WASABI: Widely-Spaced Array and Beamforming Design for Terahertz Range-Angle Secure Communications

Weijun Gao, Graduate Student Member, IEEE, Xuyang Lu, Member, IEEE, Chong Han, Member, IEEE, and Zhi Chen, Senior Member, IEEE

Abstract

Terahertz (THz) communications have naturally promising physical layer security (PLS) performance in the angular domain due to the high directivity feature. However, if eavesdroppers reside in the beam sector, the directivity fails to work effectively to handle this range-domain security problem. More critically, with an eavesdropper inside the beam sector and nearer to the transmitter than the legitimate receiver, i.e., in close proximity, secure communication is jeopardized. This open challenge motivates this work to study PLS techniques to enhance THz range-angle security. In this paper, a novel widely-spaced array and beamforming (WASABI) design for THz range-angle secure communication is proposed, based on the uniform planar array and hybrid beamforming. Specifically, the WASABI design is theoretically proved to achieve the optimal secrecy rate powered by the non-constrained optimum approaching (NCOA) algorithm with more than one RF chain, i.e., with the hybrid beamforming scheme. Moreover, with a low-complexity and sub-optimal analog beamforming, the WASABI scheme can achieve sub-optimal performance with less than 5% secrecy rate degradation. Simulation results illustrate that our proposed widely-spaced antenna communication scheme can ensure a 6 bps/Hz secrecy rate when the transmit power is 10 dBm. Finally, a frequency diverse array, as an advocated range security candidate in the literature, is proven to be ineffective to enhance range security.

Weijun Gao, and Chong Han are with the Terahertz Wireless Communications (TWC) Laboratory, Shanghai Jiao Tong University, China (email:{gaowei,jun, chong.hu}@sjtu.edu.cn).

Xuyang Lu is with the Laboratory of Ultrafast Integrated Systems (LUIS), Shanghai Jiao Tong University, China (email: xuyang.lu@sjtu.edu.cn).

Zhi Chen is with University of Electronic Science and Technology of China, China (email: chenzhi@uestc.edu.cn).
I. INTRODUCTION

A. Background

With an increasing demand for high-speed, reliable, and private information exchange, a new spectrum, as well as advanced security technologies, are awaited to be developed for next-generation wireless networks. The Terahertz (THz) band, with frequencies ranging from 0.1 to 10 THz, is envisioned to realize multi-Gbps or even Tbps data rates owing to the abundant bandwidth resource [1]–[3]. In addition to the bandwidth merit, the potential of THz communications to improve the information security is envisioned in [4], [5]. As a complementary technique for the conventional encryption-based methods, physical layer security (PLS) ensures information privacy at the physical layer of the wireless networks by exploiting transceiver and channel properties, including beamforming, fading, noise, and interference [6]. Compared with the encryption-based methods, the PLS has the advantage of owning reduced overhead for secret key distribution. Moreover, PLS can ensure information secrecy even with an eavesdropper (ED) having infinite computational power.

With the equipment of the ultra-massive multiple-input multiple-output (UM-MIMO) array for THz communications, the narrow and directional beams bring substantial benefits in PLS [5], [7], [8]. Typically, a THz beam is directed towards the legitimate user (LU) through the beam training and tracking processes, which keep the LU inside the beam sector to continuously benefit from the high beamforming gain. Since the beam width is narrow, e.g., approximately 1° for a $32 \times 32$ array, there is a high probability that the ED is located outside the beam. Under this circumstance, the ED captures fairly limited transmit power and can hardly decode confidential messages. Despite the promising confidentiality of THz communications with the ED outside the beam sector, it is still challenging when the ED is located inside the beam sector, for the following challenges [5]. First, the signals received by the ED inside the beam benefit from the same antenna gain as LUs, which suggests that the THz directivity is ineffective to enhance the security. Second, due to the sparsity feature of the THz channel, the PLS technique using multi-paths to aid the security proposed in [9] might not be useful. More critically, when the ED inside the beam sector is located near than the legitimate receiver, i.e., in close proximity, secure communication is significantly jeopardized, since the confidential codewords decodable by the LU are inevitably decodable by the ED with an even higher received signal-to-noise ratio (SNR) [8].
With an ED being located outside or inside the beam sector, the THz PLS can be divided into two categories, namely, *angle security* and *range security*, as illustrated in Fig. 1. On one hand, for the angle security, the aim is to prevent the ED from being located inside the beam sector, which improves the PLS in the angular domain. On the other hand, the range security aims at enhancing the secrecy rate when the LU and ED are both located inside the beam sector, i.e., when the propagation angles of LU and ED are the same while their ranges differ. Although the high directivity of THz communications can enhance the angle security, it fails to provide range security. This research gap motivates this work aiming at addressing both the angle and range security for THz communications.

**B. Related Work**

The fundamental limit of a wiretap channel model has been analyzed in [10] including a transmitter (Tx), a LU, and an ED, which is characterized by the *secrecy rate*, defined as the maximum data rate that can be transmitted reliably and confidentially. Traditional PLS technologies can only improve the secrecy rate for the angle security problem. For example, the secrecy capacity with the multiple antennas is calculated in [11], and the multi-antenna-based secure beamforming techniques are proposed in [12], which controls the beamforming pattern to enlarge the LU’s channel capacity while mitigating the ED’s capacity. In [13]–[16], as an extension to secure beamforming, the authors develop the artificial noise (AN)-aided beamforming technique to combat eavesdroppers in close proximity, where the AN signals
are signals without carrying any information. AN signals are designed to be injected into the transmitted confidential signal to jam the ED’s channel and enhance the secrecy rate.

Range security technologies, however, are rarely investigated for micro-wave band communications, since the micro-wave channel contains rich scattering, where angle security techniques are enough to mitigate the eavesdropping attacks. A receiver AN technique, where the receiver side sends the jamming signals while receiving the confidential signals, has been proposed in [17]–[19] as a useful range security technique. However, this technique requires a high-complexity self-interference cancellation (SIC) to simultaneously transmit the AN signal and receive the information signal. We proposed another range security technique, the distance-adaptive molecular absorption modulation (DA-APM) scheme, which hides the signal under the molecular absorption peaks in the THz band [7]. In recent years, frequency diverse array (FDA) has been recognized as a good candidate to address the security problem. By introducing a small frequency offset among different antennas in the antenna array, FDA shows a periodically range-, angle-, and time-varying beam pattern. FDA has been widely used in radar and navigation applications by taking advantage of the time-varying property. From the PLS perspective, thanks to its range-varying beam pattern, FDA is recently envisioned as a potential technique to enhance the information security. For example, The FDA beamforming approach is proposed in [20] to safeguard wireless transmission for proximal LU and ED, where the FDA is used to distinguish two proximal receivers to increase the secrecy rate. However, in Sec. V of this work, we prove and demonstrate that the FDA and any multiple antenna techniques operating in the far-field regions cannot provide range security.

Despite the studies found in the literature, an effective and low-complexity range-angle technique in the THz band is awaited to be explored. First, most conventional security techniques cannot be applied for range security due to their requirement on an uncorrelated LU’s and ED’s channels, which is not available for the range security. Second, the DA-APM scheme in [7] cannot provide range security when the ED is in near proximity of the Tx. Finally, despite the effectiveness of the receiver AN technique on addressing the THz range-angle security with the ED in close proximity, it brings additional hardware complexity and needs cooperation among the Tx and the LU [8].
C. Motivations and Contributions

To fill the gap, we propose a widely-spaced antenna and beamforming (WASABI) design, to enhance the THz range-angle security. Specifically, the THz hybrid beamforming based on ultra-massive uniform planar arrays (UM-UPA) is used to provide security in the angular domain, and a widely-spaced array (WSA), instead of a densely-packed antenna array, is applied to provide THz range security. The WSA explores additional spatial degrees of freedom (SDoF) at the cost of increasing transceiver size [21], [22]. The additional SDoF can help decouple the LU’s and ED’s channels and thereby combat the range security problem. Thanks to the sub-millimeter wavelengths of THz waves, the THz WSA phased array still has a reasonable size, which makes it more practical to implement. In addition to the WASABI scheme, we investigate FDA, as an advocated range security candidate, is ineffective to provide THz range-angle security, and extend this conclusion to the general multiple antenna techniques operating in the far-field regions. The concrete contributions of this paper are summarized as follows:

- **We develop a THz end-to-end secure communication model.** Specifically, the considered end-to-end secure communication model includes components from the baseband modulator and hybrid beamformer to the baseband demodulator at the receiver side. Moreover, a secrecy rate maximization problem is formulated, based on which the challenges on THz range-angle security are elaborated.

- **We propose a novel WASABI scheme to enhance the THz range-angle security.** The advantage of implementing WSA in the THz band is demonstrated. Moreover, we propose a hybrid beamforming strategy and a corresponding chip layout for our WSA scheme, where a non-constrained optimum approaching (NCOA) algorithm is developed to solve the non-convex optimization problem.

- **We compare our proposed scheme with the existing PLS techniques.** Monte-Carlo simulation demonstrates the convergence of the proposed NCOA algorithm. Extensive numerical results show that for a propagation distance at 10 m and transmit power of 10 dBm, the proposed method can achieve a secrecy rate of 6 bps/Hz, while the conventional antenna array fails to guarantee range security.

- **The ineffectiveness of FDA on providing the range security is proven.** We further extend this conclusion to the general multiple antenna techniques that any signal processing or multiple antenna techniques operating in the far-field regions are ineffective in providing
range security.

![Fig. 2: THz UM-UPA system.](image)

![Fig. 3: THz wireless secure communication system: End-to-end block diagram.](image)

The remainder of the paper is organized as follows. Sec. II presents the system model. The proposed WSA communication scheme is proposed in Sec. III where the NCOA hybrid beamforming algorithm is elaborated. Numerical results are described in Sec. IV to verify the convergence of the proposed algorithm and the secrecy rate enhancement compared with existing methods. Sec. V proves that the FDA and any multiple antenna techniques operating in the far-field regions cannot provide range security. The paper is concluded in Sec. VI.

Notations: matrices and vectors are denoted by boldface upper and lower case letters, respectively. $[\cdot]^+ \triangleq \max(0, \cdot)$. $\langle \cdot, \cdot \rangle$ denotes inner product. $*$ is the convolution operation. $A^*$, $A^T$, and $A^\dagger$ are the conjugate, transpose, and conjugate transpose of the matrix $A$, respectively.

II. SYSTEM MODEL

We consider a THz secure communication scenario, as shown in Fig 2, which consists of a Tx, an LU, and an ED. Thanks to the small wavelength of the THz signal in the order of millimeter down to sub-millimeter, a UM-UPA is equipped at the Tx side to overcome the large propagation loss. We assume that the UM-UPA is comprised of $N_{Tx} = N_x \times N_y$ antennas aligning uniformly in a rectangular shape, with $N_x$ antennas in each row and $N_y$ antennas in each column. The uniform antenna spacing between neighboring antennas is denoted by $d$. For analysis simplicity, we assume that the UM-UPA is vertically placed on the horizontal plane, while the LU and ED are located on the horizontal plane. The positions of the LU and the ED are represented by $(D_r, \theta_r)$, where the notation $r \in \{LU, ED\}$ denotes the receiving node as the LU or the ED.
The distance between the Tx and the node r is denoted by $D_r$. Moreover, $\theta_r$ defines the angle between the LoS propagation path and the array normal plane.

A. End-to-end Block Diagram

The block diagram of the considered end-to-end secure communication system is shown in Fig. 3, which includes a Tx baseband modulator, a hybrid beamformer realized by the UM-UPA, the THz channel, and a receiver module performing synchronization, down-conversion, and demodulation, elaborated as follows.

1) Baseband Modulation: As the input of the secure communication system, a discrete symbol stream $s_k$ represents the normalized coded confidential symbols to transmit satisfying $E[|s_k|^2] = 1$, where $E[\cdot]$ returns the expectation. The symbols are modulated into a baseband waveform $m(t)$ given by

$$m(t) = \sum_{k=-\infty}^{\infty} s_k \cdot g\left(t - kT_s\right),$$

where $k$ is the symbol identification number, $g(\cdot)$ represents the normalized pulse shape, and $T_s$ denotes the symbol time. We consider that the baseband bandwidth $B_g = 1/T_s$ is smaller than the coherence bandwidth, which implies narrowband communications.

2) Hybrid Beamforming: Since traditional fully-digital beamformer requires the same number of radio frequency (RF) chains as antennas [23], which brings tremendous hardware cost for THz communications, hybrid beamforming technology is therefore proposed as a promising yet lower-complexity structure for UM-UPA [24]. Specifically, the fully-connected hybrid beamforming structure is composed of a digital beamformer represented by $P_D \in \mathbb{C}^{N_{RF} \times 1}$ and an analog beamformer expressed as $P_A \in \mathbb{C}^{N_{Tx} \times N_{RF}}$. Each element of the matrices $P_D$ and $P_A$ represents the complex gain from the baseband signal to the RF chain, and from the RF chain to the antenna via phase shifters, respectively. $N_{RF}$ denotes the number of RF chains. The analog beamformer matrix is expressed in the form of

$$P_A = \frac{1}{\sqrt{N_{Tx}}} \begin{pmatrix} e^{j\phi_{11}} & \cdots & e^{j\phi_{1N_{RF}}} \\ \vdots & \ddots & \vdots \\ e^{j\phi_{N_{Tx}1}} & \cdots & e^{j\phi_{N_{Tx}N_{RF}}} \end{pmatrix},$$

where $\phi_{pq} \in [0, 2\pi), p \in \{1, \cdots, N_{Tx}\}, q \in \{1, \cdots, N_{RF}\}$ denotes the phase output of the phase shifter connecting the $p^{th}$ RF chain and the $q^{th}$ antenna. We assume that the hybrid beamforming
does not affect the transmit power, i.e., $\|\mathbf{P}_A \mathbf{P}_D\|^2 = 1$. The overall beamforming vector is denoted by

$$\mathbf{w} = [\mathbf{P}_A \mathbf{P}_D]^* \triangleq [w_1, \ldots, w_{N_{\text{Tx}}}]^T.$$  
(3)

With the equipment of an omnidirectional UM-UPA with carrier frequency denoted by $f_c$, the transmit signal matrix represented by $\mathbf{x} = [x_1, \ldots, x_{N_{\text{Tx}}}]^T$ is therefore expressed as

$$x_i(t) = \sqrt{P} m(t) w_i^* (t) e^{-j2\pi f_c t},$$  
(4)

where $P$ denotes the transmit power, $x_i(t)$ denotes the signal transmitted by the $i$th antenna.

3) Terahertz Channel: Due to the sparsity of the THz channel and the high directivity, the path gains of the reflected, scattered, and diffracted paths are negligible weak compared to the LoS path. Thus, it is reasonable to model the THz channel impulse response $h_{\text{LoS}}(t)$ with only a LoS path \cite{25}–\cite{27}, as

$$h_{\text{LoS}}(t, D) = a(f, D) \delta \left(t - \frac{D}{c}\right),$$  
(5)

where $a(f, D) = \frac{c}{4\pi f D}$ denotes the free-space LoS path gain with frequency $f$ and propagation distance $D$ according to Friis’ law. $c$ denotes the light speed. To simplify the notations, we use $a(D)$ to represent $a(f, D)$.

4) Synchronization and Demodulation: At the receiver side, the received signal at node $r \in \{\text{LU, ED}\}$ is given by

$$y_r(t) = \sum_{i=1}^{N_{\text{Tx}}} x_i(t) * h_{\text{LoS}}(t, D_{ir}^*) + n_r(t),$$  
(6)

where $D_{ir}^*$ denote the distance between the $i$th antenna and the receiver node $r \in \{\text{LU, ED}\}$. $n_r(t)$ stands for the additive Gaussian white noise (AWGN) noise variance $\sigma_r^2$. In this work, we assume that the noise variances for the LU and the ED are the same and both equal to $\sigma^2$, i.e., $\sigma_{\text{LU}}^2 = \sigma_{\text{ED}}^2 = \sigma^2$. After down-converting the received signal from $f_c$ and synchronization, the received baseband waveform signal $m_r(t)$ is expressed as

$$m_r(t) = y_r(t) * \delta \left(t + \frac{D_t}{c}\right) e^{2\pi f_c t},$$  
(7)

We apply the narrowband consideration, where the time delay between different antennas is much smaller than the codeword length, and thus $m \left(t - \frac{D_{ir}^*}{c}\right) \approx m \left(t - \frac{D_i}{c}\right)$ and $w_i \left(t - \frac{D_{ir}^*}{c}\right) \approx$
$w_i \left( t - \frac{D_i}{c} \right)$. By combining (1)-(7), the received baseband signal $m_r(t)$ is calculated as

$$m_r(t) = \sqrt{P} m(t) a(D_r) w^T H_r + n(t), \quad (8)$$

where the channel combining matrix $H_r$ is expressed as

$$H_r = \left[ e^{j2\pi \frac{i\Delta D_i^r}{c}}, \ldots, e^{j2\pi \frac{i\Delta D_{Nrx}^r}{c}} \right]^T, \quad (9)$$

where $\Delta D_i^r \triangleq D_i^r - D_r$ is defined as the relative propagation distance of the $i^{th}$ antenna with respect to the reference antenna. The closed-form expression for $\Delta D_i^r$ is represented by

$$\Delta D_i^r = \sqrt{D_i^2 - 2i_{row} d D_r \sin \theta_r + (i_{row}^2 + i_{col}^2) d^2} - D_r \quad (10a)$$

$$\approx -i_{row} d \sin \theta_r + O \left( \frac{d}{D_i^r} \right), \quad (10b)$$

where $i_{row} = i \mod N_y - 1$ and $i_{col} = (i - i_{row} - 1)/N_y$. Remarkably, (10a) is the ground-truth model, since it considers the spherical-wave propagation nature for EM waves. (10b) is obtained based on the first-order Taylor expansion to approximate the spherical wave front as a planar one. This planar-wave propagation model exhibits high accuracy when $d \ll D_i^r$, and therefore is widely used in conventional beamforming schemes due to its simplicity.

**B. Problem Formulation: Secrecy Rate Maximization**

The secrecy rate, defined as the capacity difference between LU’s and ED’s channels, is used as the performance metric of our THz system model. As the focus of our THz secure communication system, the aim is to design transmit power $P$, hybrid beamformer, i.e., $P_A$ and $P_D$, to maximize the secrecy rate. Thus, we formulate the hybrid secure beamforming design problem as a secrecy rate maximization (SRM) optimization problem $Q_1$ as

$$Q_1: \max_{P, P_D, P_A} R_s = \left[ \log \left( 1 + P \frac{\|\mathbf{w}^H \mathbf{H}_{LU}\|^2 a(D_{LU})^2}{\sigma^2} \right) - \log \left( 1 + P \frac{\|\mathbf{w}^H \mathbf{H}_{ED}\|^2 a(D_{ED})^2}{\sigma^2} \right) \right]^+$$

s.t. $P \leq P_{tx}$, \[ (11a) \]

$$\|P_A P_D\|^2 = 1, \quad (11b)$$

$$\|P_A P_D\|^2 = 1, \quad (11c)$$
\[
P_A = \frac{1}{\sqrt{N_{\text{Tx}}}} \begin{pmatrix} e^{j\phi_1} & \cdots & e^{j\phi_{N_{\text{RF}}}} \\ \vdots & \ddots & \vdots \\ e^{j\phi_{N_{\text{Tx}}}} & \cdots & e^{j\phi_{N_{\text{Tx}}N_{\text{RF}}}} \end{pmatrix} = \frac{1}{\sqrt{N_{\text{Tx}}}} e^{j\Phi},
\]

where (11a) denotes the secrecy rate of the THz secure communication system, and the operation \([x]^+ \triangleq \max(x, 0)\). (11b) states the transmit power constraint with the maximum power \(P_{\text{Tx}}\). (11c) describes the normalization constraint of a hybrid beamformer. The maximal secrecy rate is denoted by \(R^\text{opt}_s\) and the optimal transmit beamformer is represented by \(w^\text{opt} = [P^\text{opt}_A P^\text{opt}_D]^*\).

Solving the problem \(Q_1\) yields the optimal hybrid beamforming strategy achieving the maximum secrecy.

This secure beamforming design poses two challenges. First, due to the non-convexity of (11a) and the stringent beamformer constraint (11d), the optimization problem \(Q_1\) is non-convex and cannot be tackled directly. Second, even though the optimal secrecy rate is obtained, the optimized beamformer cannot provide the range security when the planar-wave propagation model (10b) is applied. According to (9), for the range security problem where \(\theta_{\text{LU}} = \theta_{\text{ED}}\), if the planar-wave propagation model (10b) is applied, \(\Delta D^{i}_{\text{LU}} = \Delta D^{i}_{\text{ED}}\) and the LU’s and ED’s channels are perfectly correlated, i.e., \(H_{\text{LU}} = H_{\text{ED}}\). As a result, their beamforming gains satisfy \(|w^\dagger H_{\text{LU}}|^2 = |w^\dagger H_{\text{ED}}|^2\).

Therefore, by considering that \(|w^\dagger H_i|^2 \in [0, N_{\text{Tx}}]\), the maximum secrecy rate is upper bounded by \(\left[ \log \left( 1 + \frac{P_{\text{Tx}} N_{\text{Tx}} a(D_{\text{LU}})^2}{\sigma^2} \right) \right]^+ - \left[ \log \left( 1 + \frac{P_{\text{Tx}} N_{\text{Tx}} a(D_{\text{ED}})^2}{\sigma^2} \right) \right]^+\), which is exactly the maximum secrecy rate without adopting any security technique. Moreover, if \(D_{\text{ED}} < D_{\text{LU}}\), the secrecy rate is zero, which implies that the secure beamforming assuming planar-wave assumption cannot provide the range security.

### III. WIDELY-SPACED ANTENNA COMMUNICATIONS FOR TERAHERTZ RANGE-ANGLE SECURITY

In this section, we propose a THz WASABI scheme to safeguard the THz range-angle secure communications. Specifically, We first demonstrate that the WSA structure can help decouple the LU’s and ED’s channels and combat the range security problem. To highlight, we clarify that the proposed scheme is realistic yet unique for THz band communications. We then provide a hybrid beamforming design strategy for our WSA transmission scheme based on a NCOA algorithm. Finally, we present a chip design diagram for the fully-connected beamformer.
A. Spherical-wave Propagation in the Terahertz Band

The failure of secure beamforming based on planar-wave propagation is due to the fact that the channel matrix $H_r$ only depends on the angle $\theta_r$, which leads that the LU’s and ED’s channels are perfectly correlated for the range security problem. Motivated by this fact, our idea is to enable the spherical-wave propagation to realize channel decoupling. This can be realized by deploying a WSA, which widens the antenna spacing $d$ such that the planar-wave approximation (10b) to the spherical-wave propagation is invalid. We consider the following requirement that the approximation error of the planar-wave propagation from the spherical-wave propagation approximates to half wavelength, expressed as

$$ |\Delta D_{r, \text{spherical}}^{N_{Tx}} - \Delta D_{r, \text{planar}}^{N_{Tx}}| \approx \frac{\lambda}{2}, $$

where $\lambda$ denotes the wavelength, $\Delta D_{r, \text{spherical}}^{N_{Tx}}$ and $\Delta D_{r, \text{planar}}^{N_{Tx}}$ denote the expressions of $\Delta D_{r, \text{spherical}}^{N_{Tx}}$ applying the spherical-wave and planar-wave assumptions in (10a) and (10b), respectively.

Thanks to the millimeter down to sub-millimeter THz wavelength, THz band communications can maintain a reasonable array size even when this stringent requirement (12) on the spherical-wave propagation is satisfied. For a $4 \times 4$ micro-wave communication system where the wavelength is on the order of sub-meters, e.g., 0.3 m for the 1 GHz system, this requirement is valid when the side length of the array $3d \approx 4.0$ m, which is an impractically large antenna array. However, for THz communications, with a wavelength on the order of millimeter, e.g., 1 mm for a 300 GHz system, the planar-wave assumption is valid when $3d \approx 0.08$ m. Therefore, a $0.08 \text{ m} \times 0.08 \text{ m}$ THz antenna array can well accommodate the spherical-wave propagation requirement.

B. Hybrid Beamforming Design: NCOA Algorithm

We design a hybrid beamformer to maximize the secrecy rate in (11a) for our WSA transmission scheme. Given the transmission distances $D_{LU}$ and $D_{ED}$, solving the SRM problem $Q_1$ yields our hybrid beamformer design. We propose an NCOA algorithm to solve this non-convex problem. First, we temporarily relax the non-convex constraint and transform $Q_1$ into a convex optimization problem $Q_2$. A globally optimal solution $\tilde{w}$ to $Q_2$ is derived, referred to as the non-constrained optimum. Then, by reconsidering the non-convex constraint, a sub-optimal solution is achieved by approaching $\tilde{w}$. 

1) Problem Transformation and Non-constrained Optimal Solution: We first temporarily neglect the constraint (11d). As a result, the remaining problem is converted to a convex optimization problem where a global optimum can be derived in a closed form. By maximizing the transmit power $P = P_{Tx}$ and allowing the condition that $\|w\|^2 = 1$, the secrecy rate in (11a) is calculated as

$$R_s = \log \left[ 1 + \frac{w^\dagger \left( H_{LU} H_{LU}^\dagger \cdot a(D_{LU})^2 - H_{ED} H_{ED}^\dagger \cdot a(D_{ED})^2 \right) w}{w^\dagger \left( \sigma^2 I + H_{ED} H_{ED}^\dagger \cdot a(D_{ED})^2 \right) w} \right],$$

where $\sigma^2 > 0$. Let $A \triangleq H_{LU} H_{LU}^\dagger a(D_{LU})^2 - H_{ED} H_{ED}^\dagger a(D_{ED})^2$ and $B \triangleq \sigma^2 I + H_{ED} H_{ED}^\dagger a(D_{ED})^2$, maximizing $R_s$ is equivalent to maximizing the generalized Rayleigh quotient $\lambda_{\Sigma} \triangleq w^\dagger A w / w^\dagger B w$. The transformation of the optimization problem from $Q_1$ to $Q_2$ is depicted in the following theorem.

**Theorem 1:** The SRM problem $Q_1$ without the non-convex constraint (11c) is equivalent to the problem $Q_2$

$$Q_2 : \max_w \lambda_{\Sigma} = |\langle w', v^{(a)} \rangle|^2 \lambda_a + |\langle w', v^{(b)} \rangle|^2 \lambda_b$$

$$\|w\|^2 = 1,$$

where $w' = B^{-1/2} w / \| B^{-1/2} w \|$, $\lambda_a$ and $\lambda_b$ denote the only two non-zero eigenvalues of the matrix $B^{-1/2} A B^{-1/2}$ with $\lambda_a \geq \lambda_b$. $v^{(a)}$ and $v^{(b)}$ represent their corresponding normalized eigenvectors, respectively.

**Proof:** The detailed proof is provided in Appendix A. 

Since $|\langle w', v^{(a)} \rangle| \leq |\langle v^{(a)}, v^{(a)} \rangle| = 1$, the non-constraint optimal solution to $Q_2$ is achieved when $w'$ coincides with the eigenvector of the maximum eigenvalue $v^{(a)}$. This leads the non-constrained optimal solution as

$$\hat{w} = B^{-1/2} v^{(a)} / \| B^{-1/2} v^{(a)} \|, \quad \lambda_{\Sigma} = \lambda_a, \quad R_s = \log_2 (1 + \lambda_a),$$

where setting the beamforming matrix as $\hat{w}$ achieves the maximum secrecy rate, which is an upper bound for the secrecy rate maximization problem $Q_1$.

2) NCOA Algorithm: Given the non-constrained optimal solution $\hat{w}$, our aim is to approach $w = [P_A^{\text{opt}} P_D^{\text{opt}}]^*$ to $\hat{w}$ under the analog beamforming constraint (11d). In [24], it is shown that when $N_{RF} \geq 2$, there exists a solution $P_A$ and $P_D$ that satisfies $[P_A P_D]^* = \hat{w}$. Therefore, we divide the two cases, (i) the hybrid beamforming case where $N_{RF} \geq 2$, and (ii) the fully-analog
(FA) beamforming case where \( N_{RF} = 1 \), as follows.

Case (i): For the hybrid beamforming case \( N_{RF} \geq 2 \), fortunately, it is possible to discover feasible solutions satisfying the constraint (11d) and \( \tilde{w} = \left[ P_A P_D \right]^* \), one of which is expressed as

\[
P_{HA}^{HB} = \left[ e^{j \angle \tilde{w} + \arccos \frac{\| \tilde{w} \|}{2}}, e^{j \angle \tilde{w} - \arccos \frac{\| \tilde{w} \|}{2}}, \ldots, 0 \right]^T, \tag{16a}
\]

\[
P_{HD}^{HB} = \frac{1}{\sqrt{2}} [1, 1, 0, \ldots, 0]^T, \tag{16b}
\]

where \( \angle(\cdot) \) returns the angle of the input complex element. By setting the hybrid beamformer as (16), the non-constrained optimal solution can be achieved, and the secrecy rate performance of the hybrid beamforming is maximized. According to (16), it is worth noticing that by using the first two RF chains, the hybrid beamforming achieves the optimal performance. Furthermore, using more than two RF chains cannot further improve the secrecy rate. This is consistent with intuitive understanding that for one Tx and two single-antenna LU and ED with LoS transmissions, there are two SDoFs, which equal to the DoF between Tx and LU plus the DoF between Tx and ED. Therefore, with two or more RF chains exceeding the number of SDoFs, the WSA communication system cannot further benefit from the increased RF chains.

Case (ii): For the fully-analog beamforming case with \( N_{RF} = 1 \), since \( P_{DA}^{FA} \) is a \( 1 \times 1 \) scalar number, we set \( P_{DA}^{FA} = 1 \) without loss of generality. Then, the solution \( P_{A}^{FA} = \tilde{w}^* \) does not satisfy the constraint in (11d). We use a gradient descent algorithm to recursively approach the optimal solution, where the gradient of the term (14a) versus \( P_A \) is represented by

\[
\nabla P_{A}^{FA} = \left[ \frac{\partial \lambda_S}{\partial \phi_1}, \ldots, \frac{\partial \lambda_S}{\partial \phi_{N_{Tx}}} \right]^T, \tag{17}
\]

where the term \( \frac{\partial \lambda_S}{\partial \phi_i} \) is expressed as

\[
\frac{\partial \lambda_S}{\partial \phi_i} = -\frac{2}{\sqrt{N_{Tx}}} \sum_{k \in \{a, b\}} \text{Re} \left( v_k^{B} P_{A}^{FA} e^{-j \phi_i} e_v^B \right) \lambda_k, \tag{18}
\]

where \( v_k^B = \frac{B^{-1/2} v^{(k)}}{\| B^{-1/2} v^{(k)} \|} \), and the vector \( e_i = [0, \ldots, 0, 1, 0, \ldots, 0] \) with the one in the \( i^{th} \) column, \( \text{Re}(\cdot) \) returns the real part of a complex number. By recursively updating \( P_{A}^{FA} \) via computing the gradient in each step, a near-optimal solution for the fully-analog case can be achieved.

By combining the two solutions for the hybrid beamforming (\( N_{RF} \geq 2 \)) and fully-analog beamforming (\( N_{RF} = 1 \)) cases, the NCOA algorithm for the hybrid beamforming design is
Algorithm 1. $\epsilon$ denotes the step parameter controlling the convergence speed, and $\delta$ is the convergence threshold determining the convergence destination. In this work, we choose $\epsilon = 10$ rad and $\delta = 0.003$, which results in good convergence performance. By applying WSA communications for range security and considering the narrow beam nature with a UM-UPA, the range-angle security for THz communications is thereby ensured.

Algorithm 1 NCOA Algorithm

**Input:** $D_{LU}$, $D_{ED}$, $\theta_{LU}$, $\theta_{ED}$  
**Output:** $P_{opt}$, $P_{A}^{opt}$, $P_{D}^{opt}$, $R_{s}^{opt}$

1: Compute the channel matrix $C = B^{-\frac{1}{2}}AB^{-\frac{1}{2}}$ given $D_{LU}$ and $D_{ED}$;
2: Perform eigenvalue decomposition (EVD) on $C$ to compute $\lambda_{a}$, $\lambda_{b}$, $v^{(a)}$, and $v^{(b)}$;
3: Case I Hybrid beamforming: when $N_{RF} \geq 2$,
4: Compute $P_{A}^{HB}$, $P_{D}^{HB}$ according to (16);
5: Compute $\lambda_{\Sigma}$ according to (14a);
6: Output $P_{opt} = P_{Tx}$, $P_{A}^{opt} = P_{A}^{HB}$, $P_{D}^{opt} = P_{D}^{HB}$, $R_{s}^{opt} = \log(1 + \lambda_{\Sigma})$;
7: Case II Fully-analog beamforming: when $N_{RF} = 1$,
8: $P_{D}^{FA} = 1$;
9: Randomly initialize $P_{A,0}^{FA}$, and compute $\lambda_{\Sigma,0}$;
10: repeat
11: Compute $\nabla P_{A,i}^{FA}$ and $\lambda_{\Sigma,i}$ according to (17);
12: Update $P_{A,i+1}^{FA} \leftarrow P_{A,i}^{FA} + \epsilon \nabla P_{A,i}^{FA}$;
13: Compute $\lambda_{\Sigma,i+1}$;
14: $i \leftarrow i + 1$;
15: until $|\lambda_{\Sigma,i+1} - \lambda_{\Sigma,i}| / |\lambda_{\Sigma,i}| < \delta$;
16: Output $P_{opt} = P_{Tx}$, $P_{A}^{opt} = P_{A,i+1}^{FA}$, $P_{D}^{opt} = 1$, $R_{s}^{opt} = \log(1 + \lambda_{\Sigma,i+1})$;

C. Chip Design Diagram for WASABI

Due to the optimality of a two-RF-chain hybrid beamforming WSA array, we present a chip design diagram for this special case. Fully-connected hybrid beamforming chip design is challenging due to a large number of on-chip interconnections between RF chains and the antenna array. Overlapping interconnections among different RF chains undergo strong self-interference. To address these challenges, we propose a chip design diagram of the hybrid beamformer for THz WSA communication scheme as illustrated in Fig. 4 including the following two parts. For the digital beamformer and the RF chain, we follow the traditional design for the fully-digital beamformer, where the digital beamformer precodes the baseband signal, and the precoded signal is up-converted to the carrier frequency, as demonstrated in Fig. 4(a). For the analog beamformer part, we propose a fully-connected analog beamformer structure, which synthesizes two phased
array networks, including the locally coupled network [28] and the H-type network. The locally coupled network is composed of radiating elements, with each element locally connected with a THz oscillator and connected to its neighboring row and column elements. The H-type network is a traditional phased array, where one local oscillator is connected to every radiating element through an H-shaped path.

An advantage of this hybrid network is that the overlapped interconnections between the two networks are minimized. As demonstrated in Fig. 4(b), the locally coupled network occupies all direct connections between two neighboring elements, while the H-type network occupies perpendicular bisectors between elements. Therefore, this structure minimizes the overlapped interconnections. The antenna pattern with a target direction at 30° is illustrated in Fig. 5. If setting the Tx-ED distance as 5 m, we can create a null point at 5 m inside the beam by designing a proper beamforming matrix. This point experiences a 15 dB beamforming gain reduction compared to the maximum gain. This phenomenon implies that if the ED is inside the beam sector and 5 m far from the Tx, the ED cannot perform effective eavesdropping. Combining with the fact that the beam width is less than 1°, the WASABI scheme shows good security performance both in the angular and range domain.

IV. NUMERICAL RESULTS

In this section, we evaluate numerical results of the WASABI for THz secure communications. First, we conduct Monte Carlo simulations on our recursion-based NCOA algorithm and demonstrate its convergence performance. Second, we analyze how system parameters, including
Fig. 5: Illustration of WSA antenna pattern to achieve the range-angle security.

**TABLE I: Simulation Parameters**

| Notation | Definition                          | Value | Unit |
|----------|-------------------------------------|-------|------|
| $P_{\text{Tx}}$ | Maximum transmit power             | 10    | dBm  |
| $N_x$    | Number of row antennas             | 32    | -    |
| $N_y$    | Number of column antennas          | 32    | -    |
| $N_{\text{Tx}}$ | Total number of antennas     | 1024  | -    |
| $\sigma^2$ | Noise variance                    | -80   | dBm  |
| $\theta_{\text{LU}}$ | Tx-LU angle                     | $\pi/6$ | rad |
| $f_c$    | Carrier frequency                  | 300   | GHz  |
| $D_{\text{LU}}$ | Tx-LU distance                   | 10    | m    |
| $D_{\text{ED}}$ | Tx-ED distance                   | 5     | m    |
| $\epsilon$ | Step parameter                   | 10    | rad  |
| $\delta$ | Convergence threshold             | 0.003 | -    |

the maximum transmit power, antenna spacing, and transmission distances affect the maximum secrecy rate. Moreover, the robustness of the proposed WSA scheme is studied, i.e., how the maximum secrecy rate degrades with the estimation error of the location of the ED. Finally, the WASABI scheme is compared with existing algorithms to demonstrate its improved range-angle security performance. Unless specified, the system parameters used in the simulation are described in Table I.
A. Convergence Analysis of the NCOA Algorithm

To demonstrate the feasibility of the NCOA algorithm, we need to verify the convergence performance of the used gradient descent method. First, to verify the convergence, we perform Monte Carlo simulations on the initial value of $P_{FA,0}$ in step 9 of Algorithm 1. By setting different random initial values over 1,000 times, we plot the secrecy rates achieved by the solution versus the number of iterations, as depicted in Fig. 6. Fig. 6(a) plots 100 realizations randomly chosen from 1,000 realizations for illustration, where we observe that all simulations achieve nearly the same maximum secrecy rate within 20 iterations. This implies good convergence performance. Fig. 6(b) presents statistical analysis on the distribution of the total number of iterations until convergence. Among 1,000 simulations, a Gaussian distribution with a mean of 20 is fitted, while no alias effect occurs.

In Fig. 7, we explore how the step parameter $\epsilon$ in step 12 in Algorithm 1 affects the maximum secrecy rate and the total iteration step reaching the termination condition. For each $\epsilon$, 100 Monte Carlo simulations are performed to calculate the mean secrecy rate. We can observe that when $\epsilon < 20$, the mean secrecy rate approximately reaches the maximum value. By contrast, when $\epsilon > 20$, the mean secrecy rate decays rapidly. This is due to the fact that a large iteration step $\epsilon$ leads to an early convergence before the secrecy rate approaches the maximum. Moreover, the number of total iteration steps decreases as $\epsilon$ increases, as the right y-axis of Fig. 7 presents. The numerical results demonstrate that setting $\epsilon$ within [10, 20] results in a good balance between
Fig. 7: Mean secrecy rate and total iteration steps versus step parameter $\epsilon$.

Fig. 8: Secrecy rate versus different system parameters ($N_{RF} = 2$). (a) With varying antenna spacing $d$. (b) With varying Tx-ED distance $D_{ED}$. (c) With varying array size $N_t$.

B. Maximum Secrecy Rate

We compute the maximum secrecy rate versus different system parameters for our proposed WASABI scheme for THz range-angle security. The maximum secrecy rates with different maximum transmit power values are shown in Fig. 8(a) for the different antenna spacing, in Fig. 8(b) for the different eavesdropping distances, and in Fig. 8(c) for the different antenna array sizes. In general, the secrecy rate increases with a wider antenna spacing, a nearer ED distance, and a larger array size. Moreover, with $d = 5\lambda$, $D_{ED} = 5$ m, and $N_{Tx} = 1024$, the secrecy rate with maximum transmit power of 10 dBm is 6 bps/Hz. An interesting phenomenon captured in Fig. 8(b) is that as $D_{ED}$ becomes smaller, i.e., the ED approaches the Tx, the secrecy shows an increasing trend. This is explained that when the ED is nearer from the Tx or
equivalently, farther from the LU, the ED’s channel is more uncorrelated with the LU’s channel, which enhances the secrecy rate though the ED’s channel gain increases.

Since the proposed NCOA algorithm needs to acquire the eavesdropper’s location, i.e., the Tx-ED distance and angle, we should estimate these two values as the input of our beamformer design. We study the robustness of our scheme to the estimation errors of Tx-ED distance and angle. The estimation error is defined as the difference between the estimated value and the nominal value. The estimation errors of the Tx-ED distance and angle are denoted as $D_{\text{ED}}^{\text{error}}$ and $\theta_{\text{ED}}^{\text{error}}$, respectively. The maximum secrecy rates versus $D_{\text{ED}}^{\text{error}}$ and $\theta_{\text{ED}}^{\text{error}}$ are plotted in Fig. 9. In our simulations, the true Tx-ED distance and angle are 5 m and 30°, respectively. In Fig. 9(a), we observe that as the Tx-ED distance estimation error increases, the secrecy rate degrades dramatically. Moreover, we see that as $D_{\text{ED}}$ decreases, the degradation becomes severer with the estimation error at short transmission distances. This can be explained that at short distances, a small distance estimation error leads to a large phase error on each antenna. In Fig. 9(b), we observe that for the different Tx-ED distances, the maximum secrecy rate degrades by 10% when the Tx-ED angle has a $\pm 0.03^\circ$ error. This result implies that the robustness of the WASABI scheme to the Tx-ED estimation error is highly dependent on the Tx-ED distance. Moreover, it is suggested that the estimation error of the Tx-ED angle should be less than $0.03^\circ$ to ensure a less than 10% secrecy rate degradation.
C. Performance Comparison With Different Methods

Finally, we evaluate and compare the maximum secrecy rate achieved by our proposed WASABII scheme with existing schemes in the literature. Specifically, the transmit AN scheme [15], the SIC-free receiver AN scheme [8], and traditional antenna array hybrid beamforming method [24] are compared in Fig. 10. The transmit power of the receiver AN signal for the SIC-free receiver AN scheme is 10 dBm. In Fig. 10(a), the secrecy rate versus the Tx-LU distance is plotted. Moreover, the hybrid beamforming ($N_{RF} \geq 2$) and fully-analog beamforming ($N_{RF} = 1$) cases of our WASABII secure beamforming scheme are computed to demonstrate the sub-optimal performance of fully-analog beamforming structure with respect to the optimal hybrid beamforming case. For the $N_{RF} \geq 2$ case, the maximum secrecy rate decreases as $D_{LU}$ increases. At $D_{LU} = 10$ m, the secrecy rate achieves 6 bps/Hz. The secrecy rate of the $N_{RF} \geq 1$ case, as an inferior but low-complexity architecture of the $N_{RF} = 2$ case, can achieve near-optimal performance when $D_{LU}$ is larger than 8 m. This implies that the performance degradation due to the sub-optimality of hybrid beamforming becomes severer when the distance between the Tx and the LU is small. Moreover, compared with the SIC-free receiver AN scheme [8], the proposed WASABII scheme can double the secrecy rate at $D_{LU} = 10$ m. This significant improvement is originated from the different security-enhancing strategies used by the two schemes. Specifically, the WASABII scheme directly mitigates the received power by the ED, while the SIC-free receiver AN is to jam the ED’s signal. We observe that the secrecy rates achieved by the transmit AN scheme...
and traditional hybrid beamforming are nearly zero, which is consistent with our analysis in Sec. II-B that the secure communication in the far field fails to achieve a positive secrecy rate.

In Fig. 10(b), we plot the maximum secrecy rate versus the different Tx-ED distances varying from 0.5 m to 20 m, where the Tx-LU distance is 10 m. We see that when $D_{ED}$ increases from 0.5 m to 10 m, the secrecy rate of WASABI scheme decreases as $D_{ED}$ increases. Moreover, the secrecy rate increases as $D_{ED}$ increases when $D_{ED}$ is larger than 10 m. This is due to the fact that as $D_{ED}$ approaches 10 m, the LU’s channel and the ED’s channel become correlated, which leads that the WASABI scheme cannot distinguish the two receivers in the range domain. Moreover, the WASABI scheme with two RF chains can achieve the secrecy rate of approximately 6 bps/Hz, as $D_{ED}$ approaches zero. However, this does not imply that the proposed scheme can effectively combat the extremely near eavesdropping, since the robustness against the Tx-ED distance estimation error degrades significantly as $D_{ED}$ approaches to zero.

V. CAN FREQUENCY DIVERSE ARRAY ENHANCE TERAHERTZ RANGE SECURITY?

In this section, we explore whether the FDA technique, as an advocated candidate for range security, is effective in enhancing THz range security. FDA features its range-, angle-, and time-dependent array factor, which has the capability to steer the beam automatically. In terms of range-angle security, the range-dependency of the beam can simultaneously enhance the received SNR at the LU while mitigating the received SNR at the ED since the antenna gain of FDA periodically changes with the distance \cite{20}. As a result, the range security can seem to improve with the aid of FDA. However, this intuitive understanding of FDA-aided range security is problematic. Due to the different Tx-LU and Tx-ED propagation distances, the same piece of confidential information does not reach LU and ED at the exactly same time. Instead, there is a $\frac{D_{LU}-D_{ED}}{c}$ time delay, as demonstrated in Fig. 11. Let $m(t)$ denote the confidential signal transmitted at time $t$, then the received signal at LU and ED are $m(t - \frac{D_{LU}}{c})$ and $m(t - \frac{D_{ED}}{c})$, respectively, which do not correspond to the same piece of confidential information.

Since the confidential message is modulated on the EM wave which travels at the speed of light, we should investigate the joint range-time beam pattern of FDA instead of a “snapshot” one. Unfortunately, although the FDA has a range-varying and time-varying beam pattern, the joint range-time beam pattern propagating at the speed of light is constant, as depicted in Eq. (2) of \cite{20}, where the FDA beam pattern is only dependent on the term $t - \frac{r}{c}$. 
A. Ineffectiveness of Frequency Diverse Array on Range Security

We rigorously prove the ineffectiveness of FDA on range security based on the analysis of an FDA secure communication system. We replace the uniform-frequency array in Sec. II with an FDA to reconstruct the system model for FDA and reformulate an FDA-based secrecy rate maximization problem. Specifically, the carrier frequency of the \( i \)th antenna is represented by \( f_i = f_c + \Delta f_i \), where \( \Delta f_i \ll f_c \) denotes the small frequency offset for FDA. The transmit signal of the \( i \)th antenna is therefore expressed as

\[
x_i(t) = \sqrt{P_m(t)} w_i^* (t) e^{-j2\pi f_i t},
\]

By combining (19) and (5)-(7), the channel combining matrix for FDA is given by

\[
H_{FDA}^r = H_r \otimes H_{TV}(t) \otimes H_{Res}^r,
\]

where \( \otimes \) denotes the Hadamard product, \( H_r \) is the beamforming matrix in (9) and the matrices \( H_{TV}, \) and \( H_{Res}^r \in \mathbb{C}^{N_{Tx} \times 1} \) are represented as

\[
H_{TV}(t) = \begin{bmatrix}
e^{-j2\pi \Delta f_1 t}, & \cdots, & e^{-j2\pi \Delta f_{N_{Tx}} t}
\end{bmatrix}^T,
\]

\[
H_{Res}^r = \begin{bmatrix}
e^{j2\pi \frac{\Delta f_{1}\Delta D_1}{c}}, & \cdots, & e^{j2\pi \frac{\Delta f_{N_{Tx}}\Delta D_{N_{Tx}}}{c}}
\end{bmatrix}^T,
\]

where the matrix \( H_{TV}(t) \) represents the time-varying term, making the total beam pattern time-varying due to the diverse frequency among antennas. Moreover, \( H_{TV}(t) \) does not depend on the receiving node, implying that the time-varying gains are the same at the LU and the ED.
The matrix $H^{\text{Res}}$ in (22) is denoted as the residual term, due to the fact that $\Delta f_i \ll f_c$. Thus, the elements in this matrix are negligibly small compared with $H_r$ and $H_{TV}(t)$. The secrecy rate maximization problem with FDA is formulated as

$$Q^\text{FDA} \ni \max_{P,P_D,P_A} R_s = \left[ \log \left( 1 + \frac{P \left| w^\dagger H^{\text{FDA}}_{LU} a(D_{LU})^2 \right|^2}{\sigma^2} \right) - \log \left( 1 + \frac{P \left| w^\dagger H^{\text{FDA}}_{ED} a(D_{ED})^2 \right|^2}{\sigma^2} \right) \right]^+$$

(23a)

s.t. (11b) - (11d).

(23b)

To prove the ineffectiveness of FDA for range security, we prove that the maximum secrecy rate of FDA communications denoted by $R^{\text{opt}}_{s,FDA}$ is equal to that of the uniform-frequency array, as presented in Theorem 2. Note that we apply the planar-wave propagation assumption (10b), and the relation $\Delta D_{LU} = \Delta D_{ED}^r$ is satisfied. This statement is valid when the Tx-LU and Tx-ED links are both in the far-field regions.

**Theorem 2.** For range security where $\theta_{LU} = \theta_{ED}$, the maximal secrecy rate of FDA is equal to that of a uniform-frequency array, i.e., $R^{\text{opt}}_{s,FDA} = R^{\text{opt}}_s$. Moreover, the optimal design parameters for FDA satisfy

$$P^{\text{opt}}_{\text{FDA}} = P^{\text{opt}},$$

(24a)

$$P^{\text{opt}}_{D,FDA} = P^{\text{opt}}_D,$$

(24b)

$$P^{\text{opt}}_{A,FDA} = P^{\text{opt}}_A \otimes \left( H_{TV}(t) 1_{N_{RF}} \right) \otimes \left( H^{\text{Res}}_{LU} 1_{N_{RF}} \right),$$

(24c)

$$\phi^{\text{opt}}_{pq,FDA} = \phi^{\text{opt}}_{pq} - 2\pi \Delta f_p \left( t - \frac{\Delta D_p^r}{c} \right),$$

(24d)

where $1_{N_{RF}}$ denotes the all-one $1 \times N_{RF}$ vector.

**Proof:** The detailed proof is provided in Appendix B.

This theorem implies that by introducing diverse frequency among multiple antennas, the secrecy rate does not increase, which suggests that FDA cannot bring any additional benefit to range security. This result seems contradictory to the conclusion drawn in some related work [29]. We argue the proper way to compute the true secrecy rate is to perform an end-to-end analysis on the FDA system, especially considering the synchronization process which can compensate for the time of arrival deviation as (7) represents. As a result, the end-to-end beam pattern captured by (20) do not demonstrate a range-dependent feature, which prevents FDA from
enhancing range security. Furthermore, (24d) in Theorem 2 implies that the additional phase introduced by the frequency offset of FDA is completely canceled by the analog beamformer. This reminds us of the equivalence of a constant frequency and a time-varying phase from the signal processing perspective, i.e., without the consideration of different hardware implementation, the added frequency offset $\Delta f$ is the same as adding the phase by $\Delta ft$. Therefore, FDA with beamforming cannot address the THz range security problem.

**B. Ineffectiveness of General Multiple Antenna Techniques on Range Security**

We extend our findings on the ineffectiveness of FDA on range security to the general multiple antenna techniques. To this end, we provide a different interpretation on the multiple antenna propagation process. Specifically, the THz LoS signal propagation process can be manually divided into the propagation in two phases, as depicted in Fig. 12(a). In the first phase, the transmitted signals on each antenna are combined on the plane perpendicular to the direction of propagation in the near-field region. In the second phase, the combined signal further propagates and is finally received by LU and ED. Based upon this interpretation, the combining of signals from different antennas is assumed to happen before the second phase, which indeed happens at the end of the first phase. The correctness of our interpretation is verified as follows. The signals at the receivers neglecting the noise term in (6) can be expressed as,

$$y_r(t) = \sum_i x_i(t) * \delta \left( t - \frac{D_i}{c} \right) \cdot a(D_t)$$

(25)
where $\Delta D^i_r = D^i_r - D_r$. $x^r_{\text{comb}}$ denotes the combined signal at the perpendicular plane at the end of phase I for the receiving node $r$. Note that in the far-field regions, the combined signal on the plane for different receivers is considered to be identical, i.e., $x^L_{\text{comb}} = x^E_{\text{comb}}$. Thus, as indicated by (27), the original wiretap channel model can be represented as a cascaded wiretap channel scheme as shown in Fig. 12(b). The cascaded wiretap channel exhibits as two Markov chains, e.g., $\text{TX} \rightarrow X \rightarrow \text{LU}$ and $\text{TX} \rightarrow X \rightarrow \text{ED}$, where $X$ represents the intermediate node at the end of the first phase. Based on the Markov chains, the secrecy rate transmitted from $\text{Tx}$ to $\text{LU}$ with the existence of the ED satisfies

$$R^\text{TX}_{s} = \max_{\text{TX}} I(\text{TX}; \text{LU}) - \max_{\text{TX}} I(\text{TX}; \text{ED})$$

$$\leq \max_{X} I(X; \text{LU}) - \max_{X} I(X; \text{ED})$$

$$= \log \left(1 + \frac{P_X a(D_{LU})^2}{\sigma^2_{LU}}\right) - \log \left(1 + \frac{P_X a(D_{ED})^2}{\sigma^2_{ED}}\right),$$

where $P_X$ denotes the maximum signal power of the combined signals at node $X$. (28) implies that the secrecy rate from node $\text{Tx}$ is upper-bounded by the secrecy rate from node $X$ and $P_X = \mathbb{E} [\|x_{\text{comb}}(t)\|^2] \leq N_{\text{TX}} P$, whose secrecy capacity is equal to that of a fully-digital beamforming scheme. This phenomenon proves that any signal processing and multiple antenna techniques operating in the far-field regions cannot provide THz range security. This further proves the ineffectiveness of FDA on improving the range security in Sec. V-A.

**VI. CONCLUSION**

In this paper, we have explored new technologies for THz range-angle security, which remains an open problem in the literature. Specifically, we have performed an end-to-end analysis on THz secure communication systems. First, we propose a WASABI scheme and a chip design to realize range-angle security. The WSA transmission is realized by increasing the antenna spacing to decouple the LU’s and ED’s channels. This leads that the LU and the ED are in the near-field propagation region, where the spherical-wave propagation model is invoked. To solve
the non-convex SRM problem for the optimal hybrid beamformer design, we develop an NCOA algorithm to achieve the closed-form optimal solution for the hybrid beamforming case and an epsilon-convergent sub-optimal solution for the fully-analog beamforming case, respectively. Numerical results verify the outstanding convergence of the NCOA algorithm and demonstrate that with the transmit power as 10 dBm and the legitimate distance as 10 m, the secrecy rate of the WASABI communication scheme reaches 6 bps/Hz. Finally, we prove that the FDA technique or any multiple antenna techniques operating in the far-field region cannot bring any benefit to THz range security.

APPENDIX A
PROOF OF THEOREM 1

Due to the monotonicity of the logarithmic function, Maximizing $R_s$ in (11a) is equivalent to maximizing $\frac{w^\dagger A w}{w^\dagger B w}$. First, we prove the existence of the matrix $B^{-\frac{1}{2}}$. Since for any non-zero vector $x$, we have $x^\dagger B x = x^\dagger \frac{\sigma^2}{P_{tx}} I x + x^\dagger H_{ED} H_{ED}^\dagger x \cdot a(D_{ED})^2 = \sigma^2 \frac{P_{tx}}{\|x\|^2} + \|H_{ED}^\dagger x\|^2 \cdot a(D_{ED})^2 > 0$, $B$ is positive definite, and $B^{-\frac{1}{2}}$ exists. Thus, we can assume $w' = \frac{B^{\frac{1}{2}} w}{\|B^{\frac{1}{2}} w\|}$ and $C = B^{-\frac{1}{2}} A B^{-\frac{1}{2}}$, we have $w^\dagger A w = w'^\dagger C w'$. We first prove that $\text{rank}(C) = 2$, which implies that $C$ only has two non-zero eigenvalues. First, since the ranks of vector $H_{LU}$ and $H_{ED}$ are 1, $\text{rank}(H_{LU} H_{LU}^\dagger) = \text{rank}(H_{ED} H_{ED}^\dagger) = 1$. Therefore, $\text{rank}(A) = \text{rank}(H_{LU} H_{LU}^\dagger a(D_{LU})^2 - H_{ED} H_{ED}^\dagger a(D_{ED})^2) = 2$. Second, since the identity matrix $I$ has full rank and $H_{ED} H_{ED}^\dagger a(D_{ED})^2$ is a Hermitian matrix, the matrix $B$ as well as $B^{-\frac{1}{2}}$ have full rank. As a result, $C$ is a rank-2 matrix, and there are two non-zero eigenvalues. We denote the two eigenvalues as $\lambda_a$ and $\lambda_b$ with their corresponding eigenvectors $v^a$ and $v^b$.

Next, we decompose the vector $w'$ onto the orthonormal basis, composed of all normalized
eigenvectors of $C$ denoted by $\{v^{(i)}\}, i = 1, \cdots, N_{Tx}$. As $w' = \sum_{i=1}^{N_{Tx}} \langle w', v^{(i)} \rangle v^{(i)}$, we can write

$$w'^T C w' = \left( \sum_{i=1}^{N_{Tx}} \langle w', v^{(i)} \rangle v^{(i)} \right) \left( C \sum_{j=1}^{N_{Tx}} \langle w', v^{(j)} \rangle v^{(j)} \right)$$

$$= \left( \sum_{i=1}^{N_{Tx}} \langle w', v^{(i)} \rangle v^{(i)} \right) \left( \sum_{j=1}^{N_{Tx}} \langle w', v^{(j)} \rangle \lambda_j v^{(j)} \right)$$

$$= \sum_{i,j} \langle w', v^{(i)} \rangle \langle w', v^{(j)} \rangle \langle v^{(i)}, v^{(j)} \rangle \lambda_j$$

$$= \sum_{i=1}^{N_{Tx}} |\langle w', v^{(i)} \rangle|^2 \lambda_i$$

$$= |\langle w', v^{(a)} \rangle|^2 \lambda_a + |\langle w', v^{(b)} \rangle|^2 \lambda_b,$$

which completes the proof.

**APPENDIX B**

**PROOF OF THEOREM 2**

Here we prove the equivalence of the optimal values of two optimization problems $\mathbf{Q}_1$ with and without the condition that $\Delta f_i = 0$. To distinguish, we refer to the two problems as $\mathbf{Q}_{1,FDA}$ and $\mathbf{Q}_1$, respectively. By considering the far-field communication condition $\theta_{LU} = \theta_{ED}$, we have $\Delta D_{LU}^i = \Delta D_{ED}^i$. Therefore, according to (22), we have $H_{LU}^{Res} = H_{ED}^{Res}$. Then, for any variable combination $\{P, P_D, P_A\}$ satisfying all constraints in $\mathbf{Q}_1$, let we derive that $P_{FDA}, P_{D,FDA}$ and $P_{A,FDA}$ also satisfy the constraints in $\mathbf{Q}_{1,FDA}$ as (i) $P_{FDA} = P \leq P_{TX}$; (ii) $\|P_{A,FDA} P_{D,FDA}\|^2 = \|P_A P_D \otimes H_{TV}(t) 1_{N_{RF}} \otimes H_{LU}^{Res} 1_{N_{RF}}\|^2 = 1$, (iii) $P_{A,FDA} = e^{i \phi_{FDA}}$ with $\phi_{pq,FDA} = \phi_{pq} + \Delta f_p \left( t - \frac{\Delta D_p^r}{c} \right)$. Moreover, by substituting (24) into (11a), the maximum secrecy rates satisfies $R_{s,FDA} = R_s$. Thus, we discover a one-on-one mapping between the design variables for $\mathbf{Q}_1$ and $\mathbf{Q}_{1,FDA}$.

Next, we prove the optimal secrecy rate of the two optimization problems are equal, i.e., $R_{s,FDA}^{opt} = R_s^{opt}$. First, we denote the optimal analog and digital beamformer without FDA as $\{P^{opt}, P_A^{opt}, P_D^{opt}\}$, and the corresponding secrecy rate as $R_s^{opt}$. By applying (24), We can induce a solution of variables for $\mathbf{Q}_{1,FDA}$ as $\{\tilde{P}_{FDA}, \tilde{P}_A, \tilde{P}_D\}$, and the corresponding secrecy rate as $\tilde{R}_{s,FDA}$. If there exists another solution exceeding $\tilde{R}_{s,FDA}$, we can take the inversion of the relationship (24) to find a corresponding solution having a secrecy rate exceeding $R_{s,FDA}^{opt}$, which leads to a contradiction. Thus, $\tilde{R}_{s,FDA}$ is the optimal solution to $\mathbf{Q}_{1,FDA}$, and $R_{s,FDA}^{opt} = \tilde{R}_{s,FDA} = R_s^{opt}$, which completes the proof.
REFERENCES

[1] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, “Toward 6G networks: Use cases and technologies,” IEEE Communications Mag., vol. 58, no. 3, pp. 55–61, 2020.

[2] T. S. Rappaport, Y. Xing, O. Kanhere, S. Ju, A. Madanayake, S. Mandal, A. Alkhateeb, and G. C. Trichopoulos, “Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond,” IEEE Access, vol. 7, pp. 78729–78757, 2019.

[3] I. F. Akyildiz, C. Han, Z. Hu, S. Nie, and J. M. Jornet, “Terahertz band communication: An old problem revisited and research directions for the next decade,” arXiv preprint arXiv:2112.13187, 2021.

[4] I. F. Akyildiz, J. M. Jornet, and C. Han, “Terahertz band: Next frontier for wireless communications,” Phys. Communications, vol. 12, pp. 16 – 32, 2014.

[5] J. Ma, R. Shrestha, J. Adelberg, C.-Y. Yeh, Z. Hossain, E. Knightly, J. M. Jornet, and D. M. Mittleman, “Security and eavesdropping in terahertz wireless links,” Nature, vol. 563, no. 7729, pp. 89–93, 2018.

[6] S. R. Aghdam, A. Nooriaepour, and T. M. Duman, “An overview of physical layer security with finite-alphabet signaling,” IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1829–1850, 2018.

[7] W. Gao, Y. Chen, C. Han, and Z. Chen, “Distance-adaptive absorption peak modulation (DA-APM) for terahertz covert communications,” IEEE Trans. on Wireless Communications, vol. 20, no. 3, pp. 2064–2077, 2020.

[8] W. Gao, C. Han, and Z. Chen, “DNN-powered sic-free receiver artificial noise aided terahertz secure communications with randomly distributed eavesdroppers,” IEEE Trans. on Wireless Communications, vol. 21, no. 1, pp. 563–576, 2022.

[9] V. Petrov, D. Moltchanov, J. M. Jornet, and Y. Koucheryavy, “Exploiting multipath terahertz communications for physical layer security in beyond 5G networks,” in Proc. IEEE INFOCOM, 2019, pp. 865–872.

[10] A. D. Wyner, “The wire-tap channel,” Bell system technical journal, vol. 54, no. 8, pp. 1355–1387, 1975.

[11] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas—part ii: The MIMOME wiretap channel,” IEEE Trans. on Information Theory, vol. 56, no. 11, pp. 5515–5532, 2010.

[12] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, “A survey on multiple-antenna techniques for physical layer security,” IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 1027–1053, 2016.

[13] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, “Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers,” IEEE Trans. on Communications, vol. 63, no. 11, pp. 4347–4362, 2015.

[14] T.-X. Zheng, H.-M. Wang, J. Yuan, Z. Han, and M. H. Lee, “Physical layer security in wireless ad hoc networks under a hybrid full-/half-duplex receiver deployment strategy,” IEEE Trans. on Wireless Communications, vol. 16, no. 6, pp. 3827–3839, 2017.

[15] L. Lv, Z. Ding, Q. Ni, and J. Chen, “Secure MISO-NOMA transmission with artificial noise,” IEEE Trans. on Vehicular Technology, vol. 67, no. 7, pp. 6700–6705, 2018.

[16] B. Ning, Z. Chen, Z. Tian, X. Wang, C. Pan, J. Fang, and S. Li, “Joint power allocation and passive beamforming design for IRS-assisted physical-layer service integration,” IEEE Trans. on Wireless Communications, vol. 20, no. 11, pp. 7286–7301, 2021.

[17] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, “Improving physical layer secrecy using full-duplex jamming receivers,” IEEE Trans. on Signal Processing, vol. 61, no. 20, pp. 4962–4974, 2013.

[18] G. Chen, J. P. Coon, A. Mondal, B. Allen, and J. A. Chambers, “Performance analysis for multithop full-duplex IoT networks subject to poisson distributed interferers,” IEEE Int. of Things Journal, vol. 6, no. 2, pp. 3467–3479, 2018.

[19] S. Yan, X. Zhou, N. Yang, T. D. Abbayapala, and A. L. Swindlehurst, “Secret channel training to enhance physical layer security with a full-duplex receiver,” IEEE Trans. on Inf. Forensics and Security, vol. 13, no. 11, pp. 2788–2800, 2018.
[20] J. Lin, Q. Li, J. Yang, H. Shao, and W.-Q. Wang, “Physical-layer security for proximal legitimate user and eavesdropper: A frequency diverse array beamforming approach,” *IEEE Trans. on Inf. Forensics and Security*, vol. 13, no. 3, pp. 671–684, 2018.

[21] X. Song, W. Rave, N. Babu, S. Majhi, and G. Fettweis, “Two-level spatial multiplexing using hybrid beamforming for millimeter-wave backhaul,” *IEEE Trans. on Wireless Communications*, vol. 17, no. 7, pp. 4830–4844, 2018.

[22] L. Yan, Y. Chen, C. Han, and J. Yuan, “Joint inter-path and intra-path multiplexing for terahertz widely-spaced multi-subarray hybrid beamforming systems,” *IEEE Trans. on Communications*, 2021.

[23] I. Ahmed, H. Khammari, A. Shahid, A. Musa, K. S. Kim, E. De Poorter, and I. Moerman, “A survey on hybrid beamforming techniques in 5G: Architecture and system model perspectives,” *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3060–3097, 2018.

[24] L. Yan, C. Han, and J. Yuan, “A dynamic array-of-subarrays architecture and hybrid precoding algorithms for terahertz wireless communications,” *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 9, pp. 2041–2056, 2020.

[25] C. Han, A. O. Bicen, and I. F. Akyildiz, “Multi-ray channel modeling and wideband characterization for wireless communications in the terahertz band,” *IEEE Trans. on Wireless Communications*, vol. 14, no. 5, pp. 2402–2412, 2015.

[26] B. Peng, K. Guan, A. Kuter, S. Rey, M. Patzold, and T. Kuerner, “Channel modeling and system concepts for future terahertz communications: Getting ready for advances beyond 5G,” *IEEE Vehicular Technology Magazine*, vol. 15, no. 2, pp. 136–143, 2020.

[27] Y. Chen, L. Yan, C. Han, and M. Tao, “Millidegree-level direction-of-arrival estimation and tracking for terahertz ultra-massive MIMO systems,” to appear in *IEEE Trans. on Wireless Communications*, 2022.

[28] Y. Tousi and E. Afshari, “A high-power and scalable 2-D phased array for terahertz CMOS integrated systems,” *IEEE Journal of Solid-State Circuits*, vol. 50, no. 2, pp. 597–609, 2014.

[29] S. Ji, W.-Q. Wang, H. Chen, and S. Zhang, “On physical-layer security of FDA communications over rayleigh fading channels,” *IEEE Trans. on Cognitive Communications and Networking*, vol. 5, no. 3, pp. 476–490, 2019.