OTFS-Based CV-QKD Systems for Doubly Selective THz Channels

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

***Abstract*—The feasibility of continuous variable quantum key distribution (CV-QKD) is considered in the Terahertz (THz) band, experiencing time-varying and frequency-selective fading. Advanced multi-carrier modulation is required for improving the secret key rate (SKR). However, the hostile quantum channel requires powerful classical channel coding schemes for maintaining an adequate reconciliation performance. Against this background, for the first time in the open literature, we propose a multi-carrier quantum transmission regime that incorporates both orthogonal frequency division multiplexing (OFDM) and orthogonal time frequency space (OTFS) transmission over doubly selective fading THz channels. Furthermore, we propose a modified multi-dimensional reconciliation algorithm for CV-QKD, facilitating the integration of OFDM/OTFS quantum transmission with low-density parity check (LDPC) coded key reconciliation. Moreover, we harness multiple-input multiple-output (MIMO) beamforming for mitigating the severe THz path loss. Our SKR analysis results demonstrate that the proposed OTFS-based and LDPC-assisted CV-QKD system is capable of outperforming its OFDM counterpart in mobile wireless scenarios. Moreover, we also demonstrate that increasing the MIMO dimension reduces the transmission power required for achieving the secure transmission distance target.**

***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), Terahertz (THz), secret key rate (SKR).**

I. Introduction

Quantum key distribution (QKD) is capable of supporting ultimate information security in communication systems [1]–[8]. More explicitly, a QKD scheme instructs both the transmitter (Alice) and the receiver (Bob) to encrypt their confidential messages using their reconciled keys generated at both sides. This so-called QKD-based cryptosystem possesses the capability of eavesdropping detection based on the no-cloning theorem and Heisenberg's uncertainty principle. Recently, continuous variable QKD (CV-QKD) has attracted substantial attention from both academia and industry. For CV-QKD either homodyne or heterodyne detection is utilized, which has convenient compatibility with the operational communication network infrastructure [2], [9]. As a further benefit, CV-QKD is capable of providing a higher key rate [10]–[13] than its discrete variable QKD (DV-QKD) counterpart, since its associated homodyne or heterodyne detection offers the prospect of high detection efficiency. This is beneficial, because a wide range of quantum-safe services such as banking, healthcare and government affairs might be supported not only in the ideal infinite block-length scenario [14], but also in the finite-block-length regime [15].

Moreover, to meet the explosive data-rate demand of next-generation communication systems, the substantial available bandwidth of the Terahertz (THz) range has motivated a lot of research efforts [16], [17]. Furthermore, compared to free-space optical (FSO) links, THz transmission is more robust to the presence of dust, fog and atmospheric turbulence, but its particle-like behaviour is less pronounced. Nonetheless, the feasibility of CV-QKD has also been considered in the THz band [18]–[21]. Furthermore, in order to improve the secure transmission distance limited by the high path loss of the THz band, multiple-input multiple-output (MIMO) techniques have been adopted in [22]–[25]. Moreover, the orthogonal frequency division multiplexing (OFDM) waveform also used in 4G and 5G, has been introduced to support CV-QKD in the THz band for the sake of mitigating the detrimental multipath effect of wireless channels [26]–[35].

Table I summarizes the state-of-the-art CV-QKD schemes, with a focus on using OFDM to improve the secret key rate (SKR) in wireless THz channels. Briefly, an OFDM-based CV-QKD scheme was proposed for optical fibre transmission in [26]–[30], [32], where both the security level and the SKR were investigated. Moreover, realistic imperfect modulation was considered in [30], while a singular value decomposition based method was invoked for the reliable simultaneous transmission of multiple data streams in [32]. It was demonstrated in [32] that both the maximum key rate attained at a specific distance and the overall maximum secure transmission distance can be improved with the aid of the OFDM technique. Secondly, an OFDM-based CV-QKD FSO link was established in [31], which took into account the impact of scintillation intensity, phase noise and the number of subcarriers on the system performance. As a further advance, the authors of [35] analyzed the performance of CV-QKD over FSO quantum channels with a focus on the theoretical derivation of the SKR. Thirdly, the SKR performance of an OFDM-based CV-QKD scheme operating in the THz band was analyzed both in indoor environments and in inter-satellite links in [33], where the effect of sub-channel crosstalk caused by the imperfection of optical devices was considered as well. Finally, a realistic imperfect modulation scenario was

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**	[34]	[33]	[32]	[31]	[30]	[29]	[28]	[27]	[26]	[35]	[18]	[20]	[22]	[25]
Optical fibre		✓		✓		✓	✓	✓	✓	✓					
FSO					✓						✓				
Terahertz	✓		✓									✓	✓	✓	✓
SISO	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
MIMO	✓													✓	✓
Beamforming	✓													✓	✓
Frequency selective	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				
Time-invariant fading	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Time-varying fading	✓														
OFDM	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				
OTFS	✓														

considered for OFDM-based CV-QKD in [34][1]. A specific modulation noise model was proposed for OFDM-based CV-QKD and the authors investigated the effect of both Gaussian and discrete modulation cases. It was demonstrated in [34] that the asymptotic SKR can be improved by increasing the number of sub-carriers even for realistic discrete modulations.

However, all of the OFDM aided CV-QKD schemes investigated operate based on the assumption of time-invariant fading channels in stationary scenarios. In reality, wireless users move freely and their mobility leads to the Doppler effect. The real-world time-varying frequency-selective fading channels destroy OFDM's subcarrier orthogonality and degrade the OFDM performance. Yet these deleterious effects have not been investigated in the context of CV-QKD. As a remedy, a new waveform termed as orthogonal time frequency space (OTFS) modulation has been recently proposed for classical wireless communication in the face of time-varying and frequency selective fading channels [36]–[41]. More explicitly, the OTFS scheme transforms the time-varying frequency-selective fading experienced in the time-frequency (TF) domain into quasi-static flat fading in the delay-Doppler (DD) domain. As a result, channel estimation in the DD domain requires less frequent updates, while OFDM's intercarrier interference (ICI) caused by user mobility is also mitigated. At the time of writing, the novel OTFS schemes have not been harnessed in CV-QKD systems.

Against this background, for the first time in the open literature, we propose a multi-carrier framework for supporting both OFDM and OTFS aided low density parity-check (LDPC) coded CV-QKD reconciliation systems. Time-varying frequency-selective fading, which is a typical high mobility scenario in space-air-ground integrated networks (SAGIN) [2]–[4], [40], is considered for a THz channel, where both single-input single-output (SISO) and MIMO beamforming setups are considered. As demonstrated by Table I, the novel contributions of this work are as follows:

- Firstly, a multi-carrier OFDM based LDPC assisted CV-QKD reconciliation scheme is established and studied. This is different from the existing literature both in terms of the quantum transmission and reconciliation process, which operate in the face of time-varying and frequency-selective THz propagation.
- Secondly, for the first time in the open literature, an OTFS based quantum transmission scheme is proposed for LDPC coded CV-QKD, which is capable of relying on the same multi-carrier infrastructure as its OFDM counterpart, while providing improved performance in the face of time-varying THz scenarios.
- Thirdly, in order to facilitate LDPC assisted CV-QKD reconciliation for both OFDM and OTFS, a new mapping scheme is devised for our post-processing aided multi-dimensional reconciliation (MDR) process, where realistic channel fading is taken into account. This is different from the existing MDR schemes found in the open literature, where a binary-input additive white Gaussian noise (BI-AWGN) based quantum channel is assumed [42].
- Fourthly, in order to improve the quantum transmission distance attained in the face of severe THz path loss, MIMO beamforming is conceived based on statistical channel state information (CSI), where analog beamformers are conceived based on line-of-sight (LoS) propagation without requiring full knowledge of the multipath CSI at the transmitter.
- Finally, our analysis and simulation results demonstrate that the proposed OTFS-based CV-QKD is capable of outperforming its OFDM counterpart in terms of its SKR, when the user mobility is increased. Moreover, our performance results also demonstrate that the proposed MIMO beamforming scheme is capable of improving secure CV-QKD transmission for both OTFS and OFDM.

The rest of this paper is structured as follows. Our SISO OFDM/OTFS CV-QKD system is conceived in Section II, which introduces the CV-QKD system model, OFDM and OTFS quantum transmission as well as the modified MDR for THz fading. The MIMO OFDM/OTFS CV-QKD system is proposed in Section III, which is followed by the SKR analysis in Section IV. Our simulation results are presented in Section V. Finally, our conclusions are offered in Section VI.

Notations: In this paper, bold uppercase $\mathbf{A}$ and lowercase $\mathbf{a}$ represent matrices and vectors, respectively. For matrices, $\mathbf{A}[m,:]$ and $\mathbf{A}[:,n]$ represent the mth row and the nth column of a matrix $\mathbf{A}$, respectively. Moreover, $\mathbf{A}[m,n]$ represents the element at the mth row and nth column of a matrix $\mathbf{A}$. For vectors, $\mathbf{a}[m]$ represents the mth element of a vector $\mathbf{a}$. The operation $(\cdot)^*$ represents the conjugate of a scalar or a vector. The operations $(\cdot)^{-1}$, $(\cdot)^T$ and $(\cdot)^H$ denote the

[1] The imperfect modulation entails the in-phase and quadrature-phase imbalance and intermodulation distortion in [34].

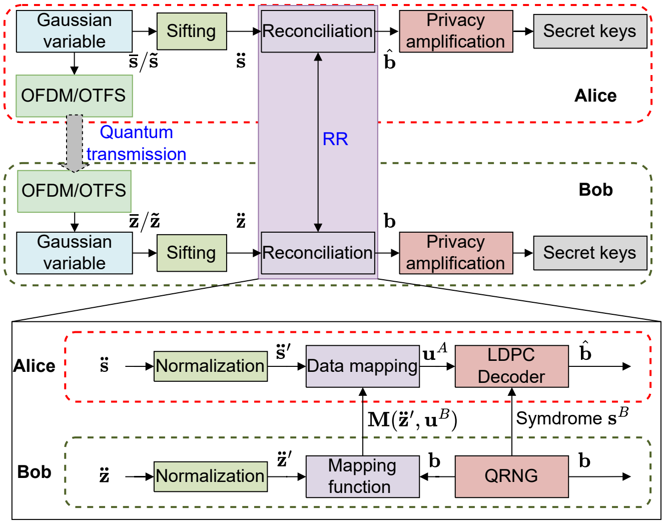


Fig. 1: CV-QKD protocol diagram of OFDM/OTFS LDPC-aided scheme. Note that the reconciliation part is the same as that in [42].

inverse of a matrix, the transpose and Hermitian transpose of a matrix, respectively. $\|\cdot\|$ denotes the Frobenius norm. The operations of $\mathfrak{Re}(\cdot)$ and $\mathfrak{Im}(\cdot)$ take the real and imaginary part of a complex value, respectively. diag $(\mathbf{a})$ represents a square diagonal matrix formed by vector $\mathbf{a}$. rem(a, b) returns the remainder after division of a by b. $\mathbb{E}(\cdot)$ takes the expectation of random variables.

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

In this section, firstly the CV-QKD system model is reviewed. Then the proposed OFDM/OTFS quantum transmission as well as our modified MDR designed for LDPC assisted CV-QKD are introduced. We note that LDPC codes are used by the syndrome-based reconciliation process and it is assumed that the classical transmission is perfect, which is the common assumption in the open literature [42]–[44].

A. CV-QKD System Model

The classic CV-QKD protocol [42] is summarized in Fig. 1, where the reverse reconciliation (RR) process using MDR mapping is highlighted.

More explicitly, firstly, Alice maps the Gaussian distributed random variables $\bar{\mathbf{s}}$ to the frequency-domain (FD) subcarriers of OFDM or $\tilde{\mathbf{s}}$ to the DD of OTFS, which are transmitted with the aid of OFDM/OTFS through wireless THz channels. The random variables received by Bob are firstly equalized in the FD or DD for OFDM and OTFS, respectively, leading to the decision variable of $\bar{\mathbf{z}}$ in the FD or $\tilde{\mathbf{z}}$ in the DD that is equivalent to the noise-contaminated version of the transmitted Gaussian variables. Secondly, in the sifting step[2], Alice and Bob synchronize their preparation and measurement basis, providing input variables for the MDR process as $\ddot{\mathbf{s}}$ at Alice's side and $\ddot{\mathbf{z}}$ at Bob's sides. Thirdly, in the RR step, the MDR mechanism is invoked for mapping the modulated version $\mathbf{u}^B$ of the binary data $\mathbf{b}$ to the normalized random variables $\ddot{\mathbf{z}}'$ after either OFDM or OTFS detection at Bob's side. Alice invokes the agreed MDR function $\mathbf{M}(\ddot{\mathbf{z}}', \mathbf{u}^B)$ for mapping the normalized random variable $\ddot{\mathbf{s}}'$ of the OFDM or OTFS transmitted symbols to $\mathbf{u}^A$, which is the contaminated version of $\mathbf{u}^B$. Then the LDPC syndrome $\mathbf{s}^B$ generated based on the key is sent from Bob to Alice, so that Alice's LDPC decoder can apply error correction to $\mathbf{u}^A$ for mitigating the noise-contamination of the raw quantum data. Finally, privacy amplification is applied for reducing Eve's proability of successfully guessing the key. The detailed MDR process will be elaborated on in Sec. II-C.

B. OFDM/OTFS based quantum transmission

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

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	$y_{n,m}$	$\bar{y}_{n,\overline{m}}$	$\widetilde{y}_{k,l}$

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 via the inverse discrete Fourier transform (IDFT), which can be expressed as

$$\mathbf{s}_n = \mathbf{F}_M^H \bar{\mathbf{s}}_n, \tag{1}$$

where $\mathbf{F}_M \in \mathcal{C}^{M\times M}$ denotes the discrete Fourier transform (DFT) matrix. Meanwhile, the relationship of preparation thermal noise between FD and TD can be represented as $\mathbf{s}_{0n} = \mathbf{F}_M^H \bar{\mathbf{s}}_{0n}$, which is the same as in (1). The received TD signal can be expressed as[3]:

$$\begin{aligned} y_{n,m} =& \sqrt{T}\sum_{l=0}^{L-1} h_{n,m,l} s_{n,<m-l>_M} \\ &+ \sqrt{T}\sum_{l=0}^{L-1} h_{n,m,l} s_{0n,<m-l>_M} + \sqrt{1-T} s_{E n,m}, \end{aligned} \tag{2}$$

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_E represents the additive white Gaussian noise

[2] Note that homodyne detection is used in our proposed scheme, which is different from the heterodyne detection based scheme, since no key sifting process is required. Further related discussions can be found in [2].

[3] We note that the input-output relationship of both (2) and (10) are direct extensions of the beam splitter models found in [18], [22]–[24], [31]–[33], [45], where doubly selective fading is introduced in our system. Furthermore, we will demonstrate in this treatise that given the same beam splitter channel model, the choice of waveforms between OFDM and OTFS as well as their detector designs have significant impact on the SKR.

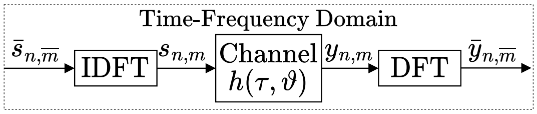

Time-Frequency Domain
$\overline{s}_{n,\overline{m}}$
IDFT
$s_{n,m}$
Channel $h(\tau,\vartheta)$
$y_{n,m}$
DFT
$\overline{y}_{n,\overline{m}}$

Fig. 2: System diagram of OFDM transmission scheme.

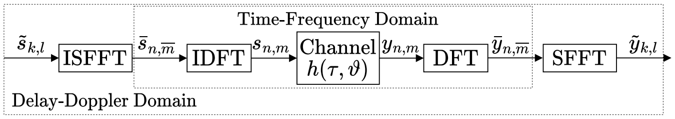


Fig. 3: System diagram of OTFS transmission scheme.

(AWGN) introduced by Eve to extract the key information [22]. Based on (2), the TD matrix form is given by

$$\mathbf{y}_n = \sqrt{T}\mathbf{H}_n\mathbf{s}_n + \sqrt{T}\mathbf{H}_n\mathbf{s}_{0n} + \sqrt{1-T}\mathbf{s}_{En} \tag{3a}$$

$$= \sqrt{T}\mathbf{H}_n\left(\mathbf{s}_n + \mathbf{s}_{0n}\right) + \sqrt{1-T}\mathbf{s}_{En} \tag{3b}$$

$$= \sqrt{T}\mathbf{H}_n\mathbf{s}_n + \mathbf{v}_n, \tag{3c}$$

where $\mathbf{H}_n \in \mathcal{C}^{M\times M}$ and $\mathbf{s}_E \in \mathcal{C}^{M\times 1}$ model the faded CIR matrix. Following this, the received TD signal is transformed into the FD by DFT as follows:

$$\overline{\mathbf{y}}_n = \mathbf{F}_M\mathbf{y}_n = \sqrt{T}\overline{\mathbf{H}}_n\overline{\mathbf{s}}_n + \overline{\mathbf{v}}_n, \tag{4}$$

where $\overline{\mathbf{v}}_n = \sqrt{T}\mathbf{H}_n\mathbf{s}_{0n} + \sqrt{1-T}\mathbf{s}_{En}$.

In time-invariant and frequency-selective fading, the CIR matrix $\mathbf{H}$ of (3) is circulent, i.e. row $m+1$ is a right shift of row m, leading to a diagonal matrix for $\overline{\mathbf{H}}_n = \mathbf{F}_M\mathbf{H}_n\mathbf{F}_M^H$. As a result, the OFDM subcarriers are orthogonal to each other, leading to the following element-wise input-output relationship:

$$\overline{y}_{n,\overline{m}} = \sqrt{T}\overline{h}_{n,\overline{m}}\overline{s}_{n,\overline{m}} + \overline{v}_{n,\overline{m}}, \tag{5}$$

where $\overline{h}_{n,\overline{m}} = \sum_{l=0}^{L-1} h_{n,\overline{m},l}\omega_M^{-\overline{m}l}$ is the $\overline{m}$th diagonal element in $\overline{\mathbf{H}}_n$, and $h_{n,\overline{m},l}$ stands for the fading gain in the TD. Therefore, single-tap FD equalization (FDE) can be invoked as follows:

$$\overline{z}_{n,\overline{m}} = \overline{y}_{n,\overline{m}}/\overline{h}_{n,\overline{m}}, 0 \le \overline{m} \le M-1. \tag{6}$$

However, when the fading channel becomes time-varying in the face of the Doppler effect, especially when the Doppler frequency f_D becomes comparable to the subcarrier spacing (SCS) Δf, the OFDM subcarrier orthogonality no longer holds, which imposes ICI. As a result, the TD fading matrix has to be equalized as a whole, leading to the following FD minimum mean squared error (FD-MMSE) detector:

$$\overline{\mathbf{z}}_n = \left(\overline{\mathbf{H}}_n^H\overline{\mathbf{H}}_n + N_0\mathbf{I}_M\right)^{-1}\overline{\mathbf{H}}_n^H\overline{\mathbf{y}}_n, \tag{7}$$

where N_0 represent the power of the AWGN[4].

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 $\left\{\left\{\widetilde{s}_{k,l}\right\}_{k=0}^{N-1}\right\}_{l=0}^{M-1}$, which is transformed into the FD via the inverse symplectic finite Fourier transform (ISFFT):

$$\overline{s}_{n,\overline{m}} = \frac{1}{\sqrt{NM}}\sum_{k=0}^{N-1}\sum_{l=0}^{M-1}\widetilde{s}_{k,l}\omega_N^{nk}\omega_M^{-\overline{m}l}, \tag{8}$$

where n, $\overline{m}$, k and l refer to the symbol index, sample index, Doppler index and delay index, respectively. Furthermore, the DD domain symbol $\widetilde{s}_{0,k,l}$ is used to represent the preparation thermal noise and the corresponding signal in FD can be derived into $\overline{s}_{0,n,m}$ using the same operation in (8). Then, an IDFT operation is applied to the FD signal $\overline{s}_{n,\overline{m}}$, hence the TD signal is generated as

$$s_{n,m} = \frac{1}{\sqrt{M}}\sum_{\overline{m}=0}^{M-1}\overline{s}_{n,\overline{m}}\omega_M^{m\overline{m}} = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\widetilde{s}_{k,m}\omega_N^{nk}. \tag{9}$$

The same operation from (9) can be applied to the FD signal $\overline{s}_{0,n,m}$ to get $s_{0,n,m}$.

Accordingly, the received TD signal can be expressed as

$$\begin{aligned} y_{n,m} =& \sqrt{T}\sum_{p=0}^{P-1}\widetilde{h}_p\omega_{MN}^{k_p[n(M+M_{cp})+m-l_p]}s_{n,<m-l_p>_M} \\ &+ \sqrt{T}\sum_{p=0}^{P-1}\widetilde{h}_p\omega_{MN}^{k_p[n(M+M_{cp})+m-l_p]}s_{0,n,<m-l_p>_M} \\ &+ \sqrt{1-T}s_{E n,m} \\ &= \sqrt{T}\sum_{p=0}^{P-1}\widetilde{h}_p\omega_{MN}^{k_p[n(M+M_{cp})+m-l_p]}s_{n,<m-l_p>_M} + v_{n,m}, \end{aligned} \tag{10}$$

where P paths fall into L resolvable TDL, i.e. $P = \sum_{l=0}^{L-1} P_l$, while $\widetilde{h}_p$ and M_{cp} represent the fading gain and the length of the cyclic prefix (CP), respectively. Following this, the received FD signal is obtained by the DFT as follows:

$$\begin{aligned} \overline{y}_{n,\overline{m}} &= \sqrt{T}\frac{1}{\sqrt{M}}\sum_{m=0}^{M-1}y_{n,m}\omega_M^{-m\overline{m}} \\ &= \sqrt{T}\frac{1}{\sqrt{M}}\sum_{m=0}^{M-1}\sum_{p=0}^{P-1}\widetilde{h}_p s_{n,<m-l_p>_M}\cdot \\ &\qquad \omega_{MN}^{k_p[n(M+M_{cp})+m-l_p]}\omega_M^{-m\overline{m}} + \overline{v}_{n,\overline{m}}. \end{aligned} \tag{11}$$

Finally, the DD domain signal can be obtained by using the symplectic finite Fourier transform (SFFT) operation as

$$\begin{aligned} \widetilde{y}_{k,l} &= \sqrt{T}\frac{1}{\sqrt{MN}}\sum_{n=0}^{N-1}\sum_{\overline{m}=0}^{M-1}\overline{y}_{n,\overline{m}}\omega_N^{-nk}\omega_M^{\overline{m}l} \\ &= \sqrt{T}\sum_{p=0}^{P-1}\widetilde{h}_p\omega_{MN}^{k_p(l-l_p)}\widetilde{s}_{<k-k_p>_N,<l-l_p>_M} + \widetilde{v}_{k,l}. \end{aligned} \tag{12}$$

There are two ways of appending CP in OTFS, namely the one using a single CP for the entire OTFS frame and the other one where a CP is inserted in each symbol duration. If a single CP is added to the entire OTFS frame, the TD circular convolution

[4] Note that 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. IV.

of (10) becomes MN-periodic according to

$$y_{n,m} =\sqrt{T}\sum_{p=0}^{P-1}\widetilde{h}_p\omega_{MN}^{k_p[nM+m-l_p]}s_{<nM+m-l>_{MN}} \\ + v_{n,m}, \tag{13}$$

where

$$s_{<nM+m-l>_{MN}} = \begin{cases} s_{n,<m-l>_M}, & m \geq l \\ s_{n-1,<m-l>_M}, & m < l \end{cases}. \tag{14}$$

As a result, the input-output relationship of (12) becomes [40]

$$\widetilde{y}_{k,l} =\sqrt{T}\sum_{p=0}^{P-1}\widetilde{h}_p\widetilde{T}(k,l,k_p,l_p)\widetilde{s}_{<k-k_p>_N,<l-l_p>_M} \\ + \widetilde{v}_{k,l}, \tag{15}$$

where the DD index-based phase rotations are defined as

$$\widetilde{T}(k,l,k_p,l_p) = \begin{cases} \omega_{MN}^{k_p(<l-l_p>_M)}, & l \geq l_p \\ \omega_N^{-(k-k_p)}\omega_{MN}^{k_p(l-l_p)} = \omega_N^{-k}\omega_{MN}^{k_p(<l-l_p>_M)}, & l < l_p. \end{cases} \tag{16}$$

In summary, the OTFS input-output relationship of (12) and (15) can be expressed in the following matrix form:

$$\widetilde{\mathbf{y}} =\sqrt{T}\widetilde{\mathbf{H}}\widetilde{\mathbf{s}} + \widetilde{\mathbf{v}}, \tag{17}$$

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 $\widetilde{\mathbf{H}}_{\kappa,\iota} = \widetilde{h}_p\omega_{MN}^{k_p(l-l_p)}$ and $\widetilde{\mathbf{H}}_{\kappa,\iota} = \widetilde{h}_p\widetilde{T}(k,l,k_p,l_p)$ for (12) and (15), respectively. Based on (17), the DD-MMSE detector can be formulated as

$$\widetilde{\mathbf{z}} = \left(\widetilde{\mathbf{H}}^H\widetilde{\mathbf{H}} + N_0\mathbf{I}_{MN}\right)^{-1}\widetilde{\mathbf{H}}^H\widetilde{\mathbf{y}}. \tag{18}$$

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

As portrayed in Fig. 1, the MDR process [42], [46] is employed for enhancing the CV-QKD performance in THz quantum channels, which is summarized as follows:

1) Bob generates the secret key $\mathbf{b}$ using a quantum random number generator (QRNG). An LDPC syndrome $\mathbf{s}^B$ generated based on the key is transmitted to Alice in a classical channel in preparation for error correction.
2) The Gaussian variables $\ddot{\mathbf{s}}$ are transmitted by Alice either in the FD based on OFDM as $\overline{\mathbf{s}}$ or in the DD domain based on OTFS as $\widetilde{\mathbf{s}}$, as shown in Fig. 1.
3) Bob maps the key onto a D-dimansional unit-radius sphere $\mathbf{u}^B$. For this work, we use $D=8$ as suggested in [42], [46], resulting in the 8-dimensional unit-radius sphere of $\mathbf{u}_i^B = \left[\frac{(-1)^{\mathbf{b}_i(0)}}{\sqrt{D}}, \frac{(-1)^{\mathbf{b}_i(1)}}{\sqrt{D}}, \dots, \frac{(-1)^{\mathbf{b}_i(D-1)}}{\sqrt{D}}\right]$, where i represents the ith segment in the MDR process. The MDR mapping function ensures that the ideally error-free transmission of Gaussian variables leads to the same unit-radius sphere at the receiver, i.e., $\mathbf{M}(\ddot{\mathbf{s}}_i', \mathbf{u}_i^B)\ddot{\mathbf{s}}_i' = \mathbf{u}_i^B$.
4) On Bob's side, the Guassian variables are received and equalized either in the FD as $\overline{\mathbf{z}}$ based on the OFDM scheme of (6) and (7) or in the DD domain as $\widetilde{\mathbf{z}}$ based on the OTFS of (18), providing input to the receiver's MDR process as $\ddot{\mathbf{z}}$. The MDR mapping function that ensures $\mathbf{M}(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B)\ddot{\mathbf{z}}_i' = \mathbf{u}_i^B$ is sent from Bob to Alice through a classical channel.
5) Alice demodulates $\ddot{\mathbf{s}}'$ based on the MDR mapping function, producing soft-decision log likelihood ratios (LLRs) for the LDPC decoder to recover the key with the aid of the syndrome-based side information.

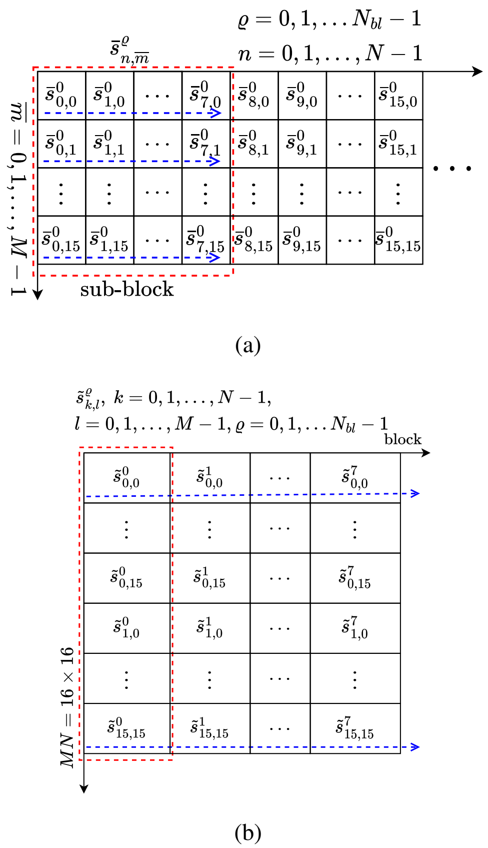

$\varrho = 0, 1, \dots N_{bl} - 1$
$n = 0, 1, \dots, N-1$
$\overline{s}^{\varrho}_{n,\overline{m}}$
$\overline{m} = 0, 1, \dots, M-1$
$\overline{s}^0_{0,0}$ $\overline{s}^0_{1,0}$ $\cdots$ $\overline{s}^0_{7,0}$ $\overline{s}^0_{8,0}$ $\overline{s}^0_{9,0}$ $\cdots$ $\overline{s}^0_{15,0}$
$\overline{s}^0_{0,1}$ $\overline{s}^0_{1,1}$ $\cdots$ $\overline{s}^0_{7,1}$ $\overline{s}^0_{8,1}$ $\overline{s}^0_{9,1}$ $\cdots$ $\overline{s}^0_{15,1}$
$\overline{s}^0_{0,15}$ $\overline{s}^0_{1,15}$ $\cdots$ $\overline{s}^0_{7,15}$ $\overline{s}^0_{8,15}$ $\overline{s}^0_{9,15}$ $\cdots$ $\overline{s}^0_{15,15}$
sub-block
(a)
$\widetilde{s}^{\varrho}_{k,l}$, $k = 0, 1, \dots, N-1$,
$l = 0, 1, \dots, M-1, \varrho = 0, 1, \dots N_{bl} - 1$
block
$\widetilde{s}^0_{0,0}$ $\widetilde{s}^1_{0,0}$ $\cdots$ $\widetilde{s}^7_{0,0}$
$\widetilde{s}^0_{0,15}$ $\widetilde{s}^1_{0,15}$ $\cdots$ $\widetilde{s}^7_{0,15}$
$\widetilde{s}^0_{1,0}$ $\widetilde{s}^1_{1,0}$ $\cdots$ $\widetilde{s}^7_{1,0}$
$\widetilde{s}^0_{15,15}$ $\widetilde{s}^1_{15,15}$ $\cdots$ $\widetilde{s}^7_{15,15}$
$MN = 16 \times 16$
(b)

Fig. 4: An example of transmission arrangements for (a) **OFDM**- and (b) **OTFS**-LDPC assisted CV-QKD, where $N = M = 16$.

However, the conventional MDR found in [47], [48] generally assume a BI-AWGN channel, where the noise variance of LLR computation is uniform across all received Gaussian variables. By contrast, the OFDM FDE decision variables $\overline{z}_{\overline{m}}$ in (6) have a noise variance that remains constant for each subcarrier index in time-invariant fading, but it varies from subcarrier to subcarrier. The OFDM FD-MMSE decision variables $\overline{\mathbf{z}}[\overline{m}]$ in (7) have a noise variance that is consistent for each subcarrier index in doubly selective fading. Moreover, the OTFS DD-MMSE decision variables have a noise variance that is always consistent for each DD index. In light of this, we propose to modify both the OFDM and OTFS transmission arrangement for MDR, which is exemplified by Fig. 4, so that the MDR demapper produces reliable LLRs based on consistent noise variance.

More explicitly, the parameters of $M = 16$ and $N = 16$ are used for the $D = 8$ MDR of OFDM/OTFS in Fig. 4. Therefore, an LDPC block length of $N_{\text{FEC}} = 2048$ includes $N_{bl} = N_{\text{FEC}}/(M \times N) = 2048/(16 \times 16) = 8$ OFDM/OTFS frames[5]. For the OFDM transmission of Fig. 4a, each $(M \times N) = (16 \times 16)$-element OFDM symbol block is devided into $N_{sb} = N/D = 16/8 = 2$ sub-blocks of $(M \times D) = (16 \times 8)$ elements, so that each MDR segment is formed by $D = 8$ FD symbols on each subcarrier. This arrangement that represents the ith segment is denoted as $\bar{\mathbf{s}}_i^{\text{MDR}} = \left[\bar{s}_{i,0}^{\text{MDR}}, \cdots, \bar{s}_{i,d}^{\text{MDR}}, \cdots, \bar{s}_{i,D-1}^{\text{MDR}}\right]^T$, where $\bar{s}_{i,d}^{\text{MDR}}$, $d = 0, 1, ..., D-1$ represents the dth element in the ith segment, and the relationship between $\bar{s}_{i,d}^{\text{MDR}}$ and $\bar{s}_{n,\overline{m}}^{\varrho}$ is as follows: $\bar{s}_{i,d}^{\text{MDR}} = \bar{s}_{n,\overline{m}}^{\varrho}$ when $i = \lfloor n/D \rfloor \cdot M + \overline{m} + \varrho\,(N/D \cdot M)$ and $d = \text{rem}(n, D)$, where $n = 0, 1, ..., N-1$, $\overline{m} = 0, 1, ..., M-1$ and $\varrho = 0, 1, ..., N_{bl} - 1$. For the OTFS transmission arrangement of Fig. 4b, a total number of $D = 8$ symbols on each DD index form a MDR segment, the ith of which is denoted as $\widetilde{\mathbf{s}}_i^{\text{MDR}} = [\widetilde{s}_{i,0}^{\text{MDR}}, \cdots, \widetilde{s}_{i,d}^{\text{MDR}}, \cdots, \widetilde{s}_{i,D-1}^{\text{MDR}}]^T$, where $\widetilde{s}_{i,d}^{\text{MDR}}$, $d = 0, 1, ..., D-1$ represents the dth element in the ith segment, and the relationship between $\widetilde{s}_{i,d}^{\text{MDR}}$ and $\widetilde{s}_{k,l}^{\varrho}$ is as follows: $\widetilde{s}_{i,d}^{\text{MDR}} = \widetilde{s}_{k,l}^{\varrho}$ when $i = k \cdot M + l$ and $d = \varrho$, where $k = 0, 1, ..., N-1$ and $l = 0, 1, ..., M-1$ and $\varrho = 0, 1, ..., N_{bl}-1$. Hence, 8 OTFS symbol blocks are enough to transmit 2048 symbols.

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

Based on the modified OFDM/OTFS transmission pattern introduced in Sec. II-C, the revised MDR process tailored for OFDM/OTFS in doubly selective THz channels is summarized in Algorithm 1. Let us introduce the steps of Algorithm 1 based on the OFDM FDE mechanism and then generalize it to OFDM FD-MMSE and OTFS DD-MMSE.

Consider a sequence of ϱ OFDM blocks with $\varrho = 0, 1, ..., N_{bl} - 1$ where $N_{bl} = N_{\text{FEC}}/(MN)$, (6) can be reformulated as

$$\overline{z}_{n,\overline{m}}^{\varrho} = \overline{y}_{n,\overline{m}}^{\varrho}/\overline{h}_{n,\overline{m}}^{\varrho} = \overline{s}_{n,\overline{m}}^{\varrho} + \overline{v}_{n,\overline{m}}^{\varrho}/\overline{h}_{n,\overline{m}}^{\varrho}. \tag{19}$$

Therefore, based on the corresponding demapping process of Fig.4, the relationship between the transmitted and segmented signal after sifting - for example taking the real part of all complex values in (19) - can be denoted as $\ddot{\mathbf{s}}_i = \mathfrak{Re}\left[\bar{\mathbf{s}}_i^{\text{MDR}}\right] = \mathfrak{Re}\left[\bar{s}_{i,0}^{\text{MDR}}, \cdots, \bar{s}_{i,d}^{\text{MDR}}, \cdots, \bar{s}_{i,D-1}^{\text{MDR}}\right]^T$, where $\bar{s}_{i,d}^{\text{MDR}} = \bar{s}_{n,\overline{m}}^{\varrho}$ represents the dth element in the ith segment with $i = \lfloor n/D \rfloor \cdot M + \overline{m} + \varrho\,(N/D \cdot M)$ and $d = \text{rem}(n, D)$, while $n = 0, 1, ..., N-1$, $\overline{m} = 0, 1, ..., M-1$ and $\varrho = 0, 1, ..., N_{bl} - 1$. Similarly, the relationship between the received and segmented signal after sifting is $\ddot{\mathbf{z}}_i = \mathfrak{Re}\left[\bar{\mathbf{z}}_i^{\text{MDR}}\right] = \mathfrak{Re}\left[\bar{z}_{i,0}^{\text{MDR}}, \cdots, \bar{z}_{i,d}^{\text{MDR}}, \cdots, \bar{z}_{i,D-1}^{\text{MDR}}\right]^T$ with $\bar{z}_{i,d}^{\text{MDR}} = \bar{z}_{n,\overline{m}}^{\varrho}$. Upon taking the real part of the noise term $\overline{v}_{n,\overline{m}}^{\varrho}/\overline{h}_{n,\overline{m}}^{\varrho}$ in (19) as $\ddot{v}$, the ith segment of the noise term can be denoted as $\ddot{\mathbf{v}}_i = \mathfrak{Re}\left[\left(\text{diag}\left(\ddot{\mathbf{h}}_i\right)\right)^{-1}\ddot{\mathbf{v}}'_i\right]$, where $\ddot{\mathbf{h}}_i = \left[\overline{h}_{i,0}^{\text{MDR}}, \cdots, \overline{h}_{i,d}^{\text{MDR}}, \cdots, \overline{h}_{i,D-1}^{\text{MDR}}\right]^T$ with $\overline{h}_{i,d}^{\text{MDR}} = \overline{h}_{n,\overline{m}}^{\varrho}$, and $\ddot{\mathbf{v}}'_i = \left[\overline{v}_{i,0}^{\text{MDR}}, \cdots, \overline{v}_{i,d}^{\text{MDR}}, \cdots, \overline{v}_{i,D-1}^{\text{MDR}}\right]^T$ with $\overline{v}_{i,d}^{\text{MDR}} = \overline{v}_{n,\overline{m}}^{\varrho}$. In summary, the system model used for our MDR algorithm of the ith segment can be expressed as

$$\ddot{\mathbf{z}}_i = \ddot{\mathbf{s}}_i + \ddot{\mathbf{v}}_i. \tag{20}$$

Algorithm 1 The description of MDR scheme conceived for OFDM/OTFS in time-varying and frequency-selective THz fading channels, where the OFDM FDE mechanism is assumed.

```
1: Partition: The sequences $\ddot{\mathbf{s}}$ of Alice's and $\ddot{\mathbf{z}}$ of Bob's data after sifting, whose length is the same as a FEC codeword length $N_{\text{FEC}}$, are partitioned into shorter segments, which can be denoted as $\ddot{\mathbf{s}} = [\ddot{\mathbf{s}}_0; \ddot{\mathbf{s}}_1; ...; \ddot{\mathbf{s}}_{I-1}]$ and $\ddot{\mathbf{z}} = [\ddot{\mathbf{z}}_0; \ddot{\mathbf{z}}_1; ...; \ddot{\mathbf{z}}_{I-1}]$, where $I = N_{\text{FEC}}/D$, and $\ddot{\mathbf{s}}_i, \ddot{\mathbf{z}}_i \in \mathcal{R}^{D \times 1}$. Furthermore, the channel coefficient is also partitioned into $\ddot{\mathbf{h}} = \left[\ddot{\mathbf{h}}_0; \ddot{\mathbf{h}}_1; ...; \ddot{\mathbf{h}}_{I-1}\right]$.
2: Normalization: Normalize each segment of $\ddot{\mathbf{s}}_i$ and $\ddot{\mathbf{z}}_i$ by $\ddot{\mathbf{s}}'_i = \frac{\ddot{\mathbf{s}}_i}{\|\ddot{\mathbf{s}}_i\|}$ and $\ddot{\mathbf{z}}'_i = \frac{\ddot{\mathbf{z}}_i}{\|\ddot{\mathbf{z}}_i\|}$, where we have $\|\ddot{\mathbf{s}}_i\| = \sqrt{\langle \ddot{\mathbf{s}}_i, \ddot{\mathbf{s}}_i \rangle} = \sqrt{\sum_{d=0}^{D-1} \ddot{\mathbf{s}}_i\,(d)^2}$ and $\|\ddot{\mathbf{z}}_i\| = \sqrt{\langle \ddot{\mathbf{z}}_i, \ddot{\mathbf{z}}_i \rangle} = \sqrt{\sum_{d=0}^{D-1} \ddot{\mathbf{z}}_i\,(d)^2}$
3: QRNG generation: At Bob's side, a random bit stream $\mathbf{b}$ is generated via QRNG, the length of which is the same as a FEC codeword length $N_{\text{FEC}}$. Then, the random bit sequence is $\mathbf{b}$ partitioned into $\mathbf{b} = [\mathbf{b}_0; \mathbf{b}_1; ...; \mathbf{b}_{I-1}]$, where $I = N_{\text{FEC}}/D$ and $\mathbf{b}_i$ is a $D$-dimensional binary column vector. For each segment of $\mathbf{b}_i, i = 0, 1, ..., I-1$, it is mapped to the unit sphere of $\mathbf{u}_i^B = \left(\frac{(-1)^{\mathbf{b}_i(0)}}{\sqrt{D}}, \frac{(-1)^{\mathbf{b}_i(1)}}{\sqrt{D}}, \ldots, \frac{(-1)^{\mathbf{b}_i(D-1)}}{\sqrt{D}}\right)$.
4: Mapping function calculation: Bob calculates the mapping function $\mathbf{M}_i\left(\ddot{\mathbf{z}}'_i, \mathbf{u}_i^B\right)$ for each segment with $\mathbf{M}_i\left(\ddot{\mathbf{z}}'_i, \mathbf{u}_i^B\right)\ddot{\mathbf{z}}'_i = \mathbf{u}_i^B$ using the following formula:
       $\mathbf{M}_i\left(\ddot{\mathbf{z}}'_i, \mathbf{u}_i^B\right) = \sum_{d=0}^{D-1} \alpha_i^d \mathbf{A}_d,$
   where $\alpha_i^d$ is the $d$th element of $\boldsymbol{\alpha}_i\left(\ddot{\mathbf{z}}'_i, \mathbf{u}_i^B\right) = \left(\alpha_i^0, \alpha_i^1, ..., \alpha_i^{D-1}\right)^T$, which is the coordinate of the vector $\mathbf{u}_i^B$ under orthonormal basis $(\mathbf{A}_0\ddot{\mathbf{z}}'_i, \mathbf{A}_1\ddot{\mathbf{z}}'_i, ..., \mathbf{A}_{D-1}\ddot{\mathbf{z}}'_i)$ and it can be expressed as $\boldsymbol{\alpha}_i\left(\ddot{\mathbf{z}}'_i, \mathbf{u}_i^B\right) = (\mathbf{A}_0\ddot{\mathbf{z}}'_i, \mathbf{A}_1\ddot{\mathbf{z}}'_i, ..., \mathbf{A}_{D-1}\ddot{\mathbf{z}}'_i)^T \mathbf{u}_i^B$. Note that $\mathbf{A}_d, d = 0, 1, ..., D-1$ is the orthogonal matrix of size $D \times D$ and has been provided in the Appendix of [42], [46].
5: Mapping function implement: Alice operates the same data mapping on $\ddot{\mathbf{s}}'_i$ to map the Gaussian distributed vector to $\mathbf{u}_i^A = \mathbf{M}_i\left(\ddot{\mathbf{z}}'_i, \mathbf{u}_i^B\right)\ddot{\mathbf{s}}'_i$, which is a noise version of $\mathbf{u}_i^B$.
6: LLR calculation: LLR is calculated in the way of
       $\mathcal{L}\left(\mathbf{u}_i^A[d]\right) = \frac{2\|\ddot{\mathbf{s}}_i\|\,\|\ddot{\mathbf{z}}_i\|\left\|\ddot{\mathbf{h}}_i\right\|^2/D}{\sqrt{D}\sigma^2}\mathbf{u}_i^A[d],$
   with the assumption that in each segment, all of the channel coefficients remain the same, which is $\ddot{\mathbf{h}}_i[d] = \overline{h}_i, \forall d \in [0, D-1]$. Then, the LLR for a whole FEC block length $\mathcal{L}\left(\mathbf{u}^A\right)$ can be constructed by those segments of $\mathcal{L}\left(\mathbf{u}_i^A\right)$, which gives
       $\mathcal{L}\left(\mathbf{u}^A\right) = \left[\mathcal{L}\left(\mathbf{u}_1^A\right); \mathcal{L}\left(\mathbf{u}_2^A\right); ...; \mathcal{L}\left(\mathbf{u}_I^A\right)\right].$
   Then, FEC decoding is carried on with the input of $\mathcal{L}\left(\mathbf{u}^A\right)$.
```

The MDR process therefore spans from step 1-Partition to step 6-LLR calculation as illustrated in Algorithm 1. As for the LLR calculation, the details are as follows. After Alice

[5] Note that binary phase-shift keying (BPSK) associated with LDPC is considered in our paper.

receives the mapping matrix $\mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)$ and $\|\ddot{\mathbf{z}}_i\|$ for each segment, she applies the same mapping to her data $\ddot{\mathbf{s}}_i'$ to obtain $\mathbf{u}_i^A = \mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)\ddot{\mathbf{s}}_i'$. By introducing a scaling factor of $\frac{\|\ddot{\mathbf{s}}_i\|}{\|\ddot{\mathbf{z}}_i\|}$, she obtains

$$\begin{aligned}\mathbf{u}_i^{A\prime} &= \frac{\|\ddot{\mathbf{s}}_i\|}{\|\ddot{\mathbf{z}}_i\|}\mathbf{u}_i^A = \frac{\|\ddot{\mathbf{s}}_i\|}{\|\ddot{\mathbf{z}}_i\|}\mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)\ddot{\mathbf{s}}_i' \\ &= \mathbf{u}_i^B - \frac{1}{\|\ddot{\mathbf{z}}_i\|}\mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)\mathfrak{Re}\left[\left(\text{diag}\left(\ddot{\mathbf{h}}_i\right)\right)^{-1}\ddot{\mathbf{v}}_i'\right].\end{aligned} \tag{21}$$

Now, we assume that in each segment, all the channel coefficients are the same, which gives $\ddot{\mathbf{h}}_i[d] = \ddot{h}_{i,0} \triangleq \overline{\ddot{h}}_i, \forall d \in [0, D-1]$. Furthermore, $\ddot{h}_{i,d} = \overline{h}_{n,\overline{m}}^{\varrho}$ with $i = \lfloor n/D \rfloor \cdot M + \overline{m} + \varrho\left(N/D \cdot M\right)$ and $d = \text{rem}(n, D)$, while $n = 0, 1, ..., N-1$, $\overline{m} = 0, 1, ..., M-1$ and $\varrho = 0, 1, ..., N_{bl} - 1$. Hence, $\mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)\mathfrak{Re}\left[\left(\text{diag}\left(\ddot{\mathbf{h}}_i\right)\right)^{-1}\ddot{\mathbf{v}}_i'\right]$ can be derived as

$$\begin{aligned}&\mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)\mathfrak{Re}\left[\left(\text{diag}\left(\ddot{\mathbf{h}}_i\right)\right)^{-1}\ddot{\mathbf{v}}_i'\right] = \mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)\mathfrak{Re}\left(\frac{\overline{\ddot{h}}_i^{*}\ddot{\mathbf{v}}_i'}{\left\|\overline{\ddot{h}}_i\right\|^2}\right) \\ &= \frac{1}{\left\|\overline{\ddot{h}}_i\right\|^2}\mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)\left(\mathfrak{Re}\left(\overline{\ddot{h}}_i\right)\mathfrak{Re}\left(\ddot{\mathbf{v}}_i'\right) + \mathfrak{Im}\left(\overline{\ddot{h}}_i\right)\mathfrak{Im}\left(\ddot{\mathbf{v}}_i'\right)\right) \\ &= \frac{1}{\left\|\overline{\ddot{h}}_i\right\|^2}\mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)\left(\ddot{\mathbf{v}}_i^{\prime R} + \ddot{\mathbf{v}}_i^{\prime I}\right) = \frac{1}{\left\|\overline{\ddot{h}}_i\right\|^2}\mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)\ddot{\mathbf{v}}_i^{\dagger},\end{aligned} \tag{22}$$

where $\ddot{\mathbf{v}}_i^{\prime R} \sim \mathcal{N}\left(0, \left[\mathfrak{Re}\left(\overline{\ddot{h}}_i\right)\right]^2\sigma^2\mathbb{I}_8\right)$, $\ddot{\mathbf{v}}_i^{\prime I} \sim \mathcal{N}\left(0, \left[\mathfrak{Im}\left(\overline{\ddot{h}}_i\right)\right]^2\sigma^2\mathbb{I}_8\right)$ with $N_0 = 2\sigma^2$, and hence $\ddot{\mathbf{v}}^{\dagger} \sim \mathcal{N}\left(0, \left\|\overline{\ddot{h}}_i\right\|^2\sigma^2\mathbb{I}_8\right)$. Thereby, (21) can be reformulated as

$$\mathbf{u}_i^{A\prime} = \mathbf{u}_i^B - \frac{1}{\|\ddot{\mathbf{z}}_i\|}\frac{1}{\left\|\overline{\ddot{h}}_i\right\|^2}\mathbf{M}\left(\ddot{\mathbf{z}}_i', \mathbf{u}_i^B\right)\ddot{\mathbf{v}}_i^{\dagger} = \mathbf{u}_i^B - \frac{1}{\|\ddot{\mathbf{z}}_i\|}\frac{1}{\left\|\overline{\ddot{h}}_i\right\|^2}\ddot{\mathbf{v}}_i^{\ddagger}, \tag{23}$$

where $\ddot{\mathbf{v}}_i^{\ddagger} \sim \mathcal{N}\left(0, \left\|\overline{\ddot{h}}_i\right\|^2\sigma^2\mathbb{I}_8\right)$ is the new noise vector after mapping, which has zero mean and a constant variance for the entire segment.

Based on this, the LLR of the sequence in one segment can be calculated by

$$\begin{aligned}\mathcal{L}\left(\mathbf{u}_i^{A\prime}[d]\right) &= \frac{\mathbb{P}\left(\mathbf{u}_i^{A\prime}[d]\right)|\mathbf{b}_i[d] = 0)}{\mathbb{P}\left(\mathbf{u}_i^{A\prime}[d]\right)|\mathbf{b}_i[d] = 1)} \\ &= \ln\frac{\frac{1}{\sqrt{2\pi\sigma}}e^{-\frac{\|\ddot{\mathbf{z}}_i\|^2\left\|\overline{\ddot{h}}_i\right\|^4\left(\frac{1}{\sqrt{D}} - \mathbf{u}_i^A[d]\right)^2}{2\pi\left\|\overline{\ddot{h}}_i\right\|^2\sigma^2}}}{\frac{1}{\sqrt{2\pi\sigma}}e^{-\frac{\|\ddot{\mathbf{z}}_i\|^2\left\|\overline{\ddot{h}}_i\right\|^4\left(-\frac{1}{\sqrt{D}} - \mathbf{u}_i^A[d]\right)^2}{2\pi\left\|\overline{\ddot{h}}_i\right\|^2\sigma^2}}} = \frac{2\|\ddot{\mathbf{z}}_i\|\left\|\overline{\ddot{h}}_i\right\|^2\mathbf{u}_i^{A\prime}[d]}{\sqrt{D}\sigma^2}\end{aligned} \tag{24}$$

By replacing $\mathbf{u}_i^{A\prime}$ with $\mathbf{u}_i^A$ using the relationship of $\mathbf{u}_i^{A\prime} = \frac{\|\ddot{\mathbf{s}}_i\|}{\|\ddot{\mathbf{z}}_i\|}\mathbf{u}_i^A$, (24) can be reformulated as

$$\mathcal{L}\left(\mathbf{u}_i^A[d]\right) = \frac{2\|\ddot{\mathbf{s}}_i\|\|\ddot{\mathbf{z}}_i\|\|\overline{\ddot{h}}_i\|^2}{\sqrt{D}N_0/2}\mathbf{u}_i^A[d]. \tag{25}$$

It becomes clear now that (25) incorporates the LLR calculations for MDR as seen in the literature that assume BI-AWGN as a special case [47], [48]. Explicitly, for the special case of a BI-AWGN channel, i.e. where we have $\ddot{\mathbf{h}}_i = \mathbf{1}_{D\times 1}, \forall i \in [0, I-1]$, the LLR for each segment is given by:

$$\mathcal{L}\left(\mathbf{u}_i^A[d]\right) = \frac{2\|\ddot{\mathbf{s}}_i\|\|\ddot{\mathbf{z}}_i\|}{\sqrt{D}N_0/2}\mathbf{u}_i^A[d]. \tag{26}$$

In summary, the LLR calculations (25) produce reliable demapping soft-decisions for MDR in fading channels, and the LLRs are passed to the LDPC decoder for further error correction.

Apart from the FDE detection, both the OFDM FD-MMSE of (7) and the OTFS DD-MMSE of (18) can also be appropriately adapted for Algorithm 1. For OFDM FD-MMSE, (7) can be further reformulated as

$$\overline{\mathbf{z}}_n^{\varrho} = \overline{\mathbf{G}}_n^{\varrho}\overline{\mathbf{y}}_n^{\varrho} \quad = \overline{\mathbf{H}}_n^{\varrho\prime}\overline{\mathbf{s}}_n^{\varrho} + \overline{\mathbf{G}}_n^{\varrho}\overline{\mathbf{v}}_n^{\varrho}, \tag{27}$$

where $\overline{\mathbf{G}}_n^{\varrho} = \left(\overline{\mathbf{H}}_n^{\varrho H}\overline{\mathbf{H}}_n^{\varrho} + N_0\mathbf{I}_M\right)^{-1}\overline{\mathbf{H}}_n^{\varrho H}$, and $\overline{\mathbf{H}}_n^{\varrho\prime} = \overline{\mathbf{G}}_n^{\varrho} \cdot \overline{\mathbf{H}}_n^{\varrho} = \left(\overline{\mathbf{H}}_n^{\varrho H}\overline{\mathbf{H}}_n^{\varrho} + N_0\mathbf{I}_M\right)^{-1}\overline{\mathbf{H}}_n^{\varrho H}\overline{\mathbf{H}}_n^{\varrho}$. Therefore, the $\overline{m}$th element of $\overline{\mathbf{z}}_n^{\varrho}$ can be approximated as $\overline{z}_{n,\overline{m}}^{\varrho} = \overline{\mathbf{G}}_n^{\varrho}[\overline{m}, :]\overline{\mathbf{y}}_n^{\varrho} = \overline{\mathbf{H}}_n^{\varrho\prime}[\overline{m}, \overline{m}]\overline{s}_{n,\overline{m}}^{\varrho} + \overline{\mathbf{G}}_n^{\varrho}[\overline{m}, :]\overline{\mathbf{v}}_n^{\varrho}$. After compensating the effect of channel fading, the equivalent $\overline{z}_{n,\overline{m}}^{\varrho\prime}$ can be expressed as (28).

$$\begin{aligned}\overline{z}_{n,\overline{m}}^{\varrho\prime} &= \frac{\overline{\mathbf{G}}_n^{\varrho}[\overline{m}, :]\overline{\mathbf{y}}_n^{\varrho}\left(\overline{\mathbf{H}}_n^{\varrho\prime}[\overline{m}, \overline{m}]\right)^*}{\left\|\overline{\mathbf{H}}_n^{\varrho\prime}[\overline{m}, \overline{m}]\right\|^2} + \frac{\overline{\mathbf{G}}_n^{\varrho}[\overline{m}, :]\overline{\mathbf{v}}_n^{\varrho}\left(\overline{\mathbf{H}}_n^{\varrho\prime}[\overline{m}, \overline{m}]\right)^*}{\left\|\overline{\mathbf{H}}_n^{\varrho\prime}[\overline{m}, \overline{m}]\right\|^2} \\ &= \overline{s}_{n,\overline{m}}^{\varrho} + \overline{v}_{n,\overline{m}}^{\varrho\prime}.\end{aligned} \tag{28}$$

The new noise term $\overline{v}_{n,\overline{m}}^{\varrho\prime}$ is still Gaussian distributed with zero mean and a variance of $\frac{\left\|\overline{\mathbf{G}}_n^{\varrho}[\overline{m}, :]\right\|^2 N_0}{\left\|\overline{\mathbf{H}}_n^{\varrho\prime}[\overline{m}, \overline{m}]\right\|^2}$. Taking for example the real part of $\overline{z}_{n,\overline{m}}^{\varrho\prime}$, we can obtain $\ddot{\mathbf{z}}_i = \ddot{\mathbf{s}}_i + \ddot{\mathbf{v}}_i$ where $\ddot{\mathbf{s}}_i = \mathfrak{Re}\left[\overline{\mathbf{s}}_i^{\text{MDR}}\right] = \mathfrak{Re}\left[\overline{s}_{i,0}^{\text{MDR}}, \cdots, \overline{s}_{i,d}^{\text{MDR}}, \cdots, \overline{s}_{i,D-1}^{\text{MDR}}\right]^T$ and $\ddot{\mathbf{z}}_i = \mathfrak{Re}\left[\overline{\mathbf{z}}_i^{\text{MDR}}\right] = \mathfrak{Re}\left[\overline{z}_{i,0}^{\text{MDR}}, \cdots, \overline{z}_{i,d}^{\text{MDR}}, \cdots, \overline{z}_{i,D-1}^{\text{MDR}}\right]^T$ with $i = \lfloor n/D \rfloor \cdot M + \overline{m} + \varrho\left(N/D \cdot M\right)$ and $d = \text{rem}(n, D)$, while $n = 0, 1, ..., N-1$, $\overline{m} = 0, 1, ..., M-1$ and $\varrho = 0, 1, ..., N_{bl} - 1$. Moreover, $\overline{s}_{i,d}^{\text{MDR}} = \overline{s}_{n,\overline{m}}^{\varrho\prime}$ and $\overline{z}_{i,d}^{\text{MDR}} = \overline{z}_{n,\overline{m}}^{\varrho\prime}$ represent the dth element in the ith segment of $\overline{s}_i^{\text{MDR}}$ and $\overline{z}_i^{\text{MDR}}$, respectively. Taking the real part of the noise term in (28), the ith segment of noise term can be denoted as $\ddot{\mathbf{v}}_i = \mathfrak{Re}\left[\overline{v}_{i,0}^{\text{MDR}}, \cdots, \overline{v}_{i,d}^{\text{MDR}}, \cdots, \overline{v}_{i,D-1}^{\text{MDR}}\right]^T$ with $\overline{v}_{i,d}^{\text{MDR}} = \overline{v}_{n,\overline{m}}^{\varrho\prime}$. Hence, the variance of each element of the noise $\ddot{\mathbf{v}}_i$ becomes $\frac{\left\|\overline{\mathbf{G}}_n^{\varrho}[\overline{m}, :]\right\|^2 N_0/2}{\left\|\overline{\mathbf{H}}_n^{\varrho\prime}[\overline{m}, \overline{m}]\right\|^2}$. Thereafter, the MDR process is carried out based on Algorithm 1, where $\ddot{\mathbf{v}}_i[d] = \ddot{\mathbf{v}}_i[0]$, i.e. $\overline{v}_{i,d}^{\text{MDR}} = \overline{v}_{i,0}^{\text{MDR}}, \forall d \in [0, D-1]$. By replacing the noise variance in (26), the corresponding LLR calculation associated with FD-MMSE detection in OFDM transmission can be obtained as

$$\mathcal{L}\left(\mathbf{u}_i^A[d]\right) = \frac{2\|\ddot{\mathbf{s}}_i\|\|\ddot{\mathbf{z}}_i\|}{\sqrt{D}}\frac{\left\|\overline{\mathbf{H}}_n^{\varrho\prime}[\overline{m}, \overline{m}]\right\|^2}{\left\|\overline{\mathbf{G}}_n^{\varrho}[\overline{m}, :]\right\|^2 N_0/2}\mathbf{u}_i^A[d]. \tag{29}$$

In OTFS transmission, Similar to (29), the LLR calculation associated with DD-MMSE detection in OTFS transmission can be obtained as

$$\mathcal{L}\left(\mathbf{u}_i^A\left[d\right]\right)=\frac{2\left\|\ddot{\mathbf{s}}_i\right\|\left\|\ddot{\mathbf{z}}_i\right\|}{\sqrt{D}}\frac{\left\|\widetilde{\mathbf{H}}^{\varrho\prime}\left[\kappa,\kappa\right]\right\|^2}{\left\|\widetilde{\mathbf{G}}^{\varrho}\left[\kappa,:\right]\right\|^2 N_0/2}\mathbf{u}_i^A\left[d\right], \quad (30)$$

where $\widetilde{\mathbf{G}}^{\varrho}=\left(\widetilde{\mathbf{H}}^{\varrho H}\widetilde{\mathbf{H}}^{\varrho}+N_0\mathbf{I}_{MN}\right)^{-1}\widetilde{\mathbf{H}}^{\varrho}$, and $\widetilde{\mathbf{H}}^{\varrho\prime}=\widetilde{\mathbf{G}}^{\varrho}\cdot\widetilde{\mathbf{H}}^{\varrho}=\left(\widetilde{\mathbf{H}}^{\varrho H}\widetilde{\mathbf{H}}^{\varrho}+N_0\mathbf{I}_{MN}\right)^{-1}\widetilde{\mathbf{H}}^{\varrho H}\widetilde{\mathbf{H}}^{\varrho}$. More explicitly, the modulated/demodulated symbols for the ith segment can be denoted as $\ddot{\mathbf{s}}_i=\mathfrak{Re}\left[\widetilde{\mathbf{s}}_i^{\mathrm{MDR}}\right]=\mathfrak{Re}\left[\widetilde{s}_{i,0}^{\mathrm{MDR}},\cdots,\widetilde{s}_{i,d}^{\mathrm{MDR}},\cdots,\widetilde{s}_{i,D-1}^{\mathrm{MDR}}\right]^T$, and $\ddot{\mathbf{z}}_i=\mathfrak{Re}\left[\widetilde{\mathbf{z}}_i^{\mathrm{MDR}}\right]=\mathfrak{Re}\left[\widetilde{z}_{i,0}^{\mathrm{MDR}},\cdots,\widetilde{z}_{i,d}^{\mathrm{MDR}},\cdots,\widetilde{z}_{i,D-1}^{\mathrm{MDR}}\right]^T$ with $i=k\cdot M+l+\lfloor\varrho/D\rfloor\cdot MN$ and $d=\mathrm{rem}(\varrho,D)$, where $k=0,1,...,N-1$, $l=0,1,...,M-1$ and $\varrho=0,1,...,N_{bl}-1$. Moreover, $\widetilde{s}_{i,d}^{\mathrm{MDR}}=\widetilde{s}_{k,l}^{\varrho\prime}$ and $\widetilde{z}_{i,d}^{\mathrm{MDR}}=\widetilde{z}_{k,l}^{\varrho\prime}$ represent the dth element in the ith segment of $\widetilde{s}_i^{\mathrm{MDR}}$ and $\widetilde{z}_i^{\mathrm{MDR}}$, respectively. The ith segment of the noise term can be denoted as $\ddot{\mathbf{v}}_i=\mathfrak{Re}\left[\widetilde{v}_{i,0}^{\mathrm{MDR}},\cdots,\widetilde{v}_{i,d}^{\mathrm{MDR}},\cdots,\widetilde{v}_{i,D-1}^{\mathrm{MDR}}\right]^T$ along with $\widetilde{v}_{i,d}^{\mathrm{MDR}}=\widetilde{v}_{n,m}^{\varrho\prime}$. Hence the variance of each element of the noise $\ddot{\mathbf{v}}_i$ becomes $\frac{\left\|\widetilde{\mathbf{G}}^{\varrho}[\kappa,:]\right\|^2 N_0/2}{\left\|\widetilde{\mathbf{H}}^{\varrho\prime}[\kappa,\kappa]\right\|^2}$.

Note that the accuracy of LLRs in (25) and (29) may be affected by the MDR process in mobile scenarios, which will degrade the corresponding SKR performance. To elaborate further, since it is assumed in the generic MDR process that the fading gains of all elements in a segment are identical, the LLR calculation for a segment will assign the same fading value to each element. However, in a time-variant channel, the FD channel $\overline{\mathbf{H}}$ will change with time, therefore the fading values of each element in a segment will differ from each other, which degrades the accuracy of the LLR calculation of (25) and (29). By contrast, the accuracy of LLR calculation in (30) remains unaffected by the MDR process in mobile scenarios, because the DD domain channel $\widetilde{\mathbf{H}}$ does not change with time.

E. Complexity analysis for OFDM/OTFS in Doubly Selective THz Channels

Admittedly, the dominant complexity of both the OFDM- and OTFS-based transceivers is that of the detectors. To elaborate further, the complexity of FDE in (6) for a single OFDM symbol is $\mathcal{O}(M)$ since the diagonal elements in $\overline{\mathbf{H}}\in\mathcal{C}^{M\times M}$ are used by the equalizer. Hence the complexity of a block is $\mathcal{O}(MN)$. Since the FD-MMSE equalizer in (7) of each OFDM symbol has the matrix inversion complexity order of $\mathcal{O}(M^3)$, the complexity for a block is $\mathcal{O}(M^3N)$. By contrast, for an OTFS-based system associated with $\widetilde{\mathbf{H}}\in\mathcal{C}^{MN\times MN}$, the complexity of a DD-MMSE equalizer in (18) for a single OTFS block has a matrix inversion complexity order of $\mathcal{O}(M^3N^3)$ [49]. In light of this, it is plausible that the complexity of the FDE of OFDM is the lowest followed by that of the FD-MMSE of OFDM. The complexity of DD-MMSE of OTFS is the highest. Note that these three detectors perform similarly in a stationary scenario. Hence, the FDE of OFDM is the best choice in stationary scenarios.

However, in high-mobility scenarios, the low-complexity single-tap FDE suffers from an error floor, where FD-MMSE based OFDM and DD-based OTFS have to be employed. Hence, it is more meaningful to compare the complexity of the FD-MSME of OFDM-based system and of the DD-MMSE of OTFS-based system in mobile scenarios. Recall that the complexity of the DD-MMSE of OTFS-based system is higher than that of the FD-MMSE of OFDM-based system, which are $\mathcal{O}(M^3N^3)$ and $\mathcal{O}(M^3N)$, respectively. However, the total complexity for a block of N_{bl} 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 $\overline{\mathbf{H}}$ will change with time, which means that the MMSE equalizer of OFDM has to be updated for each OFDM symbol, where the matrix inversion calculations required for updating the MMSE matrix have to be repeated. By contrast, the MMSE equalizer of OTFS does not have to update its MMSE matrix, owing to the fact that the DD-domain fading representation is time-invariant. In light of this, the complexity of OTFS becomes lower than that of OFDM when we have $N_{bl}>N^2$, which is the case when a large number of blocks combined with powerful LDPC codes having long frames length for the sake of achieving a near-capacity performance.

III. MIMO OFDM/OTFS CV-QKD SYSTEM MODEL

In this section, the input-output relationships of the OFDM/OTFS MIMO system model are derived.

A. OFDM MIMO in Time-Varying Frequency-Selective THz Channel

For a MIMO THz scheme using N_{Tx} transmit antennas and N_{Rx} receive antennas, the TD fading matrix is modelled by [40], [50]:

$$\mathbf{H}_{n,m,l}=\sqrt{N_{Tx}N_{Rx}}\cdot\sum_{p=0}^{P_l-1}\widetilde{h}_p\omega_{MN}^{k_p(nM+m-l_p)}\mathbf{a}_{Rx}(\theta_{Rx,p})\mathbf{a}_{Tx}^H(\theta_{Tx,p}), \quad (31)$$

where there are P_l path falling into the lth TDL. The angle of departure (AoD) and angle of arrival (AoD) $\theta_{Tx,p}$ and $\theta_{Rx,p}$ are Laplacian distributed with means $\overline{\theta}_{Tx}$, $\overline{\theta}_{Rx}$ and variances $\sigma_{\theta_{Tx}}$, $\sigma_{\theta_{Rx}}$, where $\overline{\theta}_{Tx}$ and $\overline{\theta}_{Rx}$ are uniformly distributed over $[0,2\pi)$. We adopt uniform linear arrays (ULAs) at both the transmitter and the receiver, where the antenna response vectors are given by:

$$\mathbf{a}_{Tx}(\theta_{Tx,p})=\frac{1}{\sqrt{N_{Tx}}}\left[1,e^{j\frac{2\pi d\sin(\theta_{Tx,p})}{\lambda}},e^{j2\frac{2\pi d\sin(\theta_{Tx,p})}{\lambda}},\cdots,e^{j\frac{(N_{Tx}-1)2\pi d\sin(\theta_{Tx,p})}{\lambda}}\right]^T, \quad (32)$$

$$\mathbf{a}_{Rx}(\theta_{Rx,p}) = \frac{1}{\sqrt{N_{Rx}}}\Big[1, e^{j\frac{2\pi d\sin(\theta_{Rx,p})}{\lambda}}, e^{j2\frac{2\pi d\sin(\theta_{Rx,p})}{\lambda}}, \cdots, , e^{j\frac{(N_{Rx}-1)2\pi d\sin(\theta_{Rx,p})}{\lambda}}\Big]^T, \tag{33}$$

respectively. In (32) and (32) λ is the wavelength of the signal and $d = \lambda/2$ denotes the aperture domain sample spacing. In the face of user mobility, digital beamforming that requires the time-varying CSI to be available at both the transmitter and the receiver becomes impractical. Instead, we propose to deploy analog precoding at the transmitter and analog combining at the receiver. Hence the beamformed fading channel is expressed as:

$$h_{n,m,l}^{RF} = \left(\mathbf{w}^{Rx,RF}\right)^H \mathbf{H}_{n,m,l}\mathbf{w}^{Tx,RF}, \tag{34}$$

where $\mathbf{w}^{Tx,RF} \in \mathcal{C}^{N_{Tx}\times 1}$ and $\mathbf{w}^{Rx,RF} \in \mathcal{C}^{N_{Rx}\times 1}$ are tuned to the LoS antenna response vectors that should satisfy $\left\{\left\|\mathbf{w}^{Tx,RF}[t]\right\| = \frac{1}{\sqrt{N_{Tx}}}\right\}_{t=1}^{N_{Tx}}$ and $\left\{\left\|\mathbf{w}^{Rx,RF}[r]\right\| = \frac{1}{\sqrt{N_{Tx}}}\right\}_{r=1}^{N_{Rx}}$, and $\mathbf{H}_{n,m,l} \in \mathcal{C}^{N_{Rx}\times N_{Tx}}$ is the TD fading matrix in (31).

Therefore, the received signal after analog combining is[6]

$$\begin{aligned} y_{n,m} &= \sqrt{T}\sum_{l=0}^{L-1} h_{n,m,l}^{RF} s_{n,<m-l>_M} \\ &+ \sqrt{T}\sum_{l=0}^{L-1} h_{n,m,l}^{RF} s_{0n,<m-l>_M} + \sqrt{1-T}s_{En,m} \\ &= \sqrt{T}\sum_{l=0}^{L-1} h_{n,m,l}^{RF} s_{n,<m-l>_M} + v_{n,m}. \end{aligned} \tag{35}$$

The TD matrix form is given by

$$\mathbf{y}_n = \sqrt{T}\mathbf{H}_n^{RF}\mathbf{s}_n + \mathbf{v}_n, \tag{36}$$

where $\mathbf{y}_n = [y_{n,0}, y_{n,1}, \cdots, y_{n,M-1}]^T$, $\mathbf{H}_n^{RF}[r,c] = h_{n,r,<r-c>_M}^{RF}$, $\mathbf{s}_n = [s_{n,0}, s_{n,1}, \cdots, s_{n,M-1}]^T$ and $\mathbf{v}_n = [v_{n,0}, v_{n,1}, \cdots, v_{n,M-1}]^T$. Then the FD received signal can be obtained by applying DFT, yielding:

$$\begin{aligned} \overline{y}_{n,\overline{m}} &= \frac{1}{\sqrt{M}}\sum_{m=0}^{M-1} y_{n,m}\omega_M^{-m\overline{m}} \\ &= \frac{\sqrt{T}}{\sqrt{M}}\sum_{m=0}^{M-1}\sum_{l=0}^{L-1} h_{n,m,l}^{RF} s_{n,<m-l>_M}\omega_M^{-m\overline{m}} + \overline{v}_{n,\overline{m}}. \end{aligned} \tag{37}$$

The FD matrix form is given by

$$\overline{\mathbf{y}}_n = \mathbf{F}_M\mathbf{y}_n = \sqrt{T}\overline{\mathbf{H}}_n^{RF}\overline{\mathbf{s}}_n + \overline{\mathbf{v}}_n, \tag{38}$$

where $\overline{\mathbf{y}}_n \in \mathcal{C}^{M\times 1}$, $\overline{\mathbf{s}}_n = \mathbf{F}_M\mathbf{s}_n \in \mathcal{C}^{M\times 1}$, $\overline{\mathbf{v}}_n = \mathbf{F}_M\mathbf{v}_n \in \mathcal{C}^{M\times 1}$, while $\overline{\mathbf{H}}_n^{RF} = \mathbf{F}_M\mathbf{H}_n^{RF}\mathbf{F}_M^H \in \mathcal{C}^{M\times M}$ is no longer diagonal in time-variant frequency-selective fading.

The FD-MMSE equalizer operated at the receiver gives

$$\overline{\mathbf{z}}_n = \left[\left(\overline{\mathbf{H}}_n^{RF}\right)^H\overline{\mathbf{H}}_n^{RF} + N_0\mathbf{I}_M\right]^{-1}\left(\overline{\mathbf{H}}_n^{RF}\right)^H\overline{\mathbf{y}}_n. \tag{39}$$

We note that when the MIMO fading channel is assumed to be time-invariant that ignores the Doppler effect, $\overline{\mathbf{H}}_n^{RF}$ of (38) becomes diagonal with $\overline{\mathbf{H}}_n^{RF}[\overline{m},\overline{m}] = \overline{h}_{n,\overline{m},\overline{m}}^{RF}$. Based on the OFDM subcarrier orthogonality assume, the FD received signal is given by $\overline{y}_{n,\overline{m}} = \overline{h}_{n,\overline{m},\overline{m}}^{RF}\overline{s}_{n,\overline{m}} + \overline{v}_{n,\overline{m}}$. Therefore, the conventional single-tap FDE operates based on

$$\overline{z}_{n,\overline{m}} = \left[\left(\overline{h}_{n,\overline{m},\overline{m}}^{RF}\right)^*\overline{h}_{n,\overline{m},\overline{m}}^{RF} + N_0\right]^{-1}\left(\overline{h}_{n,\overline{m},\overline{m}}^{RF}\right)^*\overline{y}_{n,\overline{m}}. \tag{40}$$

However, the full FD signal representation is $\overline{y}_{n,\overline{m}} = \sum_{\overline{m}'=0}^{M-1}\overline{h}_{n,\overline{m},\overline{m}'}^{RF}\overline{s}_{n,\overline{m}'} + \overline{v}_{n,\overline{m}}$, where the term of $\sum_{\forall\overline{m}'\neq\overline{m}}\overline{h}_{n,\overline{m},\overline{m}'}^{RF}\overline{s}_{n,\overline{m}'}$ would introduce ICI.

B. OTFS MIMO in Time-Varying Frequency-Selective THz Channel

As for the OTFS based on the OFDM Frame CP structure, the received signal after analog combining is as follows:

$$\begin{aligned} y_{n,m} &= \sqrt{T}\sum_{l=0}^{L-1} h_{n,m,l}^{RF} s_{<nM+m-l>_{MN}} \\ &+ \sqrt{T}\sum_{l=0}^{L-1} h_{n,m,l}^{RF} s_{0<nM+m-l>_{MN}} + \sqrt{1-T}s_{En,m} \\ &= \sqrt{T}\sum_{l=0}^{L-1} h_{n,m,l}^{RF} s_{<nM+m-l>_{MN}} + v_{n,m}. \end{aligned} \tag{41}$$

After performing DFT and SFFT at the receiver, the DD-domain signal is given by

$$\widetilde{y}_{k,l} = \sqrt{T}\sum_{p=0}^{P-1}\widetilde{h}_p^{RF}\widetilde{T}(k,l,k_p,l_p)\widetilde{s}_{<k-k_p>_N,<l-l_p>_M} + \widetilde{v}_{k,l}, \tag{42}$$

where $\widetilde{h}_p^{RF} = \sqrt{N_{Tx}N_{Rx}}\widetilde{h}_p \cdot \left[\left(\mathbf{w}^{Rx,RF}\right)^H\mathbf{a}_{Rx}\left(\theta_{Rx},p\right)\mathbf{a}_{Tx}^H\left(\theta_{Tx},p\right)\mathbf{w}^{Tx,RF}\right]$. The DD-domain input-output relationship cast in matrix form is hence given by

$$\widetilde{\mathbf{y}} = \sqrt{T}\widetilde{\mathbf{H}}^{RF}\widetilde{\mathbf{s}} + \widetilde{\mathbf{v}}, \tag{43}$$

where $\widetilde{\mathbf{y}} \in \mathcal{C}^{MN\times 1}$, $\widetilde{\mathbf{y}}[\kappa] = \widetilde{y}_{k,l}$, $\widetilde{\mathbf{s}} \in \mathcal{C}^{MN\times 1}$, $\widetilde{\mathbf{s}}[\kappa] = \widetilde{s}_{k,l}$, $\widetilde{\mathbf{v}} \in \mathcal{C}^{MN\times 1}$, $\widetilde{\mathbf{v}}[\kappa] = \widetilde{v}_{k,l}$, $k = \lfloor\frac{\kappa}{M}\rfloor$, $l = \kappa - kM$, $\widetilde{\mathbf{H}}^{RF} \in \mathcal{C}^{MN\times MN}$, $\widetilde{\mathbf{H}}^{RF}[\kappa,\iota] = \widetilde{h}_p^{RF}\widetilde{T}(k,l,k_p,l_p)$. Therefore, the DD-MMSE equalizer operates based on

$$\widetilde{\mathbf{z}} = \left[\left(\widetilde{\mathbf{H}}^{RF}\right)^H\widetilde{\mathbf{H}}^{RF} + N_0\mathbf{I}_{MN}\right]^{-1}\left(\widetilde{\mathbf{H}}^{RF}\right)^H\widetilde{\mathbf{y}}. \tag{44}$$

The MDR process is thereafter carried out based on (39), (40) and (44), which is similar to the SISO cases.

IV. Secret key rate analysis

The calculation of SKR in the OFDM CV-QKD systems documented in the literature [31], [33], [34], relies on the sum of M independent subchannel SKRs in time-invariant flat

[6] As in a MIMO scenario, the technique of analog precoding and combining is only used for providing a beamforming gain, but the input-output relationship is consistent with the aforementioned SISO OFDM and OTFS systems. Hence, a similar beam splitter model can be extended to their MIMO counterparts, which is shown in (35) and (41).

fading channels, since the OFDM subcarriers are orthogonal to each other. However, when the fading channel becomes time-variant in the face of the Doppler effect, especially when the Doppler frequency f_D becomes comparable to the subcarrier spacing Δf, the OFDM subcarrier orthogonality no longer holds. It is destroyed by the Doppler-induced ICI. Therefore, the SKR calculation of OFDM CV-QKD systems found in the literature is no longer valid in high-mobility scenarios. More explicitly, when quantum-safe services are provided for next-generation SAGIN [2]–[4], [40], more sophisticated solutions are sought. Against this background, we propose to mitigate this problem by using MMSE detection aided OFDM and OTFS schemes, where the effect of small-scale time-varying frequency-selective fading is equalized before SKR calculation. In this way, the classic single stream-based SKR calculation [18], [42], [51] may still be directly applied. Nonetheless, the FD-MMSE aided OFDM and DD-MMSE aided OTFS schemes have different residual noise levels, leading to different SKR performances.

Therefore, the SKR is defined as [52][7]

$$K_f = \gamma\left(1-P_B\right)\left[\beta I_{AB} - \chi_{BE} - \triangle\left(N_{\text{privacy}}\right)\right], \tag{45}$$

where γ denotes the fraction of key extractions within the total number of data exchanged by Alice and Bob, while P_B represents the BLER in the reconciliation step. Furthermore, I_{AB} is the classical mutual information between Alice and Bob based on their shared correlated data, and χ_{BE} represents the Holevo information that Eve can extract from the information of Bob[8]. Finally, $\triangle\left(N_{\text{privacy}}\right)$ represents the finite-size offset factor with the finite-size N_{privacy}. As for $\beta \in [0,1]$, it represents the reconciliation efficiency, which is defined as [53], [54]

$$\begin{aligned}\beta = \frac{R^{\text{eff}}}{C} &= \frac{R^{\text{eff}}}{\mathbb{E}\left[0.5\log_2\left(1+\text{SNR}^{Rx}\right)\right]}\\ &= \frac{R^{\text{eff}}}{\mathbb{E}\left[0.5\log_2\left(1+1/N_0^{Rx}\right)\right]},\end{aligned} \tag{46}$$

where R^{eff} represents the transmission rate and $R^{\text{eff}} = \left(1-\frac{M_{cp}}{M}\right)\cdot R$ for OFDM transmission and $R^{\text{eff}} = \left(1-\frac{M_{cp}}{MN}\right)\cdot R$ for OTFS transmission with R representing the coding rate, while C is referred to as the one-dimensional Shannon capacity [55], [56]. Furthermore, SNR^{Rx} represents the SNR after channel equalization by the receivers, which can be expressed as $\text{SNR}^{Rx} = 1/N_0^{Rx} = 1/N_0\Upsilon$. As for the noise variance N_0^{Rx}, it equals to $N_0/\left\|\overline{\ddot{h}}_i\right\|^2$, $\frac{\left\|\overline{\mathbf{G}}_n^{\varrho}[\overline{m},:]\right\|^2 N_0}{\left\|\overline{\mathbf{H}}_n^{\varrho'}[\overline{m},\overline{m}]\right\|^2}$, and $\frac{\left\|\widetilde{\mathbf{G}}^{\varrho}[\kappa,:]\right\|^2 N_0}{\left\|\widetilde{\mathbf{H}}^{\varrho'}[\kappa,\kappa]\right\|^2}$ based on (25), (29), and (30), when the FDE of OFDM, FD-MMSE of OFDM and DD-MMSE of OTFS receivers are used, respectively, while the corresponding coefficient Υ equals to $\left\|\overline{\ddot{h}}_i\right\|^2$, $\frac{\left\|\overline{\mathbf{H}}_n^{\varrho'}[\overline{m},\overline{m}]\right\|^2}{\left\|\overline{\mathbf{G}}_n^{\varrho}[\overline{m},:]\right\|^2}$, and $\frac{\left\|\widetilde{\mathbf{H}}^{\varrho'}[\kappa,\kappa]\right\|^2}{\left\|\widetilde{\mathbf{G}}^{\varrho}[\kappa,:]\right\|^2}$.

The calculations of I_{AB}, and χ_{BE} are similar to those in [18], [22], [23], [33], [42], [51]. To elaborate further, similar to [42], the total amount of noise between Alice and Bob ξ_{total} can be expressed as $\xi_{\text{total}} = \xi_{\text{line}} + \xi_{\text{det}}$, where $\xi_{\text{line}} = \frac{1-T}{T}W$ represents the impairment imposed by Eve, and W is the variance of the channel's noise [22]. Furthermore, $T = 10^{-\alpha\mathfrak{L}/10}$ represents the distance-dependent path loss, where α and $\mathfrak{L}$ represent the attenuation and distance between Alice and Bob, respectively. Moreover, $\xi_{\text{det}} = \frac{1-\eta}{\eta T}S$ is the homodyne detector's noise, where η represents the detection efficiency and S stands for the variance of the trusted detector's noise [18]. After taking the effect of imperfect detection stated above into account, the variance of Bob's received signal based on the single-tap equalization as shown in (5) can be represented as[9]

$$\begin{aligned}V_B &= \eta T\left(\|\overline{h}\|^2 V_A + \xi_{\text{total}}\right)\\ &= \eta T\|\overline{h}\|^2 V_A + \eta\left(1-T\right)W + \left(1-\eta\right)S,\end{aligned} \tag{47}$$

where $V_A = V_0 + V_s$ is the total variance of Alice's side, which contains the modulation variance[10] V_s and the thermal noise variance V_0. The variance of the thermal noise is given by $V_0 = 2\bar{n}+1$ with $\bar{n} = \left[\exp\left(\hbar f_c/k_B T_e\right)\right]^{-1}$, where $\hbar$ is Planck's constant, k_B is Boltzmann's constant, f_c is the carrier frequency and T_e is the environmental temperature in Kelvin. Furthermore, a more general expression may be formulated for the SNR at Bob's side, which is used in (7) based on (29), and it is harnessed in (18) based on (30), where FD and DD MMSE detectors are adopted for OFDM and OTFS respectively. This is as follows

$$\begin{aligned}V_B &= \eta T\left(\Upsilon V_A + \xi_{\text{total}}\right)\\ &= \eta T\Upsilon V_A + \eta\left(1-T\right)W + \left(1-\eta\right)S.\end{aligned} \tag{48}$$

We make the worst-case assumption that Eve can acquire perfect CSI knowledge and accordingly set $W = 1 + \frac{T(1-\Upsilon)V_0}{1-T}$, which is similar to that in [33]. Therefore, the mutual information between Alice and Bob can be obtained as follows:

$$\begin{aligned}I_{AB} =& \frac{1}{2}\log_2\left[1+\frac{\eta T\Upsilon V_s}{\eta T V_0 + \eta\left(1-T\right)+\left(1-\eta\right)S}\right]\\ =& \frac{1}{2}\log_2\left[\frac{\eta T(\Upsilon V_s + V_0) + \eta\left(1-T\right)+\left(1-\eta\right)S}{\eta T V_0 + \eta\left(1-T\right)+\left(1-\eta\right)S}\right],\end{aligned} \tag{49}$$

where the second term in $\log_2(\cdot)$ represents the receiver's SNR after equalization. Note that, V_s is adjustable in order to match the SNR required at the receiver by compensating the effect of fading channel gain Υ and loss T. Therefore we can rewrite $V_s' = \Upsilon V_s$ and $V_A' = V_s' + V_0$.

On the other hand, the Holevo information between Bob and Eve can be calculated as follows [54], [57]

$$\chi_{BE} = S(\rho_{AB}) - S(\rho_{A|B}), \tag{50}$$

where $S(\cdot)$ is the von Neumann entropy defined in [54],

[7] Note that (45) is the normalized SKR based on the bandwidth. As for the unnormalized SKR, it can be expressed based on (45) as $K_f^{\text{UN}} = B\cdot K_f$, where B represents the bandwith of the multi-carrier systems considered and we have $B = M\Delta f$. In our discussion normalized SKR results are used.

[8] It is assumed that the strongest attack [45], namely the so-called collective attack is used. Accordingly, Eve performs an optimal collective measurement on the collection of the stored ancilla after the key distillation procedure. Therefore, the Holevo information between Eve and Bob is harnessed as the evaluation metric for this kind of attack.

[9] The same as in the literature like [54], shot noise unit (SNU) is used as the unit to describe the power.

[10] The modulation variance here represents the variance of Gaussian signals used in the modulator of CV-QKD.

[57]. In light of this, the covariance matrix related to the information between Alice and Bob, i.e. the mode of ρ_{AB} after transmission through the quantum channel can be expressed as [54], [57]

$$\begin{aligned}\mathbf{V}_{AB} &= \begin{pmatrix} V_A'\mathbf{I}_2 & \sqrt{\eta T\left({V_A'}^2-1\right)}\mathbf{Z} \\ \sqrt{\eta T\left({V_A'}^2-1\right)}\mathbf{Z} & V_B\mathbf{I}_2 \end{pmatrix} \\ &= \begin{pmatrix} a\mathbf{I}_2 & c\mathbf{Z} \\ c\mathbf{Z} & b\mathbf{I}_2 \end{pmatrix},\end{aligned} \tag{51}$$

where we have:

$$\mathbf{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{52}$$

representing a pair of Pauli matrices. Therefore, the required symplectic eigenvalues of ρ_{AB} are given by [54], [57]

$$\lambda_{1,2}^2 = \frac{1}{2}\left(\Delta \pm \sqrt{\Delta^2 - 4D^2}\right), \tag{53}$$

where

$$\begin{aligned}\Delta &= a^2 + b^2 - 2c^2, \\ D &= ab - c^2.\end{aligned} \tag{54}$$

As for the symplectic eigenvalue of $\rho_{A|B}$, it can be shown that [54], [57]:

$$\lambda_3 = \sqrt{a\left(a - \frac{c^2}{b}\right)}. \tag{55}$$

Hence, the Holevo information can be formulated as

$$\chi_{BE} = G\left(\lambda_1\right) + G\left(\lambda_2\right) - G\left(\lambda_3\right), \tag{56}$$

where λ_1, λ_2 and λ_3 are symplectic eigenvalues and $G(*) = \left(\frac{*+1}{2}\right)\log_2\left(\frac{*+1}{2}\right) - \left(\frac{*-1}{2}\right)\log_2\left(\frac{*-1}{2}\right)$. Upon substituting (49) and (56) into (45), the corresponding SKR can be obtained.

Note that, the SKR analysis derived for MIMO scenarios obeys the same process as that for SISO scenarios, since the technique of analog precoding and combining is only used for providing a beanforming gain, but the input-output relationship is similar to that in the SISO case. In light of this, the SKR for MIMO scenarios can be derived using the process of (45), (49), and (50) with the aid of (39), (40) and (44) to derive the SNR at Bob's side.

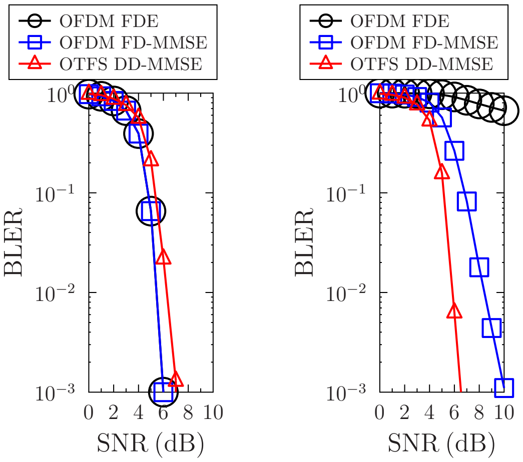
V. Performance analysis

In this section, a comprehensive parametric study of both THz OFDM and OTFS based CV-QKD is conducted. Explicitly, our BLER performance comparisons are presented for different multicarrier-based CV-QKD quantum transmission systems vs. the number of subcarriers M, FEC block length N_{FEC} 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 selected based on the seminal papers in the open literature [18], [22], [42], [58], [59]. Specifically, the attenuation coefficient α associated with the atmospheric path loss is set to 50 dB/km at 15 THz [18], [22][11]. Moreover, due to the limited number of scatters and high attenuation of the THz band [58]–[60], based on [60] we set the Ricean factor K to 0 dB. The FEC code length $N_{\text{FEC}} = 1024$ and the coding rate $R = 0.5$ are the same as in [42]. The CP length M_{cp} is set to $M_{cp} = L + 1$, where we have $L = \lceil \tau_{max} M \Delta f \rceil = 1, 2, 3$ for $M = 16, 32, 64$, respectively, and $P = L$.

TABLE III: Simulation parameters.

Parameter	Symbol	Value
Parameters for OFDM/OTFS		
The number of subcarrier	M	16,32,64
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}	1,4,8,16,32
The number of receiver antennas	N_{Rx}	1,4,8,16,32
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



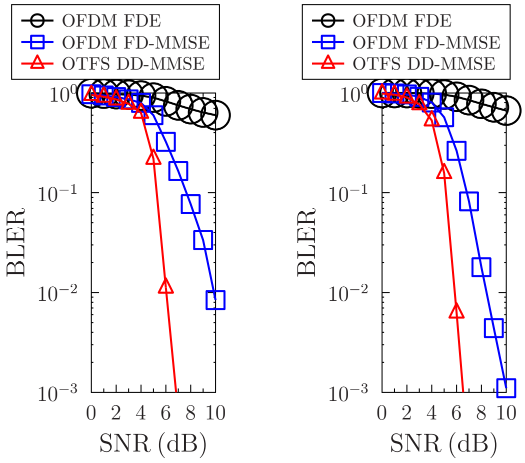
(a)

(b)

Fig. 5: Performance comparison between **SISO OFDM and OTFS-LDPC CV-QKD systems** in both (a) **stationary** ($v = 0$ m/s) and (b) **mobile** ($v = 30$ mph) scenarios, where $M = 64$ and $N = 16$ are used.

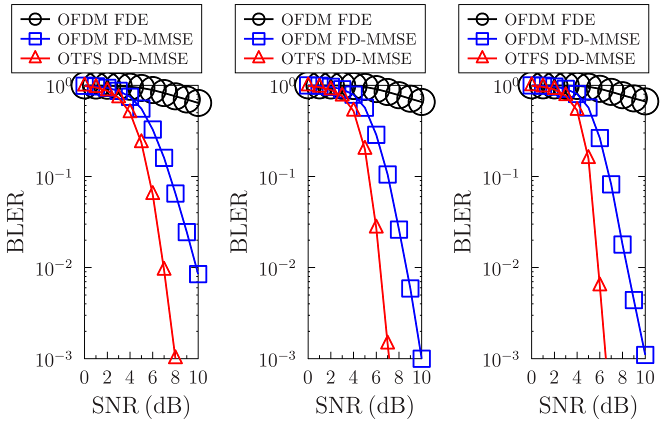
Fig. 5 provides our performance comparison between the OFDM and OTFS schemes employed by our LDPC-aided CV-QKD arrangement, where the user mobility is set to $v = 0$ mph for time-invariant fading and $v = 30$ mph for time-varying fading, respectively. Fig. 5 (a) demonstrates that all of the three

[11] In contrast to the THz wireless communication range spanning from 0.1 to 10 THz, the THz range investigated in the literature of QKD is wider, ranging from 0.1 to 50 THz [4], [18]. Therefore, the frequency set in our paper is chosen in line with [18], which exhibits low atmospheric loss and low thermal noise. Higher THz carrier frequencies are generally preferred for QKD, because the lower the frequency, the higher the thermal noise, which degrades the secure communication distance.



(a) (b)

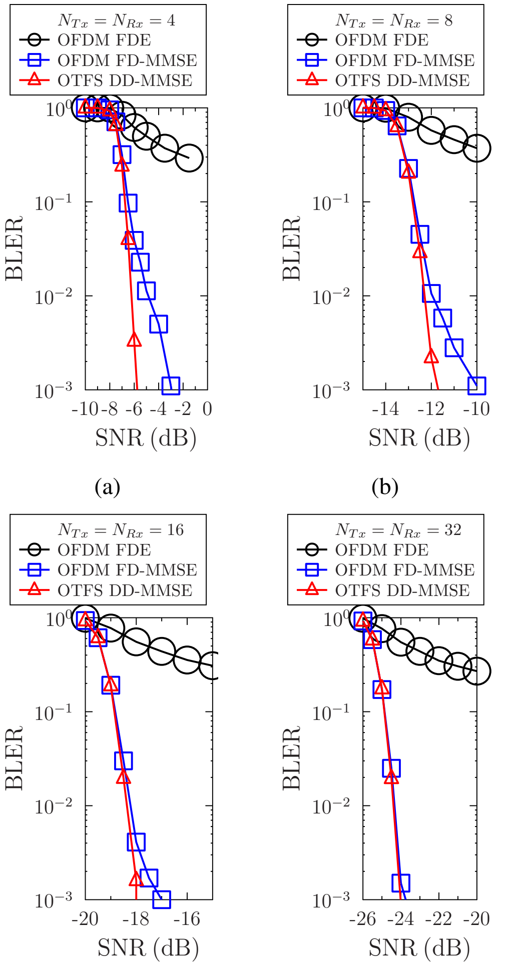
Fig. 6: Performance comparison between **SISO OFDM and OTFS-LDPC CV-QKD systems** in **mobile** scenario (v = 30 mph), where $N = 16$ and different number of subcarriers are used: (a) $M = 32$, (b) $M = 64$.



(a) (b) (c)

Fig. 7: Performance comparison between **SISO OFDM and OTFS-LDPC systems** with different block lengths of LDPC codes in **mobile** scenario (v = 30 mph), where $M = 64$ and $N = 16$ are used and we have: (a) $N_{\text{FEC}} = 256$, (b) $N_{\text{FEC}} = 512$, (c) $N_{\text{FEC}} = 1024$.

detectors of OFDM FDE, OFDM FD-MMSE and OTFS DD-MMSE achieve comparable performance, which is expected in the absence of mobility. However, Fig. 5 (b) evidences that in the mobile scenario associated with a user speed of v = 30 mph, the conventional OFDM single-tap FDE performs the worst, as OFDM subcarrier orthogonality no longer holds. As a remedy, the OFDM FD-MMSE scheme exhibits an improved performance in Fig. 5 (b), but OTFS DD-MMSE achieves the best performance in time-varying THz channels, as evidenced by Fig. 5 (b).



(a) (b)

(c) (d)

Fig. 8: Performance comparison between **MIMO OFDM and OTFS-LDPC systems** 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) $N_{Tx} = N_{Rx} = 8$, (c) $N_{Tx} = N_{Rx} = 16$, (d) $N_{Tx} = N_{Rx} = 32$.

Fig. 6 portrays our performance comparison between the OFDM and OTFS schemes employed by our LDPC-aided CV-QKD system using different numbers of subcarriers M in time-varying fading. Fig. 6 demonstrates that the BLER of our OFDM FD-MMSE based system using $M = 64$ performs better than that with $M = 32$ due to a higher gain obtained for more subcarrier. Nonetheless, the proposed OTFS scheme always performs the best in time-varying fading channels, as evidenced by Fig. 6.

Fig. 7 characterizes the effect of the FEC block length N_{FEC} on the BLER performance in the mobile (v = 30 mph) scenario. It demonstrates that the BLERs of the OFDM/OTFS detectors improve upon increasing N_{FEC}. More explicitly, take the OTFS DD-MMSE detection as an example. The SNR threshold to achieve a BLER of 10^{-3} decreases from 8.0 dB, to 7.0 dB and to 6.5 dB with N_{FEC} increasing from 256, 512 to 1024. Nonetheless, we note that the delay will also be increased with N_{FEC}, especially when an automatic repeat request (ARQ) mechanism is taken into account for retransmission if the decoding fails.

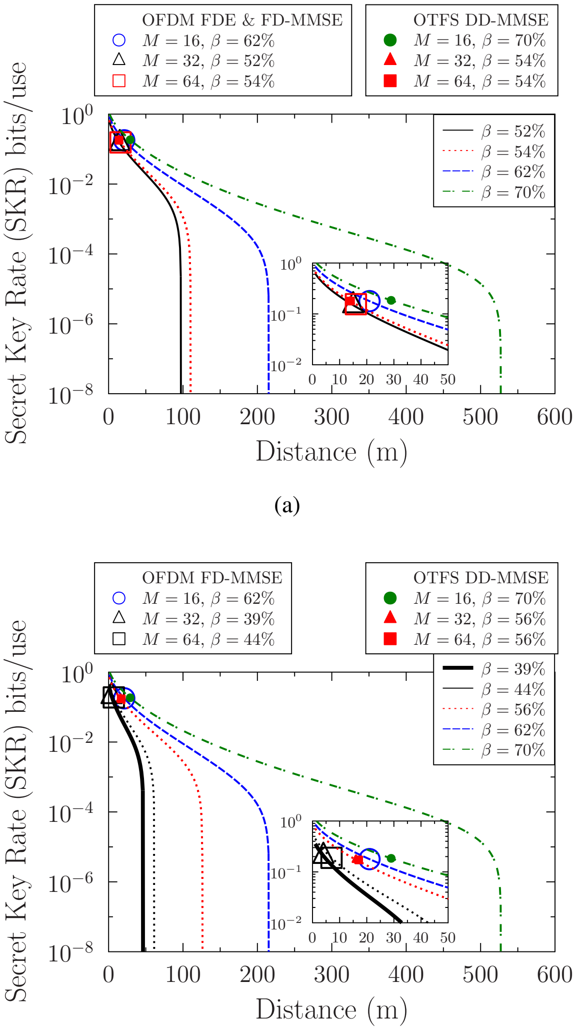
TABLE IV: Reconciliation efficiency comparison of different detection methods used in OFDM/OTFS CV-QKD system under different M and $N_{Tx} \times N_{Rx}$. The reconciliation efficiencies are calculated from Eq. (46) at the BLER threshold that equals to $\mathbf{10^{-1}}$, together with the corresponding SNRs. Note that both the stationary and mobile scenarios are considered with $v = 0, 30$ mph.

	$N_{Tx} \times N_{Tx}$	M_{FD}	OFDM FDE		OFDM FD-MMSE		OTFS DD-MMSE	
			SNR(dB)	$\beta(\%)$	SNR(dB)	$\beta(\%)$	SNR(dB)	$\beta(\%)$
SISO ($v = 0$ mph)	1×1	16	5.2	62.10	5.2	62.10	5.2	70.41
	1×1	32	4.8	52.18	4.8	52.30	5.4	54.38
	1×1	64	4.8	54.16	4.8	54.48	5.4	54.72
MIMO ($v = 0$ mph)	4×4	64	-6.8	64.79	-6.8	65.01	-6.8	69.78
	8×8	64	-12.8	65.90	-12.8	65.61	-12.8	70.05
	16×16	64	-18.8	65.73	-18.8	64.39	-18.8	69.84
	32×32	64	-24.8	65.54	-24.8	65.54	-24.8	69.63
SISO ($v = 30$ mph)	1×1	16	-	-	5.2	62.10	5.2	70.41
	1×1	32	-	-	7.5	38.94	5.2	55.56
	1×1	64	-	-	6.8	43.51	5.2	56.61
MIMO ($v = 30$ mph)	4×4	64	-	-	-6.5	63.25	-6.7	68.81
	8×8	64	-	-	-12.75	65.43	-12.8	70.05
	16×16	64	-	-	-18.8	65.73	-18.9	70.87
	32×32	64	-	-	-24.8	65.54	-24.8	69.63

Fig. 8 illustrates the effect of the MIMO size $N_{Tx} \times N_{Rx}$ on the BLER performance in a mobile (v=30 mph) scenario. Firstly, similarly to the SISO results of Fig. 5 (b), OTFS using DD-MMSE performed the best in MIMO systems, followed by OFDM with FD-MMSE and OFDM with single-tap FDE, as evidenced by Fig. 8. Secondly, Fig. 8 demonstrates that the BLER performance improves for all of the three OTFS/OFDM detectors, as the MIMO size increases. Specifically, it can be observed that the SNR threshold at a BLER of 10^{-1} is reduced from -6.8 dB, -12.8 dB, -18.9 dB to -24.8 dB with the increase of MIMO size from 4, 8, 16, to 32.

In order to investigate the effect of different parameters on the SKR, the pair of BLER and β, namely (BLER, β), are summarized in Table IV and Table V for both the stationary and mobile scenarios. We note that the BLER results of OFDM FDE recorded for both the SISO and MIMO based mobile scenarios are absent in Table IV and Table V owing to their error floors, as evidenced by Figs. 5-8. Based on this, Fig. 9 portrays the performances of the SKR versus distance for the SISO OFDM and OTFS based LDPC-aided systems using different numbers of subcarriers M in both stationary and mobile scenarios. The modulation variance is always kept at the optimal value, in the same way as in [44]. The other parameters are as follows [18], [22]: atmospheric loss $\alpha =$ 50 dB/km; room temperature $T_e = 296$ K; detector efficiency $\eta = 0.98$; detector's noise variance $S = 1$; $N_{\text{privacy}} = 10^{12}$. In Fig. 9 (a), there are four asymptotic theoretical SKR curves for different reconciliation efficiencies, which are 52%, 54%, 62%, and 70%, respectively. More explicitly, for the OFDM FDE and FD-MMSE based systems, they have the same reconciliation efficiency at the same setting, i.e. $\beta = 62\%,\ 52\%,\ 54\%$ for $M = 16,\ 32,\ 64$, respectively. For the OTFS DD-MMSE based one, the corresponding reconciliation efficiencies are $\beta = 70,\ 54,\ 54\%$ for $M = 16,\ 32,\ 64$, respectively. Therefore, as expected, similar SKR performance can be achieved under these six different modes, as shown in Fig. 9 (a), indicating around 20 meters of secure transmission distance. By contrast, in Fig. 9 (b), both the reconciliation efficiencies of the OFDM FD-MMSE with $M = 32$ and 64 decreased from $52\%,\ 54\%$ in Fig. 9 (a) to $39\%,\ 44\%$ in Fig. 9 (b). The corresponding efficiencies of the rest of the other modes remain the same. Therefore, there is a secure distance gap between the OFDM FD-MMSE based system and the OTFS DD-MMSE based scheme, indicating that the OTFS-based scheme using DD-MMSE detection outperforms the OFDM-based scheme relying on FD-MMSE detection in a mobile scenario.

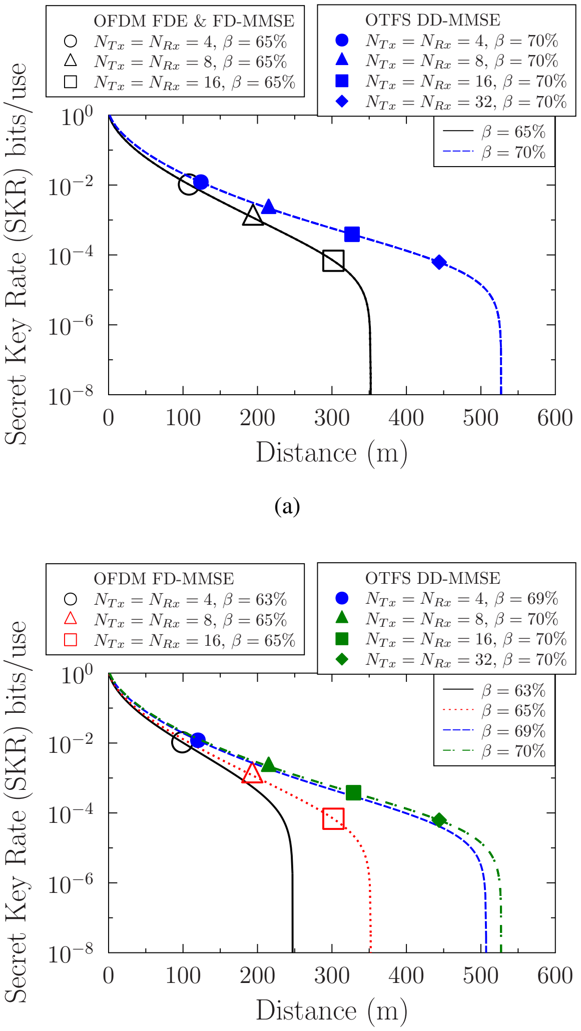
Fig. 10 (a) and Fig. 10 (b) demonstrate the SKR versus distance comparison between our MIMO OFDM and OTFS LDPC-aided systems using different detectors and MIMO sizes in both stationary and mobile scenarios, respectively. In Fig. 10 (a), there are two asymptotic theoretical SKR curves associated with different reconciliation efficiencies, which are 65% and 70%, respectively. Firstly, Fig. 10 (a) demonstrates that longer secure transmission distance is achieved by the OTFS-based CV-QKD system than by its OFDM counterpart in a stationary scenario as the OTFS-based CV-QKD system can provide higher reconciliation efficiencies than its OFDM counterpart, which can be seen in Table IV. Explicitly, the secure transmission distance of our OTFS system is around 120 meters (blue filled circle) in 4×4 MIMO setting, whereas the corresponding secure transmission distance of our OFDM system is around 110 meters (black circle) in 4×4 MIMO setting. Secondly, Fig. 10 (a) also confirms that the increased MIMO beamforming gain is capable of increasing the secure transmission distance for both OFDM and OTFS based CV-QKD systems. More explicitly, upon increasing the MIMO size from 4×4 to 8×8, 16×16 and 32×32, the secure transmission distance of OTFS-based system can be extended from 120 meters (blue filled circle), to 210 (blue filled triangle), 330 (blue filled square) and 450 meters (blue filled diamond), respectively, whereas the corresponding secure transmission distance of our OFDM system can be extended from 110 meters (black circle), to 190 meters (black triangle) and 300 meters (black square) in 4×4, 8×8 and 16×16 MIMO settings, respectively. However, for the OFDM system, the secure



(a)

(b)

Fig. 9: The SKR versus distance comparison between **SISO OFDM and OTFS-LDPC systems** using different detections and different number of subcarriers M with BLER equals to $\mathbf{10^{-1}}$ in Table IV, where $N = 16$, $f_c = 15$ THz, $N_{\text{FEC}} = 1024$ and $R = 0.5$ are used in the following scenarios: (a) $v = 0$ mph, (b) $v = 30$ mph.



(a)

(b)

Fig. 10: The SKR versus distance comparison between **MIMO OFDM and OTFS-LDPC systems** using different detections and different MIMO sizes with BLER equals to $\mathbf{10^{-1}}$ 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.

transmission distance can only be achieved by increasing the MIMO size to 16×16. This is because the low reconciliation efficiency of the OFDM-based system cannot support longer secure transmission distance, even though the larger MIMO 32×32 reduces the required SNR, as shown in Table IV.

Furthermore, in Fig. 10 (b), there are four asymptotic theoretical SKR curves having different reconciliation efficiencies, which are 63%, 65%, 69% and 70%, respectively. Similar conclusions can be made in doubly selective THz fading channels as that from Fig. 10 (a). This is evidenced by our simulation results. More explicitly, the secure transmission distance of our OTFS system is around 120 meters (blue filled circle), 210 meters (green filled triangle), 330 meters (green filled square) and 450 meters (green filled diamond) in 4×4, 8×8, 16×16 and 32×32 MIMO settings, respectively, whereas the corresponding secure transmission distance of our OFDM sytem is around 100 meters (black circle), 190 meters (red triangle) and 300 meters (red square) in 4×4, 8×8 and 16×16 MIMO settings, respectively.

To further investigate the effect of reconciliation efficiency on the secure transmission distance, Fig. 11 is portrayed based on the values in Table V, where the reconciliation efficiencies in a mobile scenario are collected based on the SNR threshold at a BLER of 10^{-2}. As shown in Fig. 11, all the reconciliation efficiencies are lower than those in Fig. 10 (b), since the SNRs threshold are higher than those in Fig. 10 (b), which can be seen by comparing Table IV and Table V. More explicitly, the reconciliation efficiencies are $65\%, 65\%$ and 66% for OTFS-based systems in 4×4, 8×8 and 16×16 MIMO settings, whereas the reconciliation efficiencies are 52% and 59% for

TABLE V: 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. (46) at the BLER threshold that equals to $\mathbf{10^{-2}}$, together with the corresponding SNRs. Note that both the mobile scenario is considered with $v = 30$ mph.

	$N_{Tx} \times N_{Tx}$	M_{FD}	OFDM FDE		OFDM FD-MMSE		OTFS DD-MMSE	
			SNR(dB)	$\beta(\%)$	SNR(dB)	$\beta(\%)$	SNR(dB)	$\beta(\%)$
MIMO ($v = 30$ mph)	4×4	64	-	-	-5	51.49	-6.25	64.53
	8×8	64	-	-	-12.0	58.81	-12.3	65.18
	16×16	64	-	-	-18.25	60.74	-18.4	65.92
	32×32	64	-	-	-24.4	61.86	-24.4	65.73

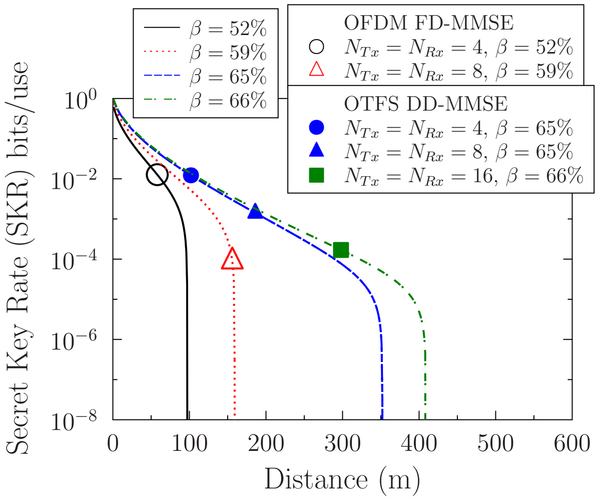


Fig. 11: The SKR versus distance comparison between **MIMO OFDM and OTFS-LDPC systems** using different detections and different MIMO sizes with BLER equals to $\mathbf{10^{-2}}$ in Table V, where $M = 64$, $N = 16$, $f_c = 15$ THz, $N_{\text{FEC}} = 1024$ and $R = 0.5$ are used in the mobile scenario with $v = 30$ mph.

OFDM-based systems in 4×4 and 8×8 MIMO settings. Therefore, the corresponding secure transmission distances for both OFDM and OTFS-based systems seen in Fig. 11 for different MIMO settings are shorter than those in Fig. 10 (b), indicating that the value of reconciliation efficiency plays a vital role in providing a long secure transmission distance.

VI. Conclusions

An OFDM/OTFS based LDPC assisted MDR CV-QKD system was conceived for transmission over time-variant frequency-selective THz channels. **Firstly**, it was demonstrated that the BLER is the same under three different OFDM/OTFS detectors in stationary ($v = 0$ mph) cases. The BLER of our OTFS DD-MMSE based system is the best, followed by that of the OFDM FD-MMSE based method. The BLER of OFDM using FDE detection is the worst in mobile ($v = 30$ mph) scenarios. **Secondly**, we investigated the effect of FEC block length. It was demonstrated that all the BLER performances are improved under all three different detectors upon increasing of the block length. However, the delay will be increased for a higher block length, especially when an ARQ mechanism is adopted for retransmissions if the decoding fails. **Thirdly**, it was demonstrated that the BLER performance will be improved upon increasing the MIMO size, thanks to the improved beamforming gain achieved by the MIMO OFDM/OTFS proposed for quantum transmission. **Lastly**, an SKR versus distance performance comparison was conducted. It was demonstrated that the OTFS-based system offers higher SKR and longer transmission distance than the OFDM-based system in both stationary and mobile ($v = 30$ mph) scenarios. Moreover, increasing the MIMO size can enhance the secure transmission distance for both the OFDM- and OTFS-based systems.

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] S. P. Kish, E. Villaseñor, R. Malaney, K. A. Mudge, and K. J. Grant, "Feasibility assessment for practical continuous variable quantum key distribution over the satellite-to-earth channel," *Quant. Eng.*, vol. 2, no. 3, p. e50, 2020.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

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

[12] 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.

[13] 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.

[14] M. Navascués, F. Grosshans, and A. Acin, "Optimality of Gaussian attacks in continuous-variable quantum cryptography," *Phys. Rev. Lett.*, vol. 97, no. 19, 2006, Article no. 190502.

[15] A. Leverrier, F. Grosshans, and P. Grangier, “Finite-size analysis of a continuous-variable quantum key distribution,” *Phys. Rev. A*, vol. 81, no. 6, 2010, Article no. 062343.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

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

[29] 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.

[30] 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.

[31] 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.

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

[33] 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.

[34] 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.

[35] 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, 2019.

[36] 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.

[37] 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.

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

[39] 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.

[40] 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 IoT-J.*, vol. 10, no. 1, pp. 682–703, 2023.

[41] 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. (accepted)*, 2024.

[42] 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.

[43] H. Mani, T. Gehring, P. Grabenweger, B. Ömer, C. Pacher, and U. L. Andersen, “Multiedge-type low-density parity-check codes for continuous-variable quantum key distribution,” *Phys. Rev. A*, vol. 103, p. 062419, Jun 2021.

[44] 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.

[45] 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, p. 022318, 2012.

[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. Surabhi and A. Chockalingam, “Low-complexity linear equalization for OTFS modulation,” *IEEE Commun. Lett.*, vol. 24, no. 2, pp. 330–334, 2019.

[50] 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.

[51] C. Weedbrook, S. Pirandola, and T. C. Ralph, “Continuous-variable quantum key distribution using thermal states,” *Phys. Rev. A - Atomic Mol., Opt. Phys.*, vol. 86, no. 2, pp. 1–12, 2012.

[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, 2018.

[53] 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.

[54] 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.

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

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

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

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

[59] 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.

[60] K. Guan, D. He, B. Ai, Y. Chen, C. Han, B. Peng, Z. Zhong, and T. Kuerner, “Channel characterization and capacity analysis for thz communication enabled smart rail mobility,” *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4065–4080, 2021.