max} = \max_p k_p = 4$), where $M = 16$ and $N = 16$ are used and we have: (a) K=6 dB, P=3, (b) K=-6 dB, P=3.



(a)



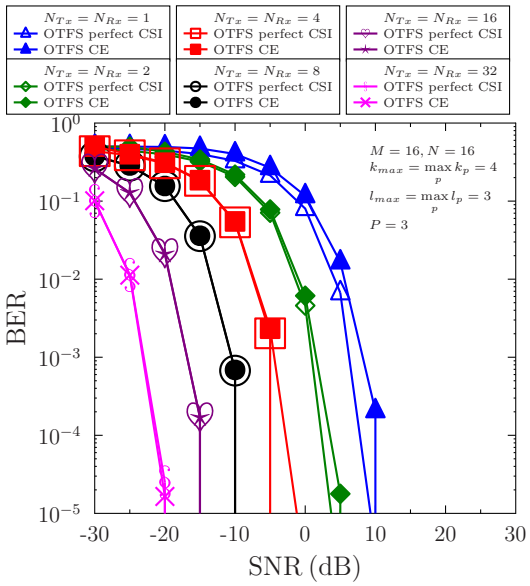
(b)

Fig. 7: Performance comparison between **HBF assisted MIMO OFDM systems with both perfect and estimated CSI** and with different MIMO sizes in both **stationary** and **mobile** scenarios, where $M = 16$ and $N = 16$ are used and we have: (a) K=6 dB, $k_{max} = \max_p k_p = 0$, (b)K=6 dB, $k_{max} = \max_p k_p = 4$.

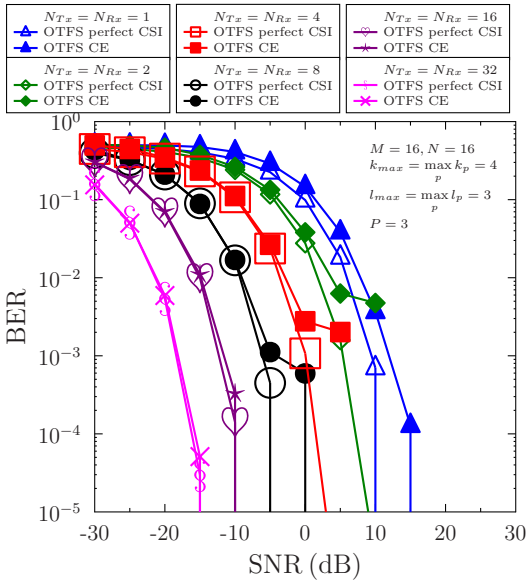
gleaned from perfect CSI. Secondly, it can be observed by comparing Fig. 6(a) and Fig. 6(b) that the BER performance results of both OFDM and OTFS are improved, as the Ricean K factor increases.

Fig. 7 portrays our comparison between HBF assisted MIMO OFDM systems with both perfect and estimated CSI based on Algorithm 1, where different MIMO sizes are investigated in both stationary and mobile scenarios. It is demonstrated by Fig. 7(a) that the BER performance with estimated CSI gradually approaches to that with perfect CSI upon increasing the MIMO size from 1×1 to 32×32 in stationary scenarios for $K = 6$ dB, since the channel estimation of MIMO OFDM is accurate in time-invariant channels. By contrast, the BER results of estimated CSI seen in Fig. 7(b) exhibits irreducible error floors, regardless of the value of Ricean K and the number of antennas. This is due to the fact that in mobile scenarios, the TF-domain channel estimation for OFDM suffers from the time-varying fluctuation of fading channels, where the inter-channel interference prevents the systems from extracting accurate CSI.

In contrast to the channel estimation performance illustrated in Fig. 7, HBF assisted MIMO OTFS using the proposed DD-



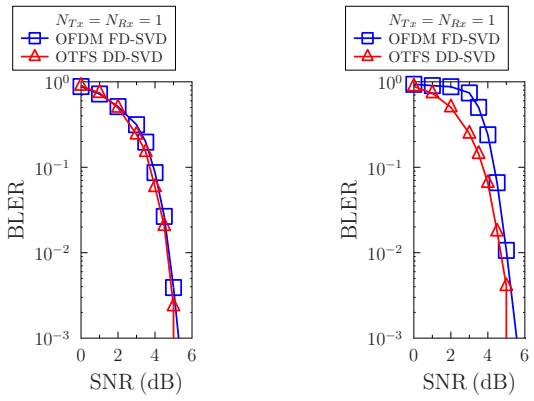
(a)



(b)

Fig. 8: Performance comparison between **HBF assisted MIMO OTFS systems with both perfect and estimated CSI** and with different MIMO sizes in **mobile** scenario ($k_{max} = \max_p k_p = 4$), where $M = 16$ and $N = 16$ are used and we have: (a) K=6 dB, P=3, (b) K=-6 dB, P=3.

domain channel estimation algorithm does not suffer from error floors, as seen in Fig. 8. Explicitly, it is demonstrated in Fig. 8 that the BER associated with estimated channel CSI based on Algorithm 2 approaches the performance of perfect channel CSI even in mobile scenarios for both high Ricean $K = 6$ dB and low Ricean $K = -6$ dB. This is a benefit of the fact that OTFS transforms the time-varying frequency-selective fading in the TF domain into quasi-static fading in the DD domain, which once again makes channel estimation trivial and accurate even in high-mobility scenarios.



(a) (b)

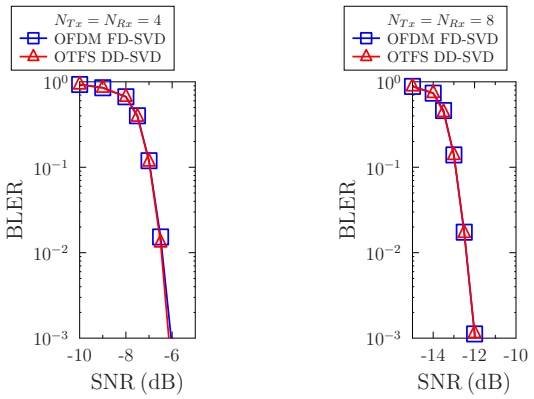
Fig. 9: Performance comparison between **SISO OFDM and OTFS-LDPC CV-QKD systems with perfect CSI** in both (a) **stationary** ($v = 0$ mph) and (b) **mobile** ($v = 30$ mph) scenarios, where $M = 64$ and $N = 16$ are used.

B. OFDM vs. OTFS in CV-QKD

Fig. 9 provides our performance comparison between the OFDM and OTFS schemes employed by our LDPC-aided CV-QKD systems relying on idealistic perfect CSI, where the user velocity is set to $v = 0$ m/s for time-invariant fading and $v = 30$ mph for time-varying fading, respectively. Fig. 9 (a) demonstrates that both the detectors of the OFDM FD-SVD and OTFS DD-SVD based CV-QKD systems achieve a comparable performance in stationary scenario, which is expected in the absence of doubly selective fading. However, Fig. 9 (b) shows that in a mobile scenario associated with a user speed of $v = 30$ mph, the OTFS DD-SVD based CV-QKD system outperforms the OFDM FD-SVD based system in time-varying THz channels.

Fig. 10 illustrates the effect of the MIMO size $N_{Tx} \times N_{Rx}$ on the BLER performance in a mobile (v=30 mph) scenario, where idealistic perfect CSI is assumed. Firstly, it is demonstrated that the OFDM FD-SVD based CV-QKD system achieves the same performance as the OTFS DD-SVD based system even in mobile cases, since the beamforming gain obtained by our MIMO assists in mitigating the gap between OTFS and OFDM observed in SISO case, as shown in Fig.9 (b). Secondly, Fig. 10 demonstrates that the BLER performance improves for both the OTFS and OFDM detectors, as the MIMO size increases. Specifically, it can be observed from Fig. 10(a) and (b) that the SNR required for a BLER of 10^{-1} is reduced from -6.9 dB to -12.8 dB with the increase of MIMO size from 4 to 8.

To analyze the impact of MIMO dimension on the SKR, the parameter pair of BLER and β, denoted by (BLER, β), are summarized in Table IV for both stationary and mobile scenarios. Based on this, Fig. 11 portrays our SKR versus distance comparison between our MIMO OFDM and OTFS LDPC-aided systems using different detectors and MIMO sizes in both stationary and mobile scenarios. The modulation variance is adjusted to its optimal value, following the approach in [65]. The remaining parameters are as follows [15], [19]:



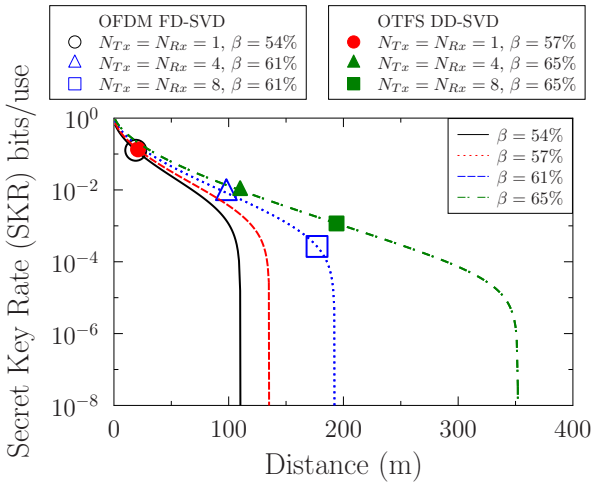
(a) (b)

Fig. 10: Performance comparison between **MIMO OFDM and OTFS-LDPC systems with perfect CSI** with different MIMO size in **mobile** scenario ($v = 30$ mph), where $M = 64$ and $N = 16$ are used and we have: (a) $N_{Tx} = N_{Rx} = 4$, (b) $N_{Tx} = N_{Rx} = 8$.

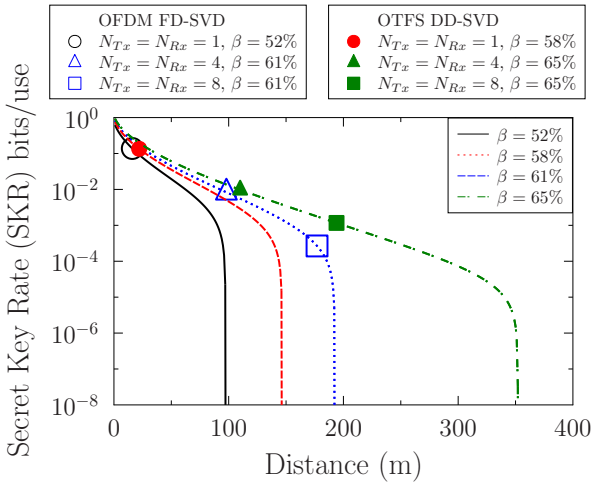
TABLE IV: Reconciliation efficiency comparison of different detection methods used in OFDM/OTFS CV-QKD system under different M and $N_{Tx} \times N_{Rx}$. The reconciliation efficiencies are calculated from Eq. (52) at the BLER threshold that equals to 0.1, together with the corresponding SNRs. Note that both the stationary and mobile scenarios are considered with $v = 0, 30$ mph.

	$N_{Tx} \times N_{Tx}$	OFDM FD-SVD		OTFS DD-SVDE	
		SNR(dB)	$\beta(\%)$	SNR(dB)	$\beta(\%)$
$v =$ 0 mph	1×1	3.85	54.17	3.75	57.44
	4×4	-6.9	60.95	-6.9	65.08
	8×8	-12.8	61.28	-12.8	65.38
$v =$ 30 mph	1×1	4.4	52.30	3.75	57.80
	4×4	-6.9	60.93	-6.9	65.08
	8×8	-12.8	61.44	-12.8	65.23

atmospheric loss $\alpha = 50$ dB/km; room temperature $T_e = 296$ K; detector efficiency $\eta = 0.98$; detector's noise variance $S = 1$; finite-size factor $N_{\text{privacy}} = 10^{12}$. In Fig. 11 (a), there are four asymptotic theoretical SKR curves associated with different reconciliation efficiencies, which are 54%, 57%, 61% and 65%, respectively. Firstly, Fig. 11 (a) demonstrates that in a stationary scenario and in the face of perfect CSI, the OFDM and OTFS-based systems achieve comparable SKR performance in the SISO case. However, in the MIMO case, longer secure transmission distance is achieved by the OTFS-based CV-QKD system than by its OFDM counterpart, since the OTFS-based CV-QKD system associated with frame-based CP overhead can provide higher reconciliation efficiencies than its OFDM counterpart, which can be seen in Table IV. Secondly, Fig. 11 (a) also confirms that the increased MIMO beamforming gain attained is capable of increasing the secure transmission distance for both OFDM and OTFS based CV-QKD. More explicitly, upon increasing the antenna size from 1×1, 4×4, 8×8, the secure transmission distance of our OTFS-based system can be extended from 20 meters (red filled circle), to 120 meters (green filled triangle) and 190 meters



(a)



(b)

Fig. 11: The SKR versus distance comparison between **MIMO OFDM and OTFS-LDPC systems with perfect CSI** using different detections and different MIMO sizes with BLER equals to 10^{-1} in Table IV, where $M = 64$, $N = 16$, $f_c = 15$ THz, $N_{\text{FEC}} = 1024$ and $R = 0.5$ are used in the following scenarios: (a) $v = 0$ mph, (b) $v = 30$ mph.

(green filled square), respectively, whereas the corresponding secure transmission distance of our OFDM system can be extended from 20 meters (black circle), to 100 meters (blue triangle) and 170 meters (blue square), respectively.

Furthermore, in Fig. 11(b), there are four asymptotic theoretical SKR curves having different reconciliation efficiencies defined in Eq. (52), which are 52%, 58%, 61% and 65%, respectively. Similar conclusions can be made in doubly selective THz fading channels as from Fig. 11(a). More explicitly, the secure transmission distance of our OTFS-based system is around 20 meters (red filled circle), 120 meters (green filled triangle) and 190 meters (green filled square) in 1×1, 4×4, 8×8 antenna settings, respectively. By contrast, the corresponding secure transmission distance of our OFDM system is around 16 meters (black circle), 100 meters (blue triangle) and

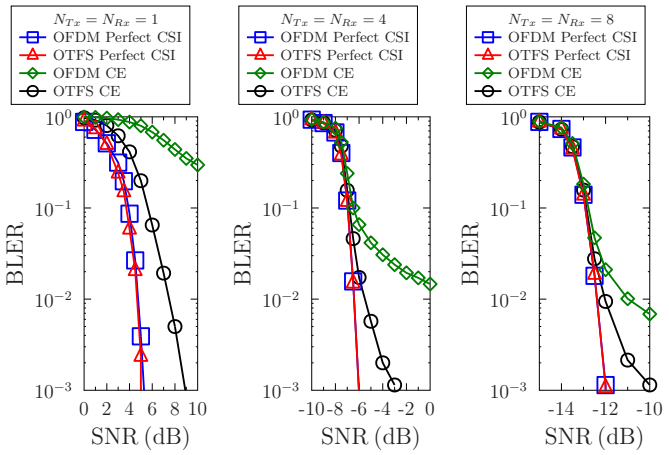


Fig. 12: Performance comparison between **OFDM and OTFS-LDPC CV-QKD systems with estimated CSI** with different MIMO sizes in **stationary** scenarios, where $M = 64$ and $N = 16$ are used and we have: (a) $N_{Tx} = N_{Rx} = 1$, (b) $N_{Tx} = N_{Rx} = 4$, (c) $N_{Tx} = N_{Rx} = 8$.

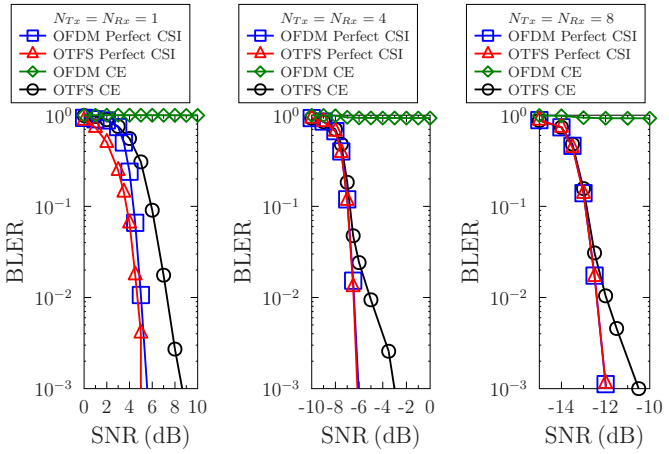


Fig. 13: Performance comparison between **OFDM and OTFS-LDPC CV-QKD systems with estimated CSI** with different MIMO sizes in **mobile** scenarios ($v = 30$ mph), where $M = 64$ and $N = 16$ are used and we have: (a) $N_{Tx} = N_{Rx} = 1$, (b) $N_{Tx} = N_{Rx} = 4$, (c) $N_{Tx} = N_{Rx} = 8$.

170 meters (blue square) in 1×1, 4×4, 8×8 antenna setting, respectively. To further investigate the effect of channel estimation on the BLER performance, Fig. 12 portrays our BLER performance comparison between the OFDM and OTFS schemes employed by our LDPC-aided CV-QKD system with estimated CSI in a stationary scenario. Fig. 12(a) demonstrates that there is almost no BLER performance gap for OTFS between the estimated CSI and perfect CSI SISO case, whilst there is a high BLER floor for OFDM with estimated CSI. Furthermore, the BLER performance of OFDM and OTFS with estimated CSI is gradually improved upon increasing the MIMO sizes from 1×1 to 8×8 as evidenced by Fig. 12(b) and (c).

By contrast, Fig. 13 presents our performance comparison between MIMO OFDM and OTFS based CV-QKD systems with estimated CSI in mobile scenarios. It is observed that the performance of OTFS with estimated CSI exhibits the same trend as that in Fig. 12, where the corresponding BLER performance of OTFS with estimated CSI is gradually improved when increasing the MIMO sizes. Therefore, similar reconciliation efficiencies and SKR versus distance can be achieved for OTFS based systems with estimated CSI as that with perfect CSI in both stationary and mobile scenarios. However, the OFDM system with estimated CSI does not perform adequately in mobile cases.

VII. Conclusions

Multi-carrier OFDM and OTFS based LDPC assisted CV-QKD reconciliation schemes have been designed and studied in the face of time-varying and frequency-selective THz scenarios, where **HBF** were developed to improve the quantum transmission distance attained in the face of severe THz path loss. **Firstly**, it was demonstrated that the OFDM FD-SVD based CV-QKD system with perfect CSI achieves comparable BLER performance to the OTFS DD-SVD based system even in mobile ($v = 30$ mph) scenarios, since the beamforming gain mitigates the gap between OTFS and OFDM observed in SISO cases, provided that perfect CSI is available at both the transmitter and receiver. **Secondly**, it was demonstrated that the BLER performance is improved upon increasing the MIMO size, thanks to the improved beamforming gain achieved by the MIMO OFDM/OTFS scheme proposed for quantum transmission. **Thirdly**, an SKR versus distance performance comparison was conducted. It was demonstrated that the OTFS-based system associated with frame-based CP overhead offers higher SKR and longer secure transmission distance than the OFDM-based system in both stationary and mobile ($v = 30$ mph) scenarios. Moreover, increasing the MIMO size enhances the secure transmission distance for both the OFDM- and OTFS-based systems. **Lastly**, the effect of channel estimation on the OFDM- and OTFS-based systems was investigated. It was demonstrated that the OTFS system with estimated CSI performs similarly to that with perfect CSI in both stationary and mobile scenarios. Therefore, similar reconciliation efficiencies and SKR vs. distance performance can be achieved for OTFS based CV-QKD systems with estimated CSI as that with perfect CSI. However, the OFDM-based system with estimated CSI cannot achieve adequate SKR and secure distance for CV-QKD in mobile cases due to its irreducible error floors in BLER.

For future research, we may harness advanced fully analog stacked intelligent metasurface (SIM) aided MIMO schemes in our multicarrier CV-QKD scenarios. They provide improved spectral efficiency at a low hardware complexity, while mitigating the effects of frequency-selective multi-path propagation with the aid of programmable multi-path propagation within the SIM itself [66]. Furthermore, in classic performance evaluation it is typically assumed that the receiver is exposed to far-field propagation in form of plane waves. By contrast, in the near-field spherical propagation takes place. Hence, near-field THz propagation modelling has been investigated in

[67], [68]. Since the corresponding Rayleigh distance grows with the array size, as well as with the reduction of the wavelength, this has been investigated in [69], [70]. Therefore, it is worthwhile considering near-field THz CV-QKD systems, since the transmission distance is limited in the THz bands.

REFERENCES

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[2] 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. Tutor.*, vol. 21, no. 1, pp. 881–919, 2019.

[3] 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. Tutor.*, vol. 24, no. 2, pp. 839–894, 2022.

[4] Z. Wang, R. Malaney, and J. Green, "Inter-satellite quantum key distribution at Terahertz frequencies," in *Pro. IEEE Int. Conf. Commun. (ICC)*, 2019, pp. 1–7.

[5] X. You, C.-X. Wang, J. Huang, X. Gao, Z. Zhang, M. Wang, Y. Huang, C. Zhang, Y. Jiang, J. Wang *et al.*, "Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts," *Sci. China Inf. Sci.*, vol. 64, no. 1, pp. 1–74, 2021.

[6] M. Fujiwara, R. Nojima, T. Tsurumaru, S. Moriai, M. Takeoka, and M. Sasaki, "Long-term secure distributed storage using quantum key distribution network with third-party verification," *IEEE Trans. Quant. Eng.*, vol. 3, pp. 1–11, 2022.

[7] A. Stanco, F. B. L. Santagiustina, L. Calderaro, M. Avesani, T. Bertapelle, D. Dequal, G. Vallone, and P. Villoresi, "Versatile and concurrent FPGA-based architecture for practical quantum communication systems," *IEEE Trans. Quant. Eng.*, vol. 3, pp. 1–8, 2022.

[8] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, no. 2, pp. 621–669, 2012.

[9] Y.-C. Zhang, Z. Li, S. Yu, W. Gu, X. Peng, and H. Guo, "Continuous-variable measurement-device-independent quantum key distribution using squeezed states," *Phys. Rev. A*, vol. 90, no. 5, p. 052325, 2014.

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

[11] 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.

[12] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching," *Phys. Rev. Lett.*, vol. 93, no. 17, p. 170504, 2004.

[13] 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, 2021.

[14] H. Chen, H. Sarieddeen, T. Ballal, H. Wymeersch, M.-S. Alouini, and T. Y. Al-Naffouri, "A tutorial on Terahertz-band localization for 6G communication systems," *IEEE Commun. Surv. Tutor.*, vol. 24, no. 3, pp. 1780–1815, 2022.

[15] 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, 2020.

[16] 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. Express*, vol. 28, no. 22, pp. 32 386–32 402, 2020.

[17] X. Liu, C. Zhu, N. Chen, and C. Pei, "Practical aspects of Terahertz wireless quantum key distribution in indoor environments," *Quant. Inf. Process.*, vol. 17, no. 11, pp. 1–20, 2018.

[18] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, "Quantum cryptography approaching the classical limit," *Phys. Rev. Lett.*, vol. 105, no. 11, pp. 1–8, 2010.

[19] 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, 2021.

[20] 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, 2022.

[21] N. K. Kundu, M. R. McKay, A. Conti, R. K. Mallik, and M. Z. Win, "MIMO Terahertz quantum key distribution under restricted eavesdropping," *IEEE Trans. Quant. Eng.*, vol. 4, pp. 1–15, 2023.

[22] M. Zhang, S. Pirandola, and K. Delfanazari, "Millimeter-waves to Terahertz SISO and MIMO continuous variable quantum key distribution," *IEEE Trans. Quant. Eng.*, vol. 4, pp. 1–10, 2023.

[23] L. Gyongyosi and S. Imre, "Adaptive multicarrier quadrature division modulation for long-distance continuous-variable quantum key distribution," *Quant. Inf. Comput. XII*, vol. 9123, no. May 2014, p. 912307, 2014.

[24] S. Bahrani, M. Razavi, and J. A. Salehi, "Orthogonal frequency-division multiplexed quantum key distribution," *J. Lightw. Technol.*, vol. 33, no. 23, pp. 4687–4698, 2015.

[25] L. Gyongyosi, "Diversity extraction for multicarrier continuous-variable quantum key distribution," in *European Sig. Process. Conf.*, vol. 2016-Novem. EURASIP, 2016, pp. 478–482.

[26] W. Zhao, Y. Guo, D. Huang, and L. Zhang, "Continuous-variable quantum key distribution with orthogonal frequency division multiplexing modulation," *Int. J. Theoret. Phys.*, vol. 57, no. 10, pp. 2956–2967, 2018.

[27] H. Zhang, Y. Mao, D. Huang, J. Li, L. Zhang, and Y. Guo, "Security analysis of orthogonal-frequency-division-multiplexing-based continuous-variable quantum key distribution with imperfect modulation," *Physical Review A*, vol. 97, no. 5, pp. 1–9, 2018.

[28] W. Zhao, Q. Liao, D. Huang, and Y. Guo, "Performance analysis of the satellite-to-ground continuous-variable quantum key distribution with orthogonal frequency division multiplexed modulation," *Quant. Inf. Process.*, vol. 18, no. 1, pp. 1–22, 2019.

[29] L. Gyongyosi, "Singular value decomposition assisted multicarrier continuous-variable quantum key distribution," *Theoret. Comput. Sci.*, vol. 801, pp. 35–63, 2020.

[30] 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.

[31] H. Wang, Y. Pan, Y. Shao, Y. Pi, T. Ye, Y. Li, T. Zhang, J. Liu, J. Yang, L. Ma, W. Huang, and B. Xu, "Performance analysis for OFDM-based multi-carrier continuous-variable quantum key distribution with an arbitrary modulation protocol," *Optics Express*, vol. 31, no. 4, p. 5577, 2023.

[32] L. Gyongyosi and S. Imre, "Secret key rates of free-space optical continuous-variable quantum key distribution," *Int. J. Commun. Syst.*, vol. 32, no. 18, pp. 1–10, 2019.

[33] C. Xu, L. Xiang, J. An, C. Dong, S. Sugiura, R. G. Maunder, L.-L. Yang, and L. Hanzo, "OTFS-aided RIS-assisted SAGIN systems outperform their OFDM counterparts in doubly selective high-Doppler scenarios," *IEEE Internet Things J.*, vol. 10, no. 1, pp. 682–703, 2023.

[34] R. Hadani, S. Rakib, M. Tsatsanis, A. Monk, A. J. Goldsmith, A. F. Molisch, and R. Calderbank, "Orthogonal time frequency space modulation," in *2017 IEEE Wireless Commun. Network. Conf. (WCNC)*. IEEE, 2017, pp. 1–6.

[35] Z. Wei, W. Yuan, S. Li, J. Yuan, G. Bharatula, R. Hadani, and L. Hanzo, "Orthogonal time-frequency space modulation: A promising next-generation waveform," *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 136–144, 2021.

[36] S. K. Mohammed, "Derivation of OTFS modulation from first principles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 8, pp. 7619–7636, 2021.

[37] C. Xu, X. Zhang, P. Petropoulos, S. Sugiura, R. G. Maunder, L.-L. Yang, Z. Wang, J. Yuan, H. Haas, and L. Hanzo, "Optical OTFS is capable of improving the bandwidth-, power- and energy-efficiency of optical OFDM," *IEEE Trans. Commun.*, vol. 72, no. 2, pp. 938–953, 2024.

[38] C. Xu, L. Xiang, S. Sugiura, R. G. Maunder, L.-L. Yang, D. Niyato, G. Y. Li, R. Schober, and L. Hanzo, "Noncoherent orthogonal time frequency space modulation," *IEEE Trans. Wireless Commun.*, vol. 23, no. 8, pp. 10 072–10 090, 2024.

[39] Z. Sui, H. Zhang, Y. Xin, T. Bao, L.-L. Yang, and L. Hanzo, "Low complexity detection of spatial modulation aided OTFS in doubly-selective channels," *IEEE Trans. Veh. Technol.*, vol. 72, no. 10, pp. 13 746–13 751, 2023.

[40] Z. Sui, H. Zhang, S. Sun, L.-L. Yang, and L. Hanzo, "Space-time shift keying aided OTFS modulation for orthogonal multiple access," *IEEE Trans. Commun.*, vol. 71, no. 12, pp. 7393–7408, 2023.

[41] Z. Sui, S. Yan, H. Zhang, S. Sun, Y. Zeng, L.-L. Yang, and L. Hanzo, "Performance analysis and approximate message passing detection of orthogonal time sequency multiplexing modulation," *IEEE Trans. Wirel. Commun.*, vol. 23, no. 3, pp. 1913–1928, 2024.

[42] X. Liu, C. Xu, S. X. Ng, and L. Hanzo, "OTFS-based CV-QKD systems for doubly selective THz channels," *IEEE Trans. Commun.*, 2025.

[43] X. Liu, C. Xu, Y. Noori, S. X. Ng, and L. Hanzo, "The road to near-capacity CV-QKD reconciliation: An FEC-agnostic design," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 2089–2112, 2024.

[44] C. Xu, L. Xiang, J. An, C. Dong, S. Sugiura, R. G. Maunder, L.-L. Yang, and L. Hanzo, "OTFS-aided RIS-assisted SAGIN systems outperform their OFDM counterparts in doubly selective high-Doppler scenarios," *IEEE Internet Things J.*, vol. 10, no. 1, pp. 682–703, 2022.

[45] B. Ning, Z. Tian, W. Mei, Z. Chen, C. Han, S. Li, J. Yuan, and R. Zhang, "Beamforming technologies for ultra-massive MIMO in Terahertz communications," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 614–658, 2023.

[46] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 77, no. 4, 2008, Articel no. 042325.

[47] Z. Cao, X. Chen, G. Chai, K. Liang, and Y. Yuan, "Rate-adaptive polar-coding-based reconciliation for continuous-variable quantum key distribution at low signal-to-noise ratio," *Phys. Rev. Appl.*, vol. 19, no. 4, 2023, Article no. 044023.

[48] M. Zhang, Y. Dou, Y. Huang, X. Q. Jiang, and Y. Feng, "Improved information reconciliation with systematic polar codes for continuous variable quantum key distribution," *Quant. Inf. Process.*, vol. 20, no. 10, pp. 1–16, 2021.

[49] G. H. Golub and C. Reinsch, "Singular value decomposition and least squares solutions," in *Handbook for Automatic Computation: Volume II: Linear Algebra*. Springer, 1971, pp. 134–151.

[50] E. Angerson, Z. Bai, J. Dongarra, A. Greenbaum, A. McKenney, J. Du Croz, S. Hammarling, J. Demmel, C. Bischof, and D. Sorensen, "LAPACK: A portable linear algebra library for high-performance computers," in *Proc. ACM/IEEE Conf. Supercomput.*, 1990, pp. 2–11.

[51] T. Peken, S. Adiga, R. Tandon, and T. Bose, "Deep learning for SVD and hybrid beamforming," *IEEE Trans. Wirel. Commun.*, vol. 19, no. 10, pp. 6621–6642, 2020.

[52] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, "Quasi-cyclic multi-edge ldpc codes for long-distance quantum cryptography," *NPJ Quant. Inf.*, vol. 4, no. 1, pp. 1–9, 2018.

[53] C. Weedbrook, S. Pirandola, and T. C. Ralph, "Continuous-variable quantum key distribution using thermal states," *Phys. Rev. A: At. Mol. Opt. Phys.*, vol. 86, no. 2, 2012, Article no. 022318.

[54] 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. Appl.*, vol. 14, no. 2, 2020, Article no. 024044.

[55] N. Hosseinidehaj, N. Walk, and T. C. Ralph, "Optimal realistic attacks in continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 99, no. 5, 2019, Article no. 052336.

[56] W. Attaoui, K. Bouraqia, and E. Sabir, "Initial access & beam alignment for mmwave and Terahertz communications," *IEEE Access*, vol. 10, pp. 35 363–35 397, 2022.

[57] V. Petrov, D. Moltchanov, Y. Koucheryavy, and J. M. Jornet, "Capacity and outage of Terahertz communications with user micro-mobility and beam misalignment," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6822–6827, 2020.

[58] C. Zhou, X. Y. Wang, Z. G. Zhang, S. Yu, Z. Y. Chen, and H. Guo, "Rate compatible reconciliation for continuous-variable quantum key distribution using Raptor-like LDPC codes," *Sci. China: Phys., Mech. and Astronomy*, vol. 64, no. 6, 2021, Article no. 260311.

[59] F. Laudenbach, C. Pacher, C. H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-variable quantum key distribution with gaussian modulation—The theory of practical implementations," *Adv. Quant. Technol.*, vol. 1, no. 1, pp. 1–37, 2018.

[60] W. Ryan and S. Lin, *Channel codes: Classical and modern*. Cambridge Univ. Press, 2009.

[61] T. Richardson and R. Urbanke, *Modern coding theory*. Cambridge Uni. Press, 2008.

[62] A. S. Holevo, M. Sohma, and O. Hirota, "Capacity of quantum gaussian channels," *Phys. Rev. A*, vol. 59, no. 3, p. 1820, 1999.

[63] J. Tan and L. Dai, "Wideband channel estimation for THz massive MIMO," *China Commun.*, vol. 18, no. 5, pp. 66–80, 2021.

[64] C. Han and Y. Chen, "Propagation modeling for wireless communications in the Terahertz band," *IEEE Commun. Mag.*, vol. 56, no. 6, pp. 96–101, 2018.

[65] C. Zhou, X. Wang, Y. Zhang, Z. Zhang, S. Yu, and H. Guo, "Continuous-variable quantum key distribution with rateless reconciliation protocol," *Phys. Rev. Appl.*, vol. 12, no. 5, 2019, Article no. 054013.

[66] Z. Li, J. An, and C. Yuen, "Stacked intelligent metasurfaces-enhanced MIMO OFDM wideband communication systems," *arXiv preprint arXiv:2503.00368*, 2025.

[67] D. Bodet, V. Petrov, S. Petrushkevich, and J. M. Jornet, "Sub-Terahertz near field channel measurements and analysis with beamforming and Bessel beams," *Sci. Rep.*, vol. 14, no. 1, 2024, Article no. 19675.

[68] V. Petrov, D. Moltchanov, and J. M. Jornet, "Accurate channel model for near field Terahertz communications beyond 6G," in *Proc. IEEE 25th Int. Workshop on Signal Process. Adv. Wirel. Commun. (SPAWC)*. IEEE, 2024, pp. 781–785.

[69] C. Han, Y. Chen, L. Yan, Z. Chen, and L. Dai, "Cross far-and near-field wireless communications in Terahertz ultra-large antenna array systems," *IEEE Wirel. Commun.*, vol. 31, no. 3, pp. 148–154, 2024.

[70] Y. Wang, S. Sun, and C. Han, "Far-and near-field channel measurements and characterization in the Terahertz band using a virtual antenna array," *IEEE Commun. Lett.*, vol. 28, no. 5, pp. 1186–1190, 2024.