Physical Layer Security Through Directional Modulation With Spatio-Temporal Millimeter-Wave Transmitter Arrays

Xuyang Lu, *Member, IEEE*, Suresh Venkatesh, *Senior Member, IEEE*, Bingjun Tang, *Member, IEEE*, and Kaushik Sengupta, *Senior Member, IEEE*

***Abstract*— Physical layer security incorporates security features embedded in the communication channels without the need to exchange cryptographic keys. Interest in exploiting such mechanisms has been increasing rapidly for 5G and beyond, due to the low overhead and low-latency properties of such encoding. Although phased arrays, by their nature of the focused beams to users, introduce secrecy, they are still vulnerable to eavesdropping at the sidelobes. In this article, we present a class of spatio-temporal modulated arrays (STMAs) with custom CMOS integrated circuits (ICs) and packaged antennas operating in the 71–76-GHz range that creates secure cones in space by preserving signal fidelity in the intended direction while emulating a time-varying channel outside the secure cone. At unintended directions, the architecture intentionally spectrally aliases signals to create noise-like features and scrambles constellations with a one-to-many mapping (including infinite constellation splitting), making it challenging to invert the mapping by eavesdroppers. Through the architecture, the secure cone can be reconfigured in space on demand and narrowed when we increase the number of elements. We also show how reconfigurable time modulation (such as through frequency chirping) can create a non-repetitive mapping of the constellation to protect against colluding attacks.**

***Index Terms*— 6G, antennas, CMOS, directional modulation, massive multiple-input–multiple-output (MIMO), MIMO, phased array, physical layer security, time-modulated arrays, wireless security, wireless transceivers.**

Manuscript received 6 December 2022; revised 11 August 2023 and 25 March 2024; accepted 27 March 2024. This article was approved by Associate Editor Arun Natarajan. This work was supported in part by the Air Force Office of Scientific Research program, in part by the Army Research Office, in part by the Office of Naval Research, in part by the National Science Foundation, and in part by the Defense Advanced research Program Agency (DARPA). *(Xuyang Lu and Suresh Venkatesh contributed equally to this work.) (Corresponding author: Xuyang Lu.)*

Xuyang Lu was with the Department of Electrical and Computer Engineering, Princeton University, Princeton, NJ 08540 USA. He is now with the University of Michigan–Shanghai Jiao Tong University Joint Institute, the State Key Laboratory of Radio Frequency Heterogeneous Integration, and the Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: Xuyang.Lu@sjtu.edu.cn).

Suresh Venkatesh is with the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27695 USA.

Bingjun Tang was with the Department of Electrical and Computer Engineering, Princeton University, Princeton, NJ 08540 USA. He is now with the Department of Electrical Engineering, Xi'an Jiaotong University, Xi'an, Shaanxi 710049, China.

Kaushik Sengupta is with the Department of Electrical and Computer Engineering, Princeton University, Princeton, NJ 08540 USA.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JSSC.2024.3384373.

Digital Object Identifier 10.1109/JSSC.2024.3384373

I. Introduction

THE ramp-up of high-bandwidth (BW) 5G devices drives the need for a higher channel capacity and introduces a higher demand for enhanced security [1], [2], [3], [4], [5], [6], [7], [8], [9]. Any broadcasting that relies on time or frequency multiplexing can be potentially compromised by active and passive attacks, including masquerade attacks, denial-of-service attacks, and simply eavesdroppers monitoring the entire channel. To address the security issue, popular security features implemented in higher layers of an open-system-interconnection (OSI) model may not be sufficient since protections implemented in the higher layers do not protect the lower layers in a network. For power-limited 5G networks, complex encryption processing on low-power devices can be challenging. In high-speed networks, on the other hand, encryption usually comes at the cost of latency. Therefore, there has been increasing interest in physical layer security that utilizes the physical properties of the channel to impart secrecy [1]. Such effects can come through the time-varying nature or randomness inherent in the channel itself, including fading, multipath, and diversity (with multiantenna systems). Hybrid approaches that use an optimal combination of encryption and physical layer security can emerge as potential solutions to address stringent security, data rates, and latency requirements for 5G and beyond [10], [11], [12].

The security of phased arrays can be quantified by Wyner's wiretap model that expresses secrecy capacity through the difference in the SNR between the target and the eavesdroppers [13]

$$\text{Secrecy} = \log_2\left(1+\frac{P_{\text{target}}}{N_{\text{target}}}\right) - \log_2\left(1+\frac{P_{\text{eve}}}{N_{\text{eve}}}\right) \quad (1)$$

where P_{target} (P_{eve}) and N_{target} (N_{eve}) represent the signal power and the noise power in the targeted direction and the eavesdropper, respectively. As shown in Fig. 1(a), an eavesdropper sitting on a sidelobe will receive exactly the same spectrum and constellation (albeit with low SNR) and therefore might be able to fully decode the transmitted signal or at least extract compromising information (statistics) of the link with a sufficiently sensitive receiver. Recent work has shown this vulnerability with smart passive eavesdroppers in high-frequency directional links [7].

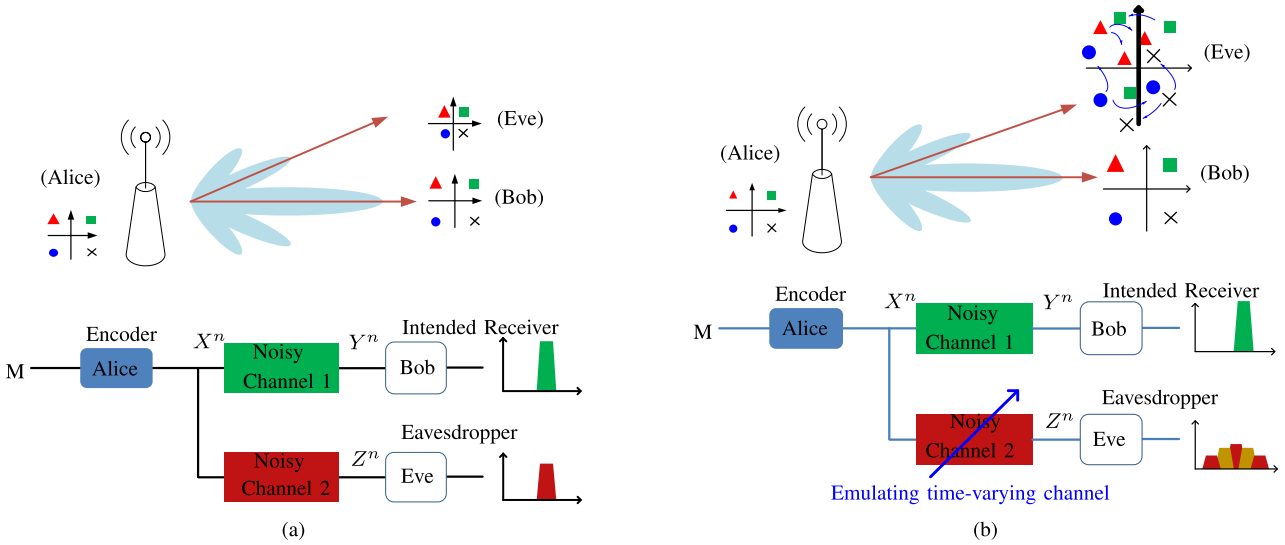


Fig. 1. Concept of physical layer security with STMAs compared to phased arrays. (a) Phase arrays incorporate security through directionality and SNR reduction at the eavesdropper—preservation of spectrum and constellation at all spatial angles makes it vulnerable to eavesdropping. (b) STMA, by the nature of the operation, creates a secure cone for Bob, by preserving the signal at Bob, and by emulating a time-varying channel to Eve enforcing spectrum aliasing, one-to-many constellation splitting, and loss of information.

Directional modulation, on the other hand, intentionally distorts the constellation in unintended directions to incorporate security into the links [14]. As illustrated in Fig. 1(b), in a directional modulation scheme, a spatially dependent signal is transmitted, where the eavesdropper ("Eve") located outside the intended direction receives a signal that is not correlated with the signal received by the targeted receiver ("Bob"). This can be implemented by switching parasitic elements [14], through proper phase encoding at RF frequencies [15] or in the digital domain [16], with antenna arrays that vary in time [17], [18], and with antenna subset selections [19]. However, distortion of the constellation itself does not constitute security since the eavesdropper can revert to techniques that invert the mapping. In [20], the quasi-optical combination of I and Q signals naturally distorts the constellation in off-axis directions, but this one-to-one (bijective) mapping makes it vulnerable to eavesdropping using signal processing and/or machine learning-based classification techniques. Multiple colluding eavesdroppers outside the security cone can also break directional modulation by learning the channel, and exploiting the correlation in space [21].

In this article, we present a spatio-temporal modulated array (STMA) across 71–76 GHz that demonstrates physically secure directional links by preserving the signal fidelity at the intended direction in a secure cone, and emulates a time-varying channel outside the cone. It, thereby, enforces loss of information through spectral aliasing, scrambling of the constellation, and one-to-many mapping (including infinite constellation splitting). Through subsymbol modulation at the millimeter-wave (mmWave) power amplifiers (PAs), we demonstrate non-repetitive time-varying mapping of the constellation at unintended directions, and "noise-like" spreading of the spectrum outside the secure cone. Through such programmable time modulation, one can allow dynamic reconfiguration of constellation scrambling and spectrum shaping, making the inversion of the channel exceedingly challenging. With custom silicon integrated circuits (ICs) and packaged antennas, we showed that the secure cone can be narrowed with a larger number of elements. The proposed method is compatible with large-scale multiple-input–multiple-output (MIMO) architectures, allowing incorporation of the architecture into 5G systems and beyond, operating under low-latency requirements and energy constraints.

This article is organized as follows. Section II presents the operating principle of STMAs, their incorporation of security features, their dependence on time modulation, and the tradeoff space. Section III presents the architecture and constituent circuits. Measurement results are presented in Section IV followed by conclusions.

II. Spatio-Temporal Modulated Arrays

In STMAs, time is incorporated as an additional degree of freedom by including a time-varying term to a phased array representation [22]. Such arrays can not only allow physical layer security into the channels but also allow ultralow sidelobe level [23], harmonic beamforming [24], direction finding [25], and adaptive beamforming applications [26].

A. Symbol-to-Antenna Mapping: Conceptual Operation of the Array for Physical Layer Security

The operating principle of an STMA to incorporate security is illustrated in Fig. 2. Consider a sequence of symbols, denoted as $S = (S_1, S_2, \ldots, S_N)$, which are modulated at the carrier frequency f_0. This signal needs to be transmitted to Bob, who is the target receiver.

Without losing generalization, consider the case where "Bob" is located on the broadside where the phase settings of the array elements are identical ($\Delta\theta_1 = \Delta\theta_2 = \cdots = \Delta\theta_N = 0$). Unlike a phased array, where the entire sequence of the symbols is sent to all the array elements, in STMA, we map symbols uniquely to antennas.

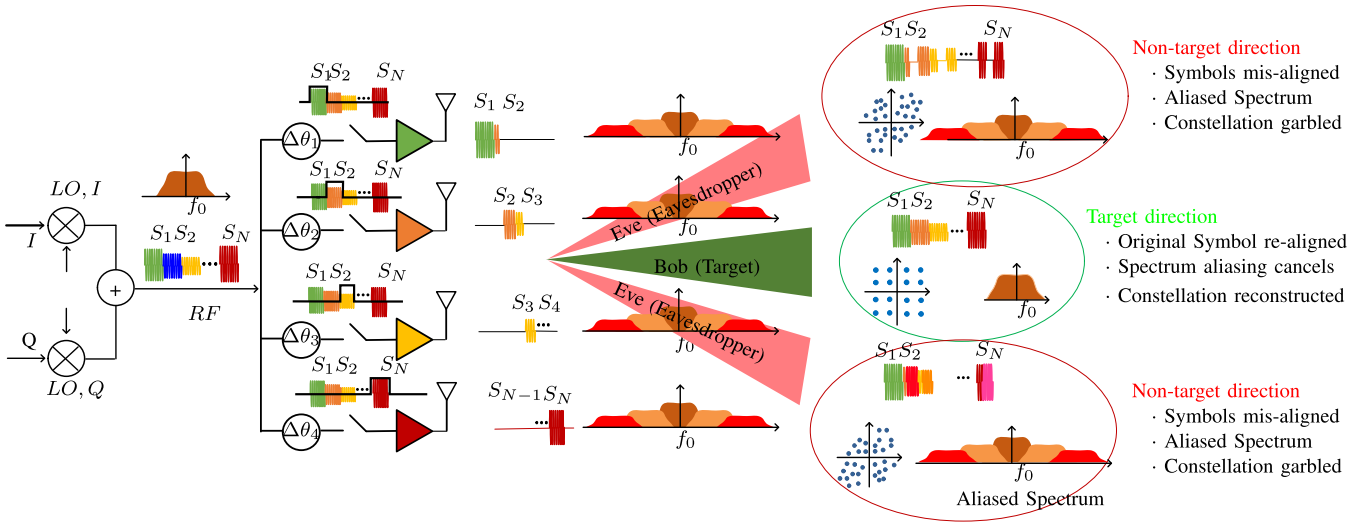


Fig. 2. Principle of operation of the STMAs. Each transmit path is modulated at a frequency f_{mod} < BW through a symbol-to-antenna mapping, potentially at even subsymbol level. Only at the intended direction do the spectral-aliased signals align perfectly in time, recreating the original waveform and canceling the spectrum aliasing through spatial filtering. Outside the secure cone, the signal remains spectrally aliased with loss of information.

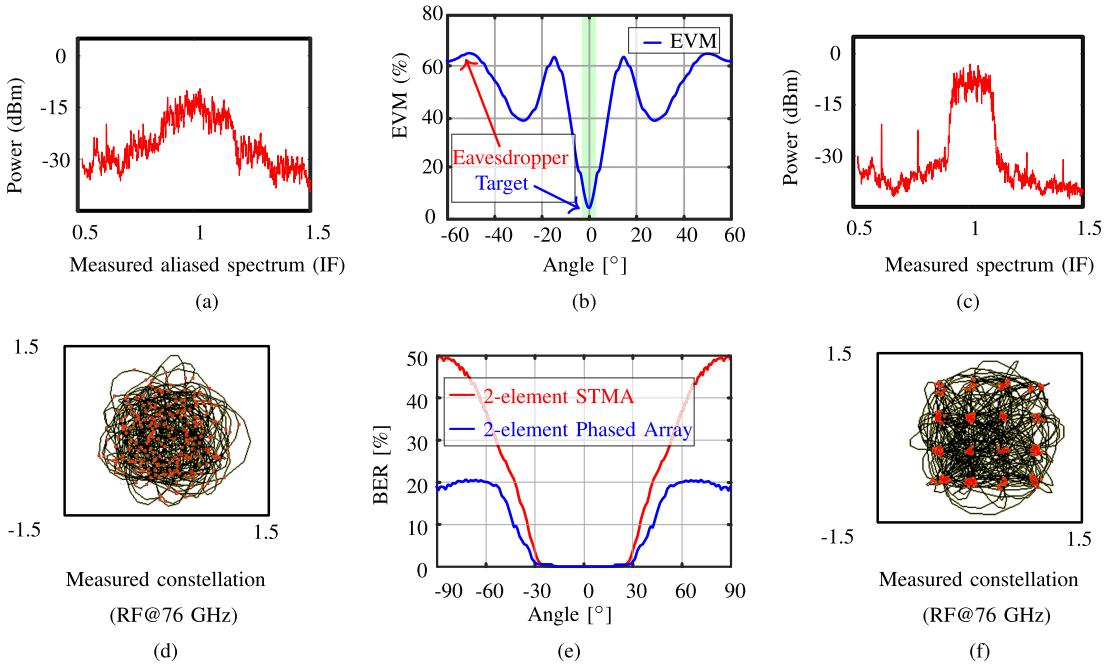


Fig. 3. Characterization of the security features in STMA. (a) and (c) Measured spectrum (eavesdropper's spectrum and target spectrum, respectively). (b) and (e) Simulated EVM and BER of a two-element STMA and comparison with a two-element phased array showing the narrowing of the security cone outside which EVM and BER remain high. (d) and (f) Measured constellations in the 71–76-GHz array at the desired receiver and the eavesdropper, which demonstrates the constellation scrambling and intentional spectral aliasing.

In the example illustrated in Fig. 2, we chop symbols (at the subsymbol level) and direct the modulated chains to multiple antennas. Since each antenna transmits only a fraction of the symbol train, the modulation frequency needs to be low enough to create strong spectrum aliasing at each element.

As the spectrally aliased waveforms quasi-optically combine in space, only at the intended direction (here at broadside), the symbols align up perfectly, reconstructing the original symbol train. Spectrum aliasing, through the spatial filter of combining, cancels in the intended direction. At angles away from "Bob" (the potential location of the eavesdroppers), the symbols arrive with different delays, allowing symbol superposition, retaining the spectrum aliasing, and resulting in strong constellation scrambling that cannot be inverted with equalization.

The nature of the security cone created with such spatiotemporal arrays is distinct from phased arrays. A comparison is shown in the simulated results in Fig. 3 that shows the error vector magnitude (EVM) and the bit error rate (BER) against spatial angle for a two-element STMA and phased array. As can be seen, the time-modulated operation creates a narrower secure cone with high EVM and high BER. Fig. 3 also shows the measured spectrum and constellation at the broadside (intended direction) and at 45° (eavesdropper) for

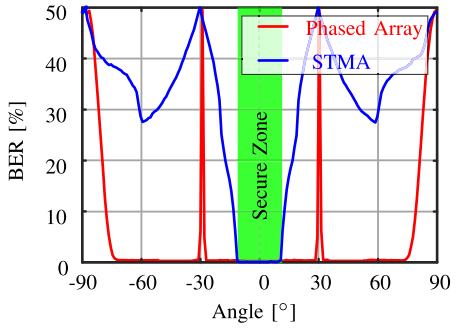


Fig. 4. Simulated security cone comparison between a four-element phased array and an STMA. The figure shows high BER outside the secure cone in the latter.

the two-element chip presented in this work at 76 GHz with a 16-QAM modulation. As can be seen, while the spectrum and the constellation are well preserved in the intended direction, it is heavily aliased, and the constellation is scrambled in the direction outside the secure cone. The effect is more clear in Fig. 4 that shows the comparison between a four-element phased array and an STMA with a broadside SNR of 33 dB. As can be seen, the BER can be constantly low across most spatial angles, including sidelobes for a phased array (except nulls). However, in a time-modulated operation (with the same SNR at the broadside), the BER is significantly increased outside the secure cone.

It is clear that the nature of the security features enabled through spectrum aliasing and constellation scrambling depends on how the symbols are mapped to antennas, via the time modulation technique. Here, we present an intuitive approach to understand constellation splitting, and techniques to optimize complexity of such scrambling outside the secure cone.

B. Spectral Domain Analysis

Before we embark on the time-domain analysis, it is helpful to analyze the nature of spectrum aliasing through a frequency-domain perspective. As shown in Figs. 2 and 5, by mapping the symbol to the antenna, each RF signal in the time domain is multiplied by a time modulation signal. Although in this example, the time modulation signal is periodic in nature, it does not necessarily have to be that way. When modulated with such a periodic waveform (with frequency f_{mod}), the resulting output spectrum consists of copies of the modulated RF signal at frequencies $f_0 \pm mf_{\text{mod}}$, where $m \in I$ is the harmonic number, as shown in Fig. 5. As can be seen, the necessary condition to enforce spectrum aliasing is $f_{\text{mod}} \leq$ BW, where BW is the bandwidth of the modulated signal. Higher speed modulation will not cause spectral aliasing and, therefore, will not incorporate any security features.

It can be noted that such time modulation creates beamforming at the intermodulation frequencies, where each frequency points to a different direction in space. The resultant signal in any direction (such as at the eavesdropper) is a superposition of all these harmonic components. The time-domain pattern at far-field angle θ and at time t of an N-element STMA can be expressed as

$$E(\theta, t) = e^{j2\pi f_0 t} \sum_{n=1}^{N} e^{ja_n} e^{j(n-1)kd\sin\theta} I_n(t) \tag{2}$$

where k is the wavenumber, d is the element spacing, $I_n(t)$ represents a modulation waveform of the nth element, and α_n represents the additional phase shift for the nth element.

Considering a periodic time modulation (though it does not necessarily need to be so), from (2), the mth harmonic of the intermodulation product $(f_0 + mf_{\text{mod}})$ can be expressed as:

$$E_m(\theta) = \sum_{n=1}^{N} e^{j(n-1)kd\sin\theta} \cdot \frac{1}{T_{0,\text{mod}}} \int_0^{T_{0,\text{mod}}} \left[I_n(t) e^{-j2\pi m f_{\text{mod}} t}\right] dt \tag{3}$$

where $T_{0,\text{mod}} = 1/f_{\text{mod}}$ is the time period of the modulation signal ($T_{0,\text{mod}} = 2T_{\text{mod}}$ in Fig. 5). Each intermodulation component generates a radiation pattern pointing in a different direction. As an example, for a sequentially switched array, the element switching function $I_n(t)$ is a periodic function with a time period ($T_{0,\text{mod}}$) and can be expressed as

$$I_n(t) = \begin{cases} 1, & (n-1)T_{\text{mod}} + t_{\text{ON}} + kT_{0,\text{mod}} \leq t < \\ & (n-1)T_{\text{mod}} + t_{\text{OFF}} + kT_{0,\text{mod}}, \ k \in I \\ 0, & \text{others} \end{cases} \tag{4}$$

where t_{ON} and t_{OFF} represent the timing alignment of the time modulation with the RF signal element and its duty cycle where $t_{\text{OFF}} - t_{\text{ON}} = T_{\text{mod}}$ (Fig. 5). For the example illustrated in Fig. 6, $t_{\text{ON}} = 0$, and $t_{\text{OFF}} = T_{\text{mod}} = T_{0,\text{mod}}/2$.

The Fourier component of the mth harmonic of the modulation waveform at the nth element can be expressed as

$$s_m = \frac{\sin\{\pi m(\tau_{\text{OFF}} - \tau_{\text{ON}})\}}{\pi m} e^{-j\pi m(\tau_{\text{OFF}} + \tau_{\text{ON}} + 2(n-1)T_{\text{mod}})} \tag{5}$$

where $\tau_{\text{OFF}} = (t_{\text{OFF}}/T_{0,\text{mod}})$ and $\tau_{\text{ON}} = (t_{\text{ON}}/T_{0,\text{mod}})$.

The excess phase difference between the elements is captured in the term $e^{-j\pi m(\tau_{\text{OFF}} + \tau_{\text{ON}} + 2(n-1)T_{\text{mod}})}$, which depends on the harmonic number. This dependency suggests that each intermodulation product $(f_0 \pm mf_{\text{mod}})$ has a different main beam direction. The direction can be captured by

$$\theta_m = \arcsin\left(\frac{2m}{N}\right). \tag{6}$$

The harmonic pattern for a sequentially switched four-element array is shown in Fig. 5(b). The fundamental frequency points at the broadside (intended direction), where the time-domain signals transmitted by each transmitter (Tx) stitch seamlessly to reconstruct the original time-domain signal. Therefore, we observe the null of the other harmonics at 0°. At angles other than broadside, we see the intermodulation products, where the different harmonic components pointing in different directions satisfying (6) all superimpose on each other. Fig. 5(c) shows the simulated spectrum at the broadside and 50° with a sequentially switched spatio-temporal four element with a carrier frequency of 10 GHz, a symbol rate of 1 Gsym/s, and a modulation frequency of 1/4 GHz. The effect of strong spectrum aliasing can be seen in 50°.

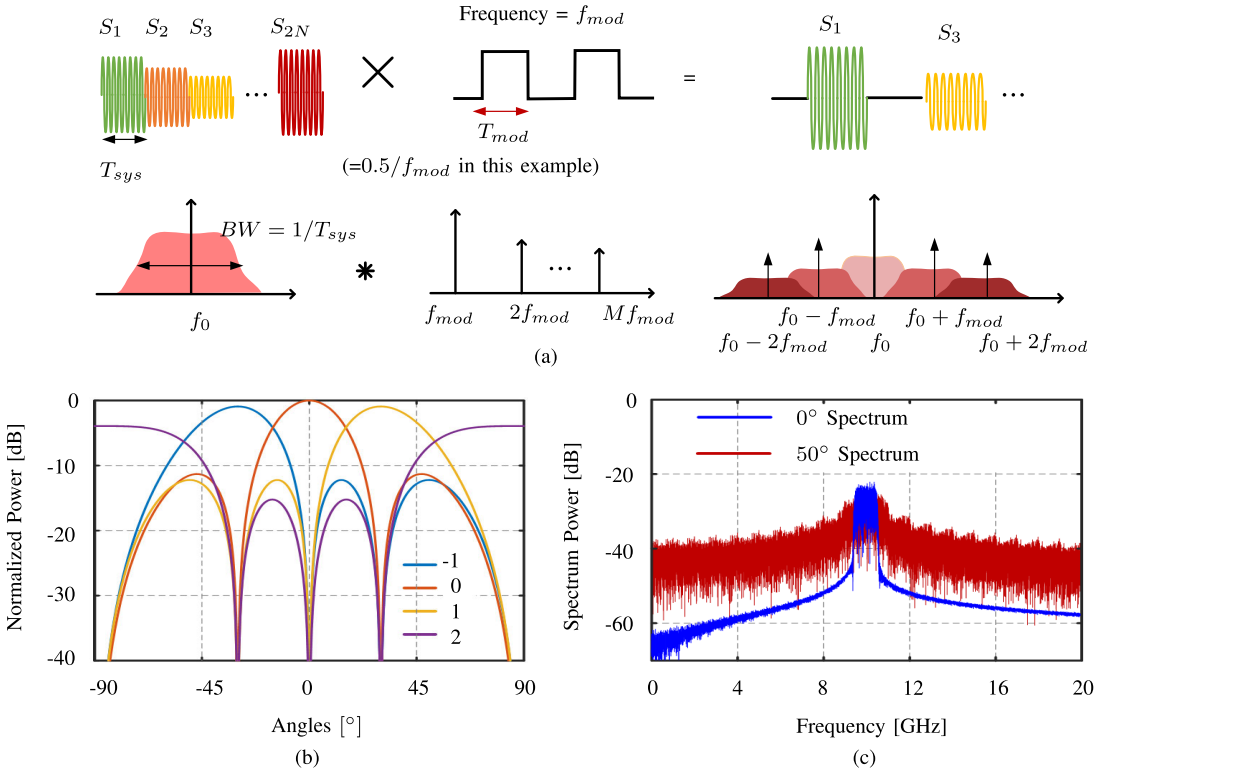


Fig. 5. Spectral aliasing in STMA. (a) Spectral aliasing with time modulation at frequencies $f_{\text{mod}} < \text{BW}$. (b) Simulated radiation patterns of the intermodulation products in STMA. A similar result can be found in [18]. (c) Simulated spectrum preservation and intentional spectral aliasing in a four-element STMA (0° versus 50°).

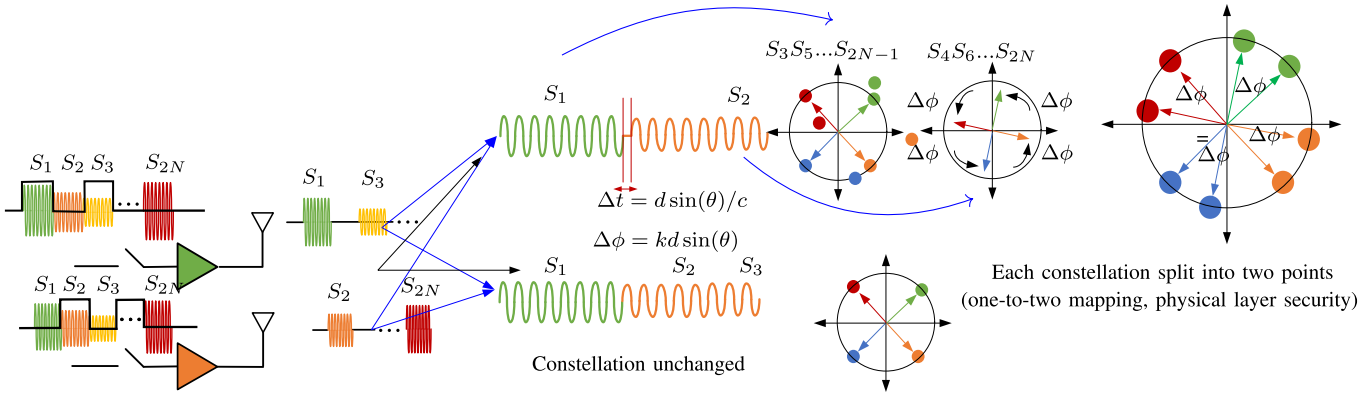


Fig. 6. Constellation splitting outside the secure cone observed in the case of synchronous time modulation for a two-element STMA.

C. Directional Constellation Splitting Analysis and Its Effect on BER

To understand how a constellation splits in off-axis directions, we can resort to the time-domain representation of the simple case of a two-element array illustrated in Fig. 6. Here, the modulation frequency $f_{\text{mod}} = 0.5$ BW, where each alternate symbol is assigned to the two antennas, that is, the odd and even symbols are transmitted to the two antennas. To focus on constellation splitting, we assume instantaneous switching and do not consider here switching imperfections such as amplitude depth control and transients. We will discuss later the effect of finite amplitude control on the nature of constellation garbling in unintended directions. As can be seen, $T_{\text{mod}} = T_{\text{sys}}$, where T_{sys} is the symbol period. In a direction θ away from the intended direction, the even symbol train reaches after a time delay corresponding to a phase change of $\Delta\Phi = kd\sin(\theta)$, where k is the wavenumber and d is the antenna separation. As shown in Fig. 6, this results in the even symbol leading to a constellation that rotates by $\Delta\Phi = kd\sin(\theta)$, whereas the odd symbols stay as they are. The resultant is a superposition of the two constellations that leads to each point splitting into two. Of course, at the angle $-\theta$, the constellation rotates by $-\Delta\Phi$. It can be seen that, in this example, the modulation waveform is synchronized with the RF signal.

This example helps to illustrate the case where the time modulation is a rational fraction of the BW. In this specific example, entire symbols are assigned to one of the antennas.

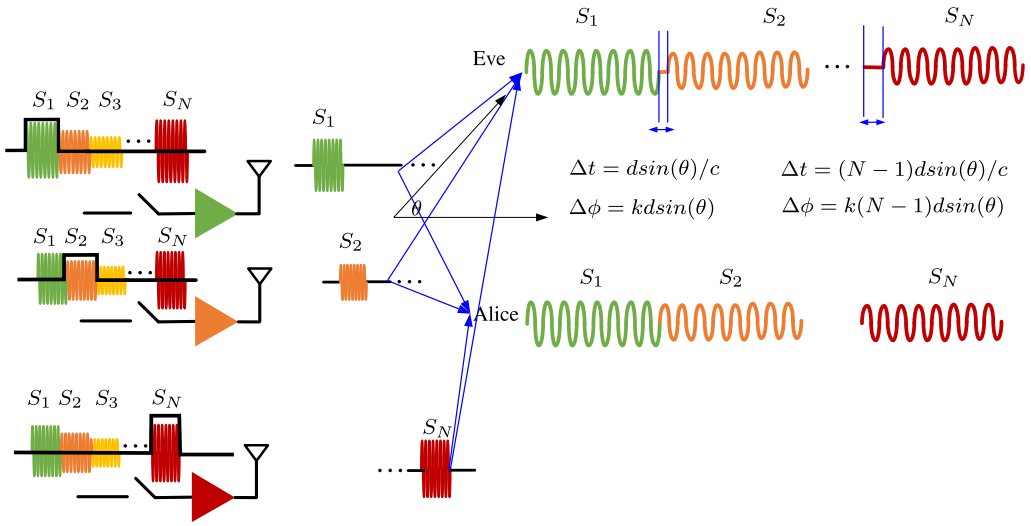


Fig. 7. Spectral splitting in an N-element array with synchronous modulation for which we analyze the delays and accumulated phase shifts that cause constellation splitting.

Taking this further, it is helpful to consider the more complex cases, where the time modulation periodicity may be an irrational fraction of the BW and the periodicity itself might be time-varying. Such time-variant symbol-to-antenna mapping leads to much more complex constellation splitting, approaching infinite one-to-many mapping, making eavesdropper attacks even more challenging. In the generalized case, the signal received by Eve located at a far-field angle θ_{eve}, due to an N-element linear STMA array, is given by

$$s_{\text{Eve}}(t,\theta_{\text{Eve}}) = \sum_{n=1}^{N} \Pi_n\left(\frac{t}{T_{\text{mod}}}\right)\cdot A_{i,q}(t) \cdot \exp(-j\left[2\pi f_o t + (n-1)kd(\sin\theta_{\text{Eve}} - \sin\theta_{\text{Bob}})\right] \quad (7)$$

where θ_{Bob} corresponds to the spatial location of the intended receiver ("Bob"), $\Pi_n(t)$ is a periodic modulation function of the nth element, and $A_{i,q}(t) = A_i(t) + jA_q(t)$ are the in-phase and quadrature-phase components of the modulated ith symbol (e.g., for quadrature phase-shift keying (QPSK) $(A_i, A_q) \in [\pm(1/\sqrt{2})]$).

1) Synchronous Modulation: In this case, we analyze the constellation splitting for simple synchronous switching of an STMA, where the modulation time period T_{mod} and the symbol time period T_{sys} have a rational relationship, i.e., $(T_{\text{sys}}/T_{\text{mod}}) = (p/q)$, where $(p/q) \in I$. For an N-antenna array, if only one antenna is active at any given time, then the modulation frequency is $f_{\text{mod}} = (1/NT_{\text{mod}})$.

The rational relationship implies that if at $t = 0$, the modulation and symbol waveforms align, they align after a finite number (K) of cycles such that KNT_{mod} is a multiple of T_{sys}. In such a situation, the resultant constellation splitting is a superposition of a finite number of rotated constellations, as illustrated in the simplified example in Fig. 6.

For simplicity, let us consider the case represented in Fig. 6, where $(p/q) = 1$, i.e., odd and even symbols are routed to the two antennas. The modulation waveform $\Pi_n(t)$ can be represented as

$$\Pi_n(t) = \begin{cases} 1, & (n+2k-1)T_{\text{mod}} \le t < (n+2k)T_{\text{mod}}, \quad k \in I \\ 0, & \text{others.} \end{cases} \quad (8)$$

The constellation received (C_{Eve}) at a particular elevation angle θ_{Eve} is now a superposition of rotated constellations. Taking into account the unique phase transitions that occur within the K cycles, it can be represented by

$$C_{\text{Eve}}(\theta_{\text{Eve}}) = \sum_{m=1}^{U} \alpha_m C e^{jf_m(\theta_{\text{Eve}}, T_{\text{sys}}, T_{\text{mod}})} \quad (9)$$

where C is the original constellation, U is the unique number of phase transitions that occur before the cycle repeats after K cycles, α_m is the amplitude scaling, and $f_m(\theta_{\text{Eve}}, T_{\text{sys}}, T_{\text{mod}})$ is the phase rotation at θ_{Eve}.

For an N-element array, where the modulation time period $T_{\text{mod}} = T_{\text{sys}}$ and each antenna is active at a given time as shown in Fig. 7, i.e., $f_{\text{mod}} = BW/N$, the constellation is a superposition of N rotations each phase shifted by $kd\sin(\theta_{\text{Eve}})$

$$C_{\text{Eve}}(\theta_{\text{Eve}}) \approx \sum_{m=1}^{N} \alpha_m (\approx 1) C e^{j(m-1)kd\sin(\theta_{\text{Eve}})}. \quad (10)$$

The simulated case for the two- and four-element arrays at different spatial angles is shown in Fig. 8. As can be seen, the constellations split into two and four points. In such cases, the rotation is dependent on the spatial angle of measurement as $kd\sin(\theta_{\text{Eve}})$.

D. Asynchronous Modulation: Infinite Constellation Splitting

The splitting of the constellation outside the secure cone into a finite set depends on the rational relationship between the modulation time period (T_{mod}) and the symbol period (T_{sys}), which results in the repetition of the entire process after a finite number of cycles. When the ratio of the modulation

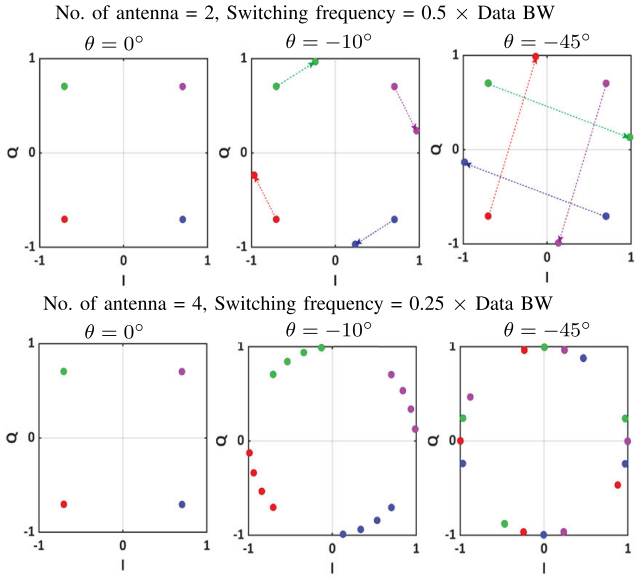


Fig. 8. Simulated constellation splitting for a two-element and a four-element STMA with $T_{\text{mod}} = T_{\text{sys}}$ in both (i.e., each symbol gets mapped to one antenna), and $f_{\text{mod}} = 0.50$ BW and $f_{\text{mod}} = 0.25$ BW.

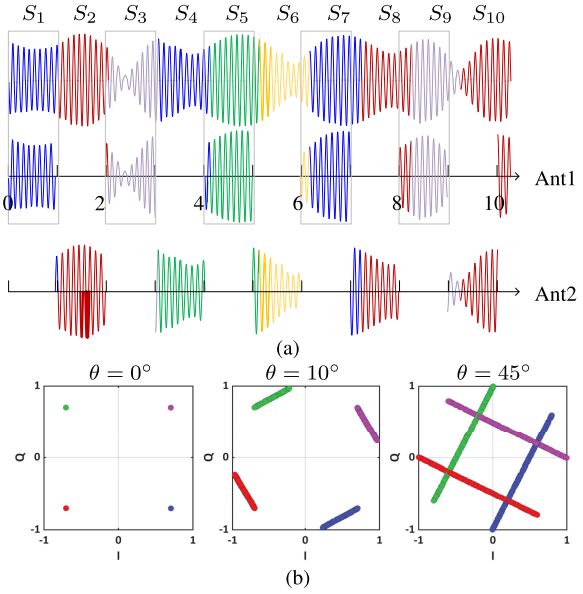


Fig. 9. Asynchronous modulation and infinite constellation splitting where the fraction of symbols that get chopped never repeats. The figure shows the case for a two-element STMA with QPSK modulation where $f_{\text{mod}} = \text{BW}/\pi$, and every constellation point traces a locus of points along a line in the constellation space. (a) Illustration of Switching mode. (b) Effect of constellation splitting at different spatial angles (number of antennas = 4 and switching frequency = $1/\pi$ × data BW).

and symbol period is an irrational number, as illustrated in Fig. 9, the symbols get chopped at irrational fractions, where the process never repeats again. This leads to infinite phase transitions of each point in the constellation leading to a locus of points in the constellation space. These transitions not only lead to multiple constellation points at eavesdropper locations, but also do not necessarily follow the unit amplitude circle for a given constellation point. This is because the periodic modulation waveform $\Pi_n(t)$ creates an intercept leading to split constellation points, where each point forms a locus of points

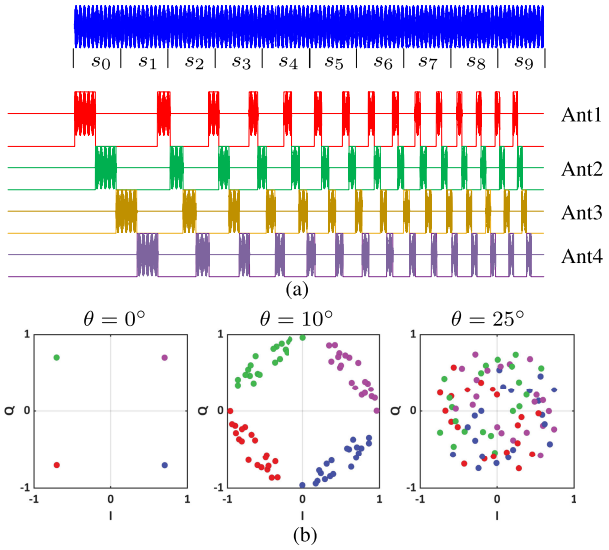


Fig. 10. Simulated case of QPSK modulation for four-element STMA with chirped frequency switching. The switching frequency changes continuously from BW/3 to 2 BW. (a) Number of antennas = 4 and switching frequency = chirped frequency. (b) Resulting constellation.

along a line in a polar plot, having a form $r = \alpha/\cos(\theta - \theta')$, where α is the intercept term arising from the switching wave and $(\theta - \theta') = \beta$ is the angle difference between the intended constellation point and the split constellation point.

As shown in Fig. 9, the constellation splitting effect is illustrated in the simulation for a two-element STMA with QPSK modulation, at different receiver locations for a modulation period of $T_{\text{mod}} = T_{\text{sys}}/\pi$, showing the location of the constellation points into an ideally infinite number of points. In a practical system, where such irrational frequencies are not possible to generate, the splitting will be finite but can be made large with suitable dithering in a phase-locked loop. This can be enabled by frequency chirping, as shown in Fig. 10.

The BER against the number of elements and various modulation schemes is shown in Fig. 11. As can be seen, the secure cone can be made sharper with more elements. Although constellation dynamics change for different types of switching (synchronous or asynchronous) that lead to resilience against distributed and colluding eavesdropper attacks [8], the overall secure cone angle for a single eavesdropper with a classical receiver mostly remains the same for a given SNR and the number of element arrays. All simulations were performed assuming a constant SNR = 10 dB in Alice. For a varying number of space–time modulated antenna elements and modulation types, we also compare the widths of the information cone and the security cone. In this analysis, the information cone is defined as the first null beamwidth (FNBW) of a conventional phased array with a similar number of total elements. The security cones are measured at 5% BER levels. The results of this comparison are highlighted in Fig. 11(c). In the time-modulated architecture, the security cone width is always smaller than the information cone width.

E. Security and Effective Isotropic Radiated Power Tradeoff

In an STMA, since portions of the array elements are turned off at any given instant, the PAs need to be boosted to achieve

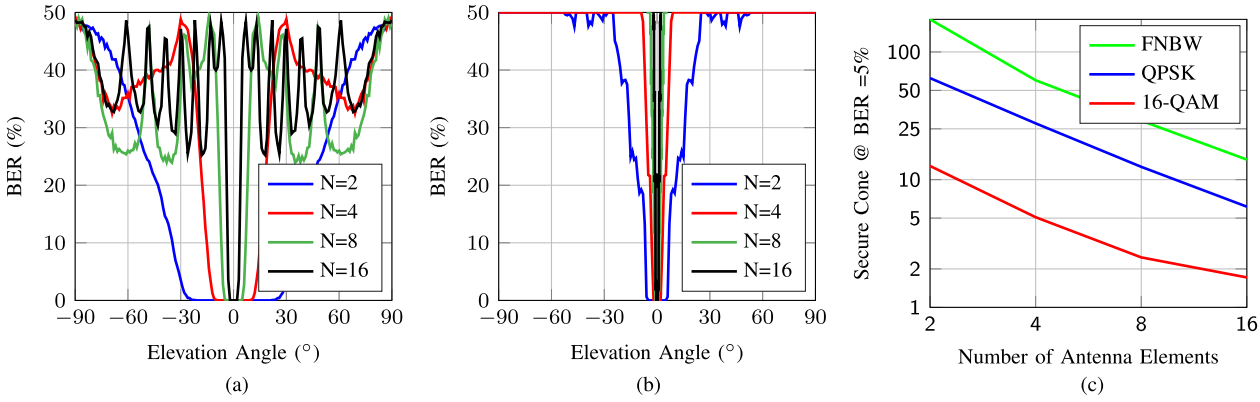


Fig. 11. Secure cones with a varying number of elements and different modulation schemes. (a) BER across spatial angles for a varying number of antenna elements for QPSK modulation. (b) BER across spatial angles for a varying number of antenna elements for 16-QAM. (c) Variation of the secure cone region (corresponding to BER = 5%) for QPSK and 16 QAM modulations and a varying number of antennas. The information cone is also shown, which refers to the FNBW of a conventional phased array.

the same SNR at the intended receiver. In other words, there is a tradeoff between the overall effective isotropic radiated power (EIRP) and the achievable security metric. While prior works have highlighted security metrics for such directional modulation [28], here we focus on the tradeoff between security and EIRP. Unlike the case illustrated in Fig. 9, where at any given instant, only one antenna is active, in a 2-D array, one can time-modulate a random subset (say 75%) of the array elements to be active. In such a case, to achieve the same SNR in Bob's direction, each PA must generate nearly two times more power. To quantify this tradeoff, we can define two parameters, namely, the power enhancement factor (PEF) and the security enhancement factor (SEF) as in [8]

$$\text{PEF} = \frac{P_{\text{out}} \text{ per element in an STMA}}{P_{\text{out}} \text{ per element in a Phased array}}\Bigg|_{\text{EIRP = constant}} \tag{11}$$

$$\text{SEF} = \frac{\text{BER at the same angle for an STMA}}{\text{BER (sidelobe) for a Phased array}}\Bigg|_{\substack{\theta=\text{sidelobe angle} \\ \text{EIRP = constant}}}. \tag{12}$$

In Fig. 12, we show the tradeoff between PEF and SEF as a function of a total number of elements and a number of subset elements turned on in the overall array. The baseline for comparison is the overall N-element phased array (4, 8, and 16 elements in Fig. 12) without any time modulation where PEF = 1 and SEF = 1. As shown in the simulation, even a modest increase in the PEF for an STMA can lead to an enormous decrease in BER (at the eavesdroppers), allowing enhancement of physical layer security.

III. Spatio-Temporal Modulated Transmitter Architecture

The implemented two-element array architecture is shown in Fig. 13(a). With each chip containing two channels, we test with two- and four-element arrays with packaged antennas. Each Tx chain consists of a current-bleeding double-balanced mixer, two differential PA drivers, and a single-ended main PA stage. A single-ended local oscillation (LO) signal is fed into the chip, divided, and subsequently converted into differential mode using an on-chip balun to drive mixers of the two Tx

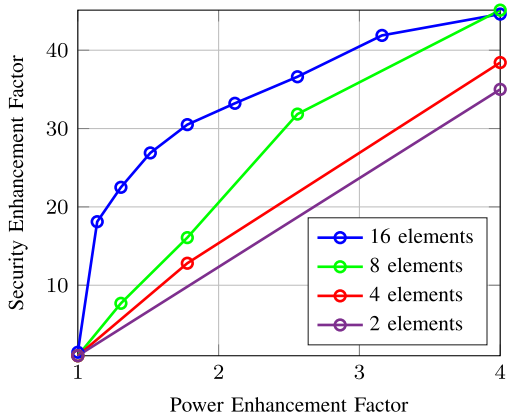


Fig. 12. Simulated tradeoff between PEF and SEF for different subset modulation for different sized arrays.

channels. The intermediate frequency (IF) signals are mixed with the LO signals and then amplified with three stages of PAs. The time-domain modulation can be done at either IF or after upconversion at the RF frequency. Here, we implement the time modulation with high-speed switches at the source of both the driver and the main PA stages.

The LO input matching network, which is based on a transmission line divider and two transformers, is shown in Fig. 13(b). Fig. 14(a) and (b) shows the simulated scattering parameters of the LO input matching network showing an asymmetry in its differential power of less than 0.5 dB and an overall efficiency of >43% over 71–76 GHz.

As shown in Fig. 13(c), a double-balanced current-bleeding mixer [29] is chosen to allow the entire chip to operate with a 1.2-V supply voltage. Fig. 13(d) shows three stages of PAs designed to produce an output saturation power of 9 dBm over 71–76 GHz. The switching is implemented at the source of both the 2nd-stage and the 3rd-stage amplifiers. The first two stages are designed to be differential, and the last stage is single-ended. A differential-to-single-ended conversion is implemented between the 2nd stage and the 3rd stage using a transformer balun.

The time modulation transistors in the 2nd and 3rd stages are approximately 4–5 times larger than the PA to minimize

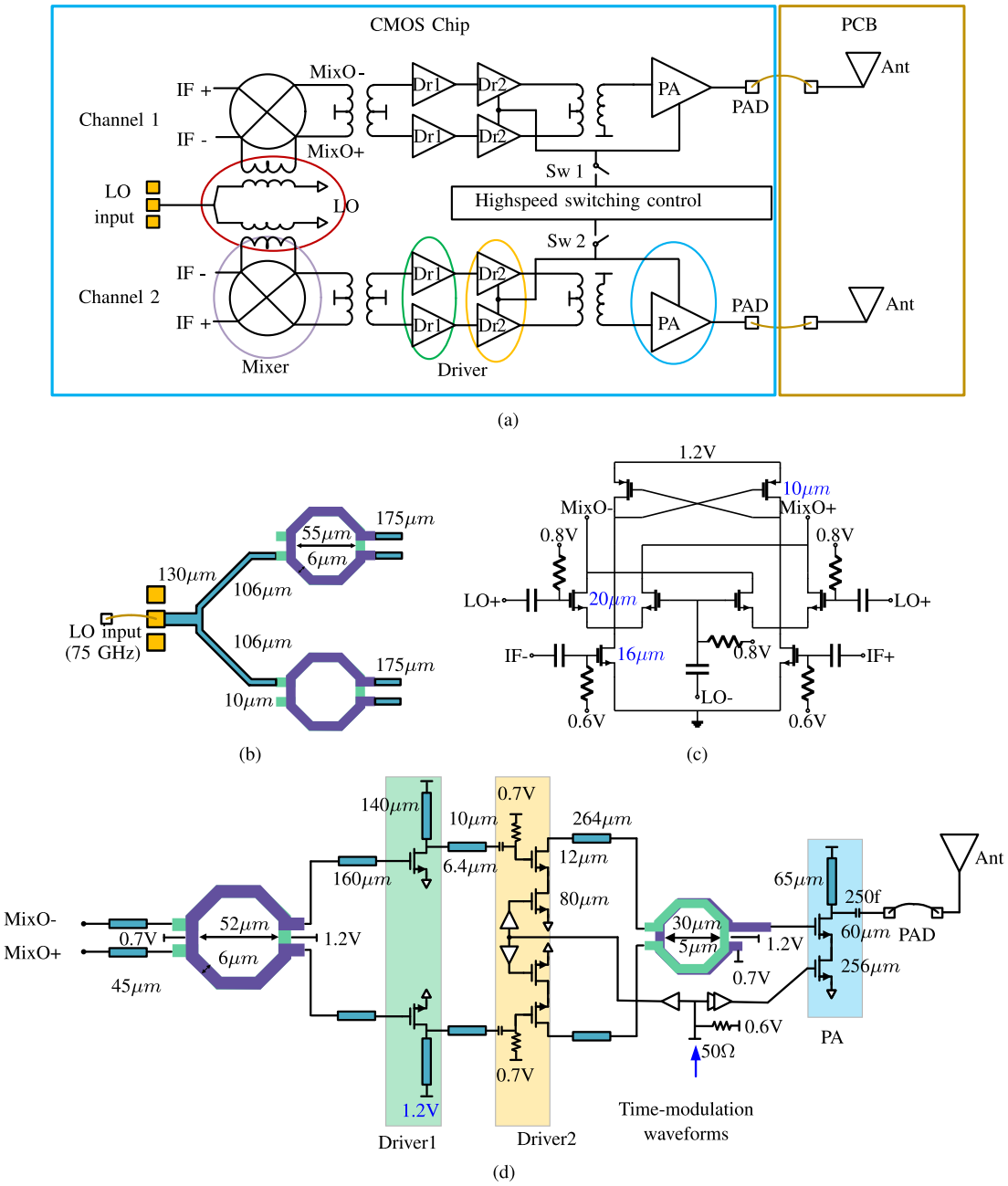


Fig. 13. Architecture of the STMA chip with two-dual-channel Txs and constituent circuits. Time modulation is performed in the RF signal path implemented in the 2nd stage and the 3rd stage of the PAs [27]. (a) Architecture of the STMA chip. Each chip contains two channels. (b) Input LO network. (c) Schematics of the mixer. (d) Schematics of two stages of the driver amplifier and the PA.

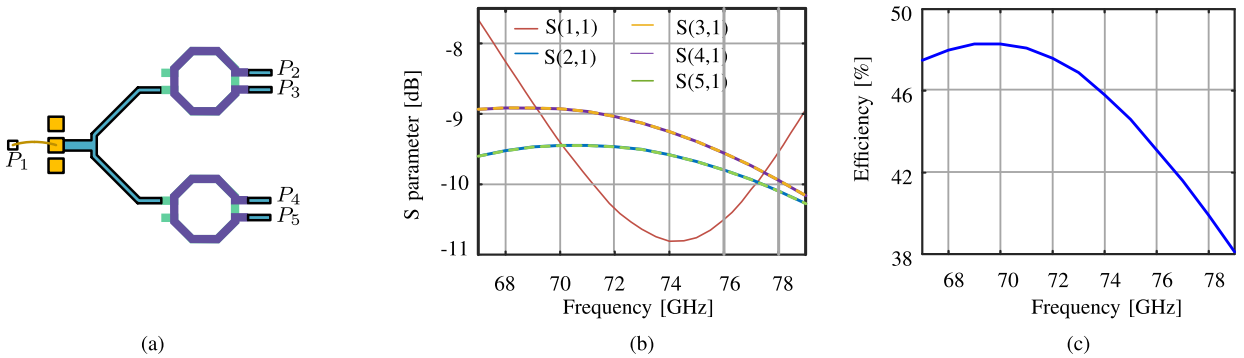


Fig. 14. LO distribution network. (a) Simulated scattering parameters of LO input matching showing asymmetry < 0.5 dB. (b) Efficiency of the LO input network on 71–76 GHz $> 43\%$.

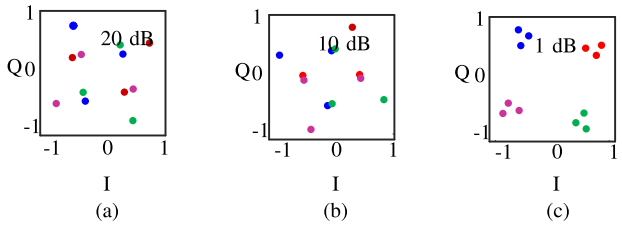


Fig. 15. Impact of effective switching of the PA on constellation splitting outside the security cone. Constellations are simulated at 45° for a 200-MHz signal with 100-MHz modulation with (a) 20-dB ON–OFF ratio, (b) 10-dB ON–OFF ratio, and (c) 1-dB ON–OFF ratio.

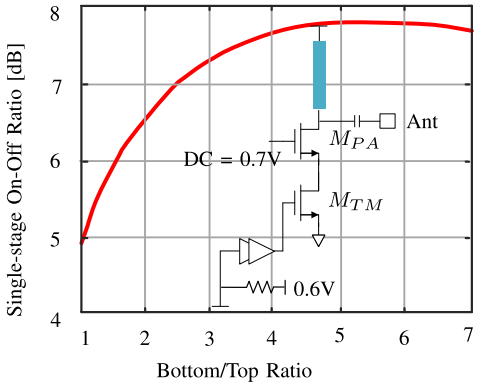


Fig. 16. Variation of the single-stage ON–OFF ratio of a 73-GHz signal with varying size of the switching transistor compared to the PA cell.

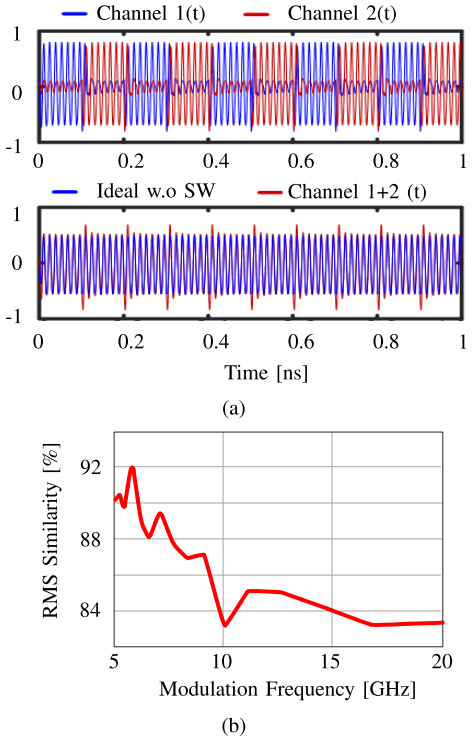


Fig. 17. Impact of transients on modulation BW. (a) Time-domain waveform to illustrate the transient non-idealities due to switching. An ideal waveform has zero amplitude when turned off and an instant transition from on to off. The sum of the time-domain waveforms of channels 1 and 2 should be an ideal waveform with equal amplitude. (b) RMS value of the difference between the original waveform and the reconstructed signal at Bob can be used to measure the impact of the transients of switching. The rms value is a measure of the average amplitude of the difference signal, and it can be used to quantify the amount of distortion caused by the transients. Modulation frequencies lower than 5 GHz introduce less than 10% of rms dissimilarity.

source degeneration and achieve a large ON–OFF ratio. A small ratio will reduce the constellation splitting at the off-angles as expected and ultimately degenerate to a classical phased array operation for very inefficient modulation. A comparison of the constellation splitting to decrease switching efficiency is shown in Fig. 15. The simulation is performed using MATLAB modeling, where the signal's ON and OFF amplitudes are maintained at a specific modulation depth. This suggests that for a TMA application, the switching ratio should be greater than at least ∼10 dB to provide sufficient constellation splitting. In this work, efficient modulation is achieved with a measured 15-dB ON–OFF ratio of the PA at gigahertz speed.

Fig. 16 shows the variation in the switching ratio of a single stage with the size of the bottom transistor. We choose a ratio of 4–5 to allow around 7–8 dB of modulation at each stage, resulting in a total ON–OFF ratio of more than 15 dB across both stages. The transient effects of switching also need to be considered. In Fig. 17(a), a comparison between the modulated mmWave input signal and the re-aligned signal at Bob is shown. In the time modulation technique, the signal is divided into segments and, in an ideal scenario, the signal received in the intended far-field direction is the sum of these segments, reproducing the original signal. However, real-world devices introduce glitches and jitter in the waveform, resulting in changes to the received signal. In this simulation, the goal is to capture these effects by sweeping the modulation frequency. Intuitively, lower frequencies tend to exhibit better switching quality, while higher frequencies may introduce more overshoot and undershoot. The percentage similarity is calculated by comparing the waveform obtained after summation with the original waveform. This comparison is made using the root mean square (rms) difference, expressed as the square root of the summation of the squared differences between the received wave and the original waveform. The impact of high-BW modulation can be seen in Fig. 17(b). As the modulation frequency increases, the received waveform distortion also increases. This requires the co-design of pulse shaping and time modulation together to minimize distortion and spectral outgrowth.

The impact of time-domain jitter can be observed in Fig. 18, where the level of jitter is determined by the standard deviation of the rising and falling edges from their intended positions, normalized by the data rate. To analyze this effect, a 16-QAM sequence consisting of 128 bits is generated. To ensure the visibility of the RF part, a carrier frequency of 5 GHz is chosen for the plot, although this analysis can be applied to carriers of any frequency. The modulation frequency is set at 20 MHz, while the data BW is 100 MHz. Observing Fig. 18(a), it becomes evident that due to timing misalignment, there are instances where the previous antenna has turned off before the next one has turned on, resulting in gaps or vacancies in the received signal. Consequently, the constellation plot in Fig. 18(b) demonstrates distortion, with a selected jitter level (σ) of 0.6% leading to an EVM of 3.52%. When sweeping the jitter level and observing the change in EVM, it becomes clear that an increase in jitter directly corresponds to an increase in EVM. In particular, this phenomenon remains independent

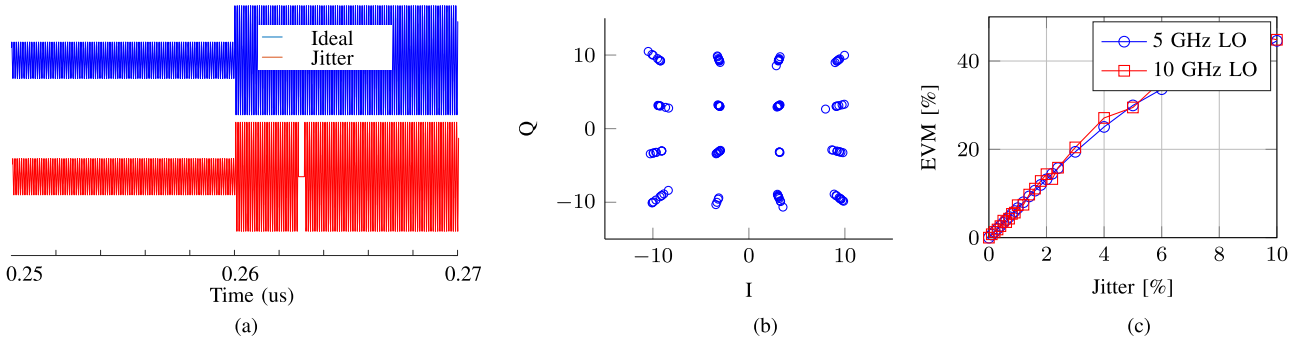


Fig. 18. Illustration of the impact of time-domain jitter on the performance of STMA. A 16-QAM sequence comprising 128 bits is generated with a carrier frequency of 5 GHz for illustrative purposes. The chosen modulation scheme is sequential, activating one of the four array elements alternately at a modulation frequency of 20 MHz while maintaining a data BW of 100 MHz. (a) Impact of time-domain jitter, as the subsequent antenna unit experiences a slight delay in activation. (b) Constellation diagram demonstrates the effect of jitter, with a chosen jitter level (σ) of 0.6%, resulting in an EVM of 3.52%. (c) Variation of the EVM when the jitter levels are varied from 0% to 10%, showing an expected increase in the EVM.

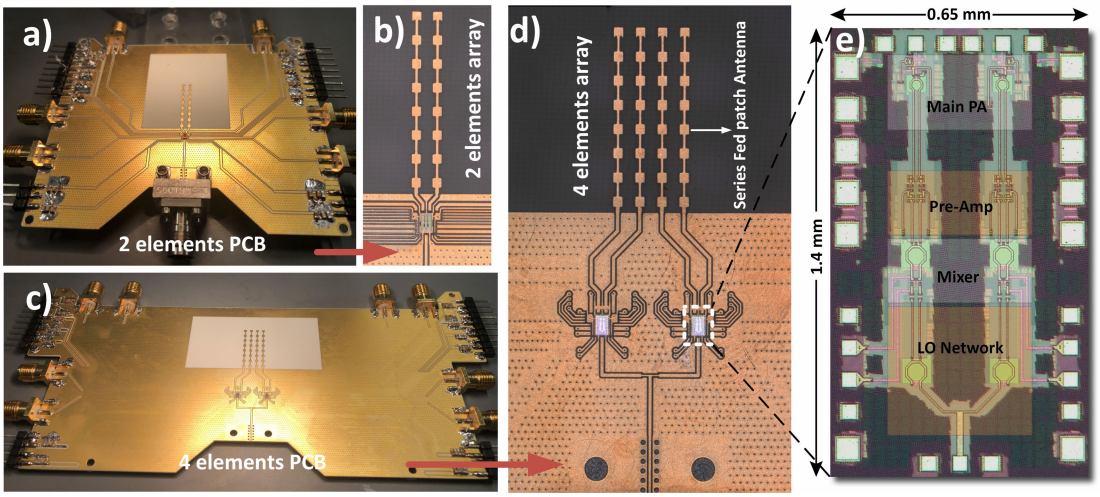


Fig. 19. Custom chip packaging and chip photograph. (a) Two-element STMA PCB. (b) Zoomed portion of the two-element STMA PCB with series-fed patch antennas. (c) Four-element STMA PCB. (d) Four-element STMA with series-fed patch antenna array. (e) Custom TMA chip photograph fabricated using the 65-nm CMOS process.

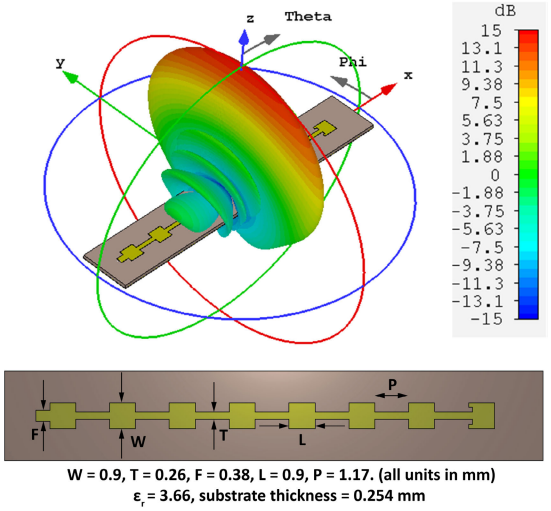


Fig. 20. Simulated series-fed patch antenna radiation pattern at 75 GHz.

of the carrier frequency, as indicated by the two traces that represent different carrier frequencies of 5 and 10 GHz in Fig. 18(c).

IV. Measurement Results

The chip was manufactured in 65-nm bulk CMOS technology and occupies a 1.4 × 0.65 mm area. The micrograph is shown in Fig. 19. The chip is packaged in a two- and four-element array (with two chips) and is co-designed and packaged with series-fed patch antennas [30], [31]. The photographs of the two- and four-channel printed circuit boards (PCBs) are shown in Fig. 19(a)–(d). The antenna has a directivity of ∼16.9 dB with a radiation efficiency of approximately 82%. The radiation pattern of the designed serial-fed patch is shown in Fig. 20.

A. Tx Chain Characterization

The performance of the chip is first characterized by probing. Each Tx chain provides a saturated gain of 20 dB, a power-added efficiency (PAE) of 19%, and P_{sat} of 9 dBm, with a BW of 71–76 GHz. The results of large-signal measurement against simulation for varying IF, RF power, and LO frequency are shown in Fig. 21. The output power for various IF frequencies is shown in Fig. 22(a). The IC can support data rates of up to 7.5 Gb/s with 32 QAM at 76 GHz. Each Tx achieves OIP_3 of 12.6 dBm, as shown in Fig. 22(b).

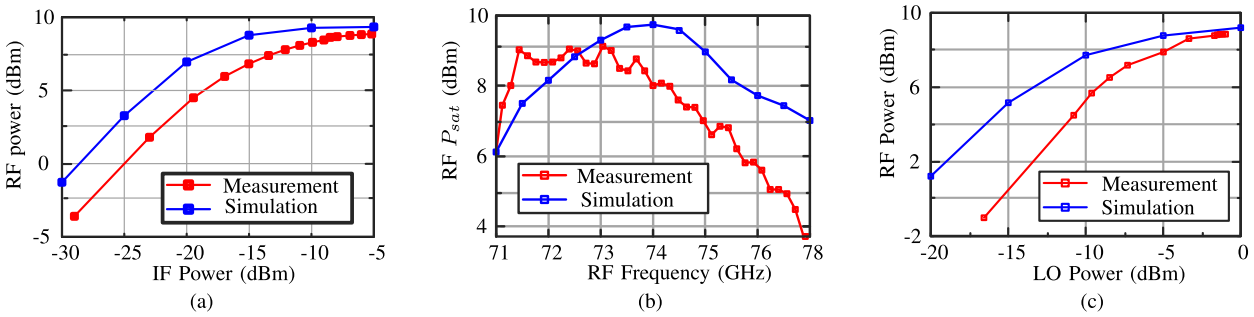


Fig. 21. Measured large-signal characteristics of the Tx chain. (a) RF versus IF power where $f_{RF} = 73$ GHz and $f_{IF} = 100$ MHz. (b) Saturation power against LO frequency. (c) RF power versus LO power where $f_{RF} = 73$ GHz and $f_{IF} = 100$ MHz.

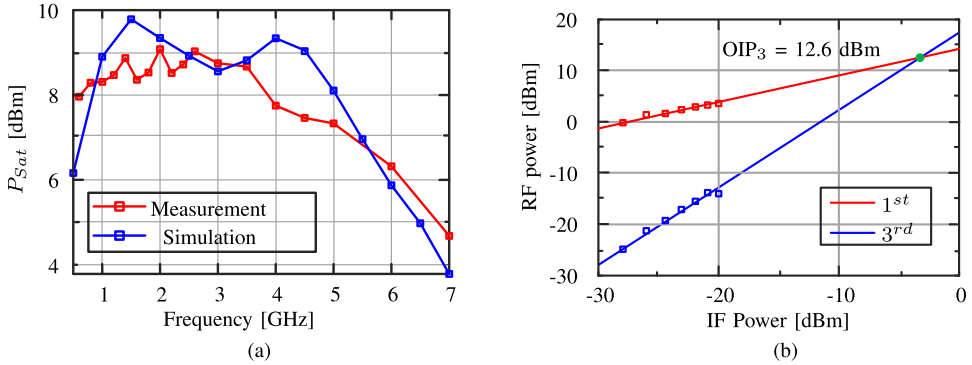


Fig. 22. Measured large-signal characteristics of the Tx chain. (a) Saturation power versus IF frequency. (b) Two-tone measurement shows OIP$_3$ of 12.6 dBm.

To measure the dynamics of time modulation, we capture the time-domain waveform at the output of the PA (of one Tx chain) with an 80-GS/s oscilloscope with a 20-GHz BW. As illustrated in Fig. 23(a), we can observe an ON–OFF ratio of 15 dB. The effect of this switching on a constellation can be observed in Fig. 23(b) for a QPSK modulation. As expected, the output constellation is a superposition of those in the ON–OFF states that result in the four corner bulbs representing the QPSK modulation when the PA is ON and the center bulb representing the OFF state.

B. Spatio-Temporal Modulation Operation for Physical Layer Security

We first measure the chip in a connecterized setup to demonstrate spatial-dependent demodulation in a controlled setting and, then, a wireless setup. The IF signals and switching waveform are generated by two arbitrary waveform generators (AWGs). The single-ended LO signal is generated using mmWave multipliers, amplified, and fed into the chip. The RF outputs are bonded to the transmission line on the PCB and combined, down-converted, and captured in the oscilloscope. In the wireless setup, we capture the radiated signal from the STMAs directly at a 1-m distance by a horn antenna with a gain of 22 dB. Spatial variation of spectrum and constellation to capture the impact of time modulation on security is measured by placing the chip on a rotational stage.

To demonstrate physical layer security, we choose three modulation conditions: 1) no modulation (phased array operation); 2) modulation at 100 MHz ($f_{mod} \approx$ BW/2 to route the even and odd symbols to the two different channels); and 3) modulation at 400 MHz ($f_{mod} \approx 2 \times$ BW).

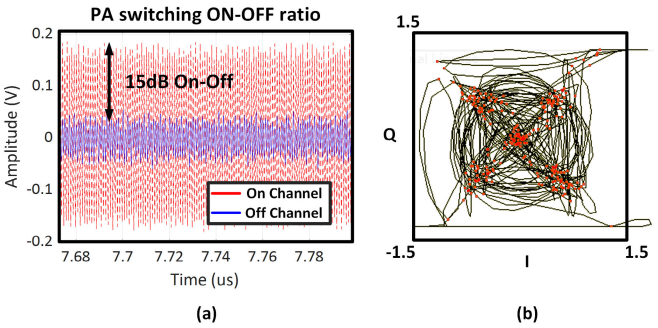


Fig. 23. Dynamics of the modulation at the output of one Tx chain. (a) Measured time-domain signal showing 15-dB ON–OFF ratio. (b) Measured constellation showing the superposition of those in the ON–OFF states that result in the four corner bulbs representing the QPSK modulation when the PA is ON and the center bulb representing the OFF state.

Fig. 24(a) shows the measured constellation across the spatial angles. As expected for the phased array operation, the spectrum and constellation remain unchanged, albeit with varying SNRs. For the two-element STMA, when modulated either at 100 or 400 MHz, the spectrum aliasing cancels off in the broadside direction, stitching up the time-modulated signals from the two channels and reconstructing the original signal and constellation. The notable difference can be seen in the two modulation rates outside the broadside direction. As shown with the 400-MHz modulation (where $f_{mod} \approx$ 2 BW), we see spectral copies at the inter-modulation products at the eavesdroppers, but no spectrum aliasing and consequently no constellation scrambling and security. When modulated at 100 MHz, we see the predicted effect of constellation splitting and spectral aliasing that increases with spatial angle.

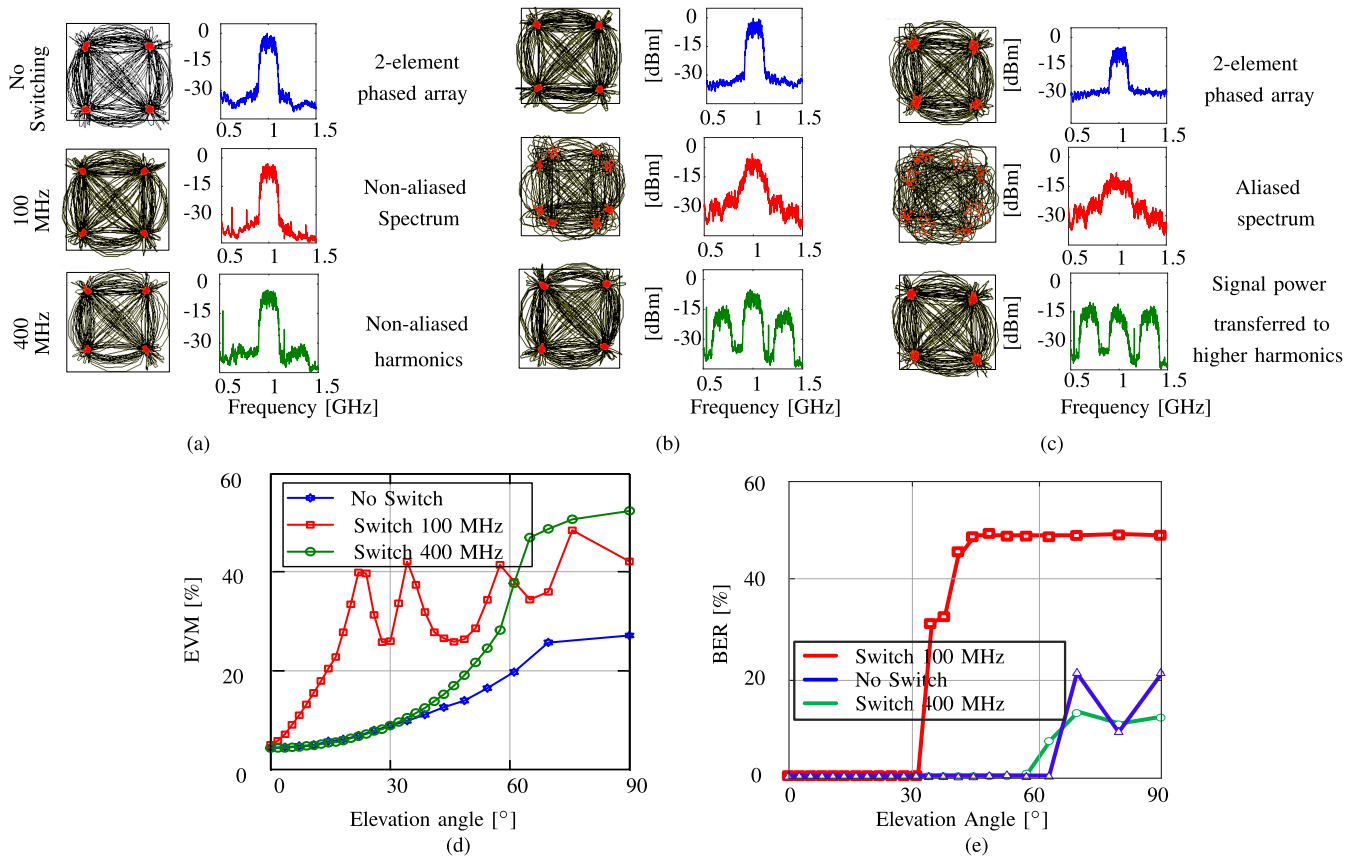


Fig. 24. Measured BER and EVM across spatial angles for the two-element STMA. (a) Constellation measured at $\theta = 0°$ with varying modulation frequencies. The spectrum remains narrowband, while the constellation can be accurately reconstructed regardless of the modulation frequency. (b) Measured constellation at $\theta = 20°$, revealing spectrum aliasing and constellation splitting. At 400-MHz modulation speed, exceeding the data BW, an unaliased spectrum is observed, resulting in the correct constellation. (c) Similar observation at $\theta = 50°$ where the constellation becomes increasingly discernible. (d) Measured EVM and (e) BER analysis conducted for three operating modes across different angles.

The EVM and BER against angle for three operating modes are plotted in Fig. 24(b) and (c). We observe that in the phased array mode (no switching), the EVM increases purely due to the reduction in signal power at higher spatial angles. In these measurements, the SNR at the broadside is kept the same. The EVM for 400-MHz switching increases similar to a phased array mode, with a slightly higher slope due to decreased SNR, since the portion of the radiated power gets distributed across the inter-modulation products. When modulated at the appropriate frequency of 100 MHz, the measured spectrum and constellation at the intended direction ($\theta = 0°$) shows suppression of spectrum aliasing and preservation of constellation for the time-modulated array with an EVM $\approx 4\%$. It can also be seen that each point in the constellation splits into two points at low spatial angles as illustrated before in Fig. 6. The physical layer security is evident in the narrowing of the secure cone with the EVM always above 20% outside a $\sim 15°$ angle. However, even in such cases, if the split constellations are close enough, Eve can remap them back to the same data point. Therefore, we measure the BER across spatial angles and, as can be seen, the BER increases sharply after 30°, with a much narrower security cone compared to a phased array operation.

C. Two- and Four-Element STMA Wireless Measurement

The free-space measurement results for a two-element STMA at 76 GHz when operated in a phased array mode and when appropriately time-modulated (100 MHz for a 200-MS/s baseband) are shown in Fig. 25(a) and (b), where the initial direction of the intended receiver is at broadside. The measured EVM and constellations at $-40°$, 0°, and 40° show that the EVM remains low not only at the broadside but also outside the secure cone. Correct constellations can be demodulated from those regions as well. In comparison, in the TMA operating mode, the EVM stays high outside the secure cone, outside which the constellation remains scrambled. The narrowing of the secure cone with a four-element STMA is shown in Fig. 25(c).

The wireless setup also allows us to toggle the targeted direction elsewhere to deliberately scramble a region in the space where the eavesdroppers can be potentially located. This is done by engineering the relative phase (time delay) of both the IF signal and the switching signal to allow beam formation to occur in the direction of interest. In the example shown in Fig. 26, the secure cone is adjusted between $-30°$ and 30°. We clearly observe the effect in the EVM contour across spatial angles and the selected constellations.

D. Chirped Switching Waveform to Avoid Colluding Eavesdropper Attacks

In the simple periodic modulation case as shown before, where symbols can be mapped to antennas in a pre-defined static fashion that leads to finite constellation splitting, the

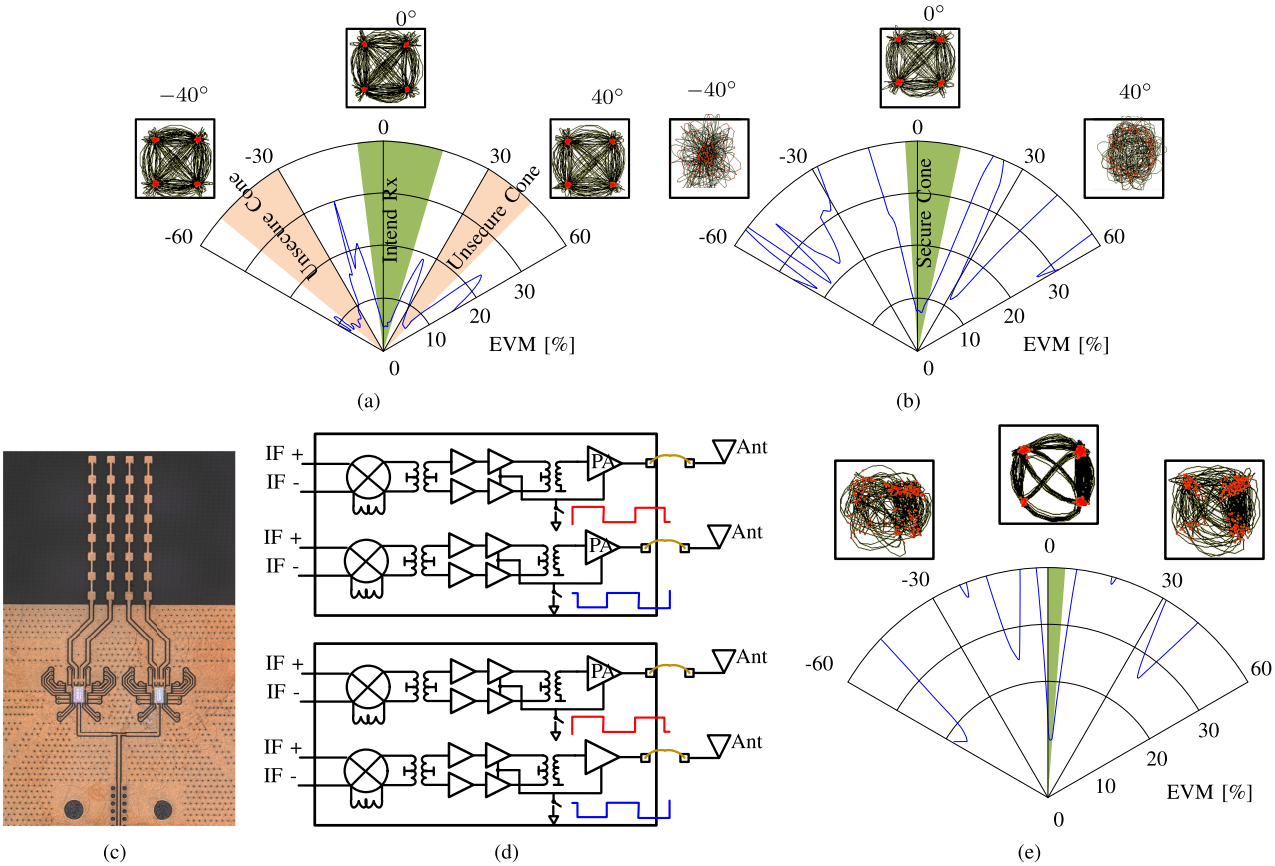


Fig. 25. Radiated wireless measurement results. Constellation measured in space for the two-element array when operated in (a) phased array mode and (b) time modulated at $f_{\text{mod}} = 0.5$ BW. (c) PCB setup of a four-element STMA. (d) Schematic of the four-element STMA setup. The same modulation waveform is sent to antennas 1 and 3, and the complement of it is sent to antennas 2 and 4. (e) Narrowing of the secure cone with a four-element STMA.

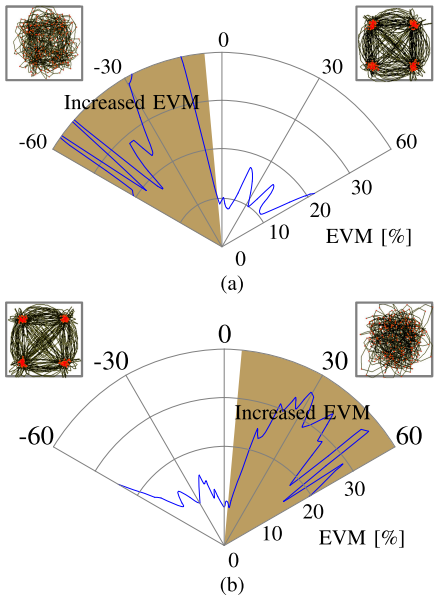


Fig. 26. Reconfigurability of positioning the secure cone. (a) 30°. (b) −30°.

link becomes vulnerable to colluding eavesdropper attacks. Multiple eavesdroppers can simultaneously measure the finite constellation splitting and remap it back to break the channel. They can also monitor the relative change in the power spectrum to determine the modulation frequency and the relative location of the Tx antenna arrays (Alice-to-Eve channel), as seen in the spatial dependence of the spectrum in Fig. 24.

To make the mapping time variant much more challenging for eavesdroppers to collude and learn the channel, one can apply frequency chirping as the time modulation, as illustrated in Fig. 27(a). While a detailed discussion of the attack is beyond the scope of this article [8], the colluding attack is based on the principle that the signals arriving at a set of multiple colluding Eves after free-space propagation are a linear transformation of the modulated signals radiated from the antenna arrays of Alice. For any array excitation of the N-element STMA at Alice ($\mathbf{x}_{\text{Alice}}$), the received signal at the set of colluding Eves ($\mathbf{y}_{\text{Eves}}$) can be expressed as

$$\mathbf{y}_{\text{Eve}} = \mathbf{H}_{\text{Alice-Eves}} \cdot \mathbf{x}_{\text{Alice}} + \mathbf{n}_{\text{Eves}} \tag{13}$$

where $\mathbf{n}_{\text{Eves}}$ is the noise at Eves and $\mathbf{H}_{\text{Alice-Eves}}$ is the channel matrix. With a sufficient number of Eves and with complete channel knowledge ($\mathbf{H}_{\text{Alice-Eves}}$), in principle, the array excitation $\mathbf{x}_{\text{Alice}}$ (and therefore the signal at Bob) can be recovered with channel inversion. This is true unless the SNR is low enough to make recovery extremely challenging.

Since chirping has a flattop spectrum over the frequency range of interest, frequency chirping averages the inter-modulation spectral power, thereby reducing the information exposed by the spectrum. With enough transmitting antennas and wide enough chirping BW, it is possible to hide

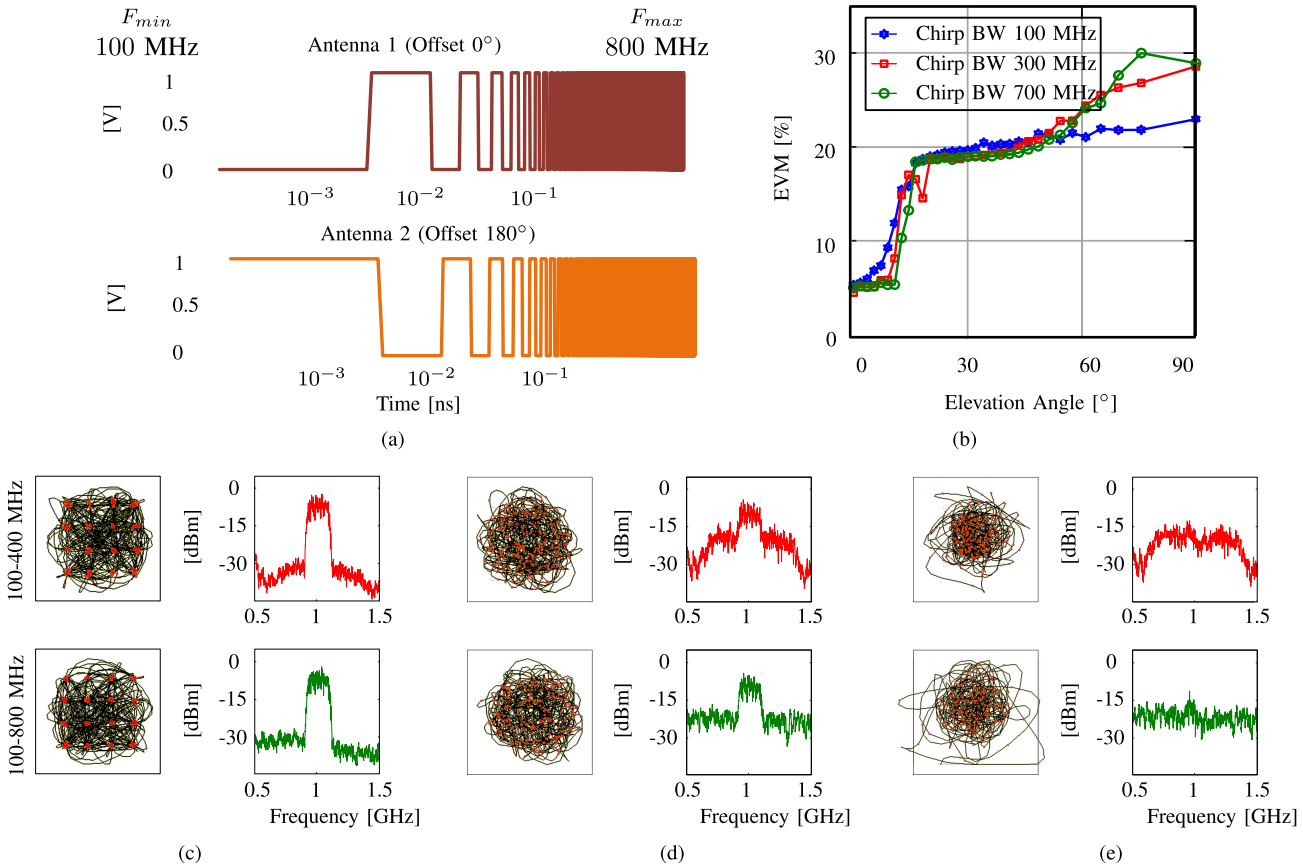


Fig. 27. Enhanced security with noise-like spectral spreading outside the cone and time-varying symbol-to-antenna mapping. (a) Chipping waveform in the time domain used for two Tx chains. (b) EVM across angle for three different chirped cases. (c)–(e) Measured constellation and spectrum for a 200-MHz 16-QAM signal with two different chirped frequencies (100–400 MHz and 100–800 MHz) ranges showing the spectral spread outside the secure cone.

TABLE I
COMPARISON WITH STATE-OF-THE-ART ARCHITECTURES FOR DIRECTIONAL MODULATION

Metrics	This work	[14]	[20]	[11]	[18]	[17]
frequency (GHz)	71-76	60	60	60	2.6	2.6
Process	65nm CMOS	IBM 8HP	65nm COS	40nm CMOS	FPGA+RF switches	CPLD+RF switches
Physical layer security	Time modulation and spectral aliasing	Directional modulation with Near-field anterna modulation	Constellation distortion at off axis angles	Classical phased array (No aliasing)	Tmme modulation and spectral aliasing	Time modulation and spectral aliasing
Operating principle and detection probability reduction	Sub-symbol chopping and non-repetitive mapping, infinite constellation splitting and chirped switched modulation	Antenna switching subset for constellation distortion at off axis angles	Quasi-optical IO combining	NA	Switching optimization	Random time modulation
Antenna	PCB Series Fed Patch	Dipole + silicon lens	PCB Patch	PCB H-shape Patch	PCB dipole	PCB dipole
Bandwidth	With/Wo. Switch 4 Gb/s - 7.5 Gb/s	-	6 Gb/s	4.6 Gb/s	50 kb's	16 Mb's
Psat (dBm)	9	7	9.6	6.5	N/A	N/A
DC Power mW	49/cha.	N/A	4775/cha. w. LO doubler	27/cha.	N/A	N/A
Chip size (mm × mm)	14 × 0.63	2.5 × 5 w. LO + Ant	3 × 3: 8 Cha. + doubler	4.68 × 4.68 TRX+BB	Non-integrated	Non-integrated

the spectrum under the noise floor of eavesdroppers, while the legitimate receiver still sees an original signal above the noise. This is analogous to steganography, in which encryption and power spreading can be achieved by the channel matrix, and

the encryption key to demodulate is the correct receiving angle information.

The effect of frequency chirping with two chains is evaluated. Fig. 27(a) illustrates the chirping waveform used. Two chirping frequency ranges, 100–400 MHz and 100–800 MHz, are compared here in Fig. 27(c) for a 200-MHz 16-QAM signal. The resulting constellations in three directions, 0°, 30°, and 60°, are shown in Fig. 27. Similar to the periodic modulation case, all intermodulation products are canceled at the intended direction (here, broadside). As expected, frequency chirping spreads the spectrum aliasing, thereby raising the noise floor. Therefore, chirping not only hides the Tx's directional information but also makes the link more resistant to possible eavesdropping by spectrum spreading [8]. We can clearly see that the spectrum at broadside is a band-limited signal of 200 MHz approximately 26 dB above the noise floor where, at the eavesdropper at 60°, a scrambled constellation and a near-flat "noise"-like spectrum are observed.

Table I presents the comparison of the presented work with previous works on directional modulation, showing the first STMAs at mmWave with Gb/s links, and techniques to allow reconfigurable time modulation, time-varying symbol-to-antenna mapping, infinite constellation splitting, and chirping to spread the signal spectrum, similar to ambient noise.

V. Conclusion

We present STMAs that incorporate physical layer security into directional mmWave links by creating a secure cone and encoring spectral aliasing, constellation scrambling, and loss of information. We present the tradeoff space and show how effective subsymbol chopping can lead to time-varying symbol-to-antenna mapping that leads to near-infinite constellation splitting, as can be achieved with asynchronous time modulation and frequency chirping. We experimentally demonstrate the functionality of such arrays with 71–76-GHz dual-Tx integrated CMOS chips and packaged antennas. Such physical layer security techniques can be an important part of ensuring security in low-latency and high-BW wireless communication for 5G and beyond.

Acknowledgment

The authors would like to thank all members of IMRL for the technical discussions.

References

[1] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci. USA*, vol. 114, no. 1, pp. 19–26, 2017.

[2] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[3] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[4] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, 2nd Quart., 2017.

[5] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2018.

[6] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, "Jamming strategies for physical layer security," *IEEE Wireless Commun.*, vol. 25, no. 1, pp. 148–153, Feb. 2018.

[7] J. Ma et al., "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, no. 7729, pp. 89–93, Nov. 2018.

[8] S. Venkatesh, X. Lu, B. Tang, and K. Sengupta, "Secure space–time-modulated millimetre-wave wireless links that are resilient to distributed eavesdropper attacks," *Nature Electron.*, vol. 4, no. 11, pp. 827–836, Nov. 2021.

[9] S. Venkatesh, X. Lu, and K. Sengupta, "Spatio-temporal modulated mm-wave arrays for physical layer security and resiliency against distributed eavesdropper attacks," in *Proc. 5th ACM Workshop Millim.-Wave Terahertz Netw. Sens. Syst.*, Oct. 2021, pp. 19–24.

[10] A. Chorti et al., "Context-aware security for 6G wireless: The role of physical layer security," *IEEE Commun. Standards Mag.*, vol. 6, no. 1, pp. 102–108, Mar. 2022.

[11] T. Sowlati, "A 60-GHz 144-element phased-array transceiver for backhaul application," *IEEE J. Solid-State Circuits*, vol. 53, no. 12, pp. 3640–3659, Dec. 2018.

[12] S. Venkatesh, H. Saeidi, X. Lu, and K. Sengupta, "Active tunable millimeter-wave reflective surface across 57–64 GHz for blockage mitigation and physical layer security," in *Proc. IEEE Radio Freq. Integr. Circuits Symp. (RFIC)*, Jun. 2022, pp. 63–66.

[13] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 356–360.

[14] A. Babakhani, D. B. Rutledge, and A. Hajimiri, "Transmitter architectures based on near-field direct antenna modulation," *IEEE J. Solid-State Circuits*, vol. 43, no. 12, pp. 2674–2692, Dec. 2008.

[15] M. P. Daly, E. L. Daly, and J. T. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Trans. Antennas Propag.*, vol. 58, no. 5, pp. 1545–1550, May 2010.

[16] A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, "Directional modulation via symbol-level precoding: A way to enhance security," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1478–1493, Dec. 2016.

[17] Q. Zhu, S. Yang, R. Yao, and Z. Nie, "Directional modulation based on 4-D antenna arrays," *IEEE Trans. Antennas Propag.*, vol. 62, no. 2, pp. 621–628, Feb. 2014.

[18] J. Guo, L. Poli, M. A. Hannan, P. Rocca, S. Yang, and A. Massa, "Time-modulated arrays for physical layer secure communications: Optimization-based synthesis and experimental assessment," *IEEE Trans. Antennas Propag.*, vol. 66, no. 12, pp. 6939–6949, Dec. 2018.

[19] N. Valliappan, A. Lozano, and R. W. Heath Jr., "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231–3245, Aug. 2013.

[20] J. Chen et al., "A digitally modulated mm-Wave Cartesian beamforming transmitter with quadrature spatial combining," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2013, pp. 232–233.

[21] C. Rusu, N. González-Prelcic, and R. W. Heath, "An attack on antenna subset modulation for millimeter wave communication," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Apr. 2015, pp. 2914–2918.

[22] H. E. Shanks and R. W. Bickmore, "Four-dimensional electromagnetic radiators," *Can. J. Phys.*, vol. 37, no. 3, pp. 263–275, Mar. 1959.

[23] J. Guo, S. Yang, Y. Chen, P. Rocca, J. Hu, and A. Massa, "Efficient sideband suppression in 4-D antenna arrays through multiple time modulation frequencies," *IEEE Trans. Antennas Propag.*, vol. 65, no. 12, pp. 7063–7072, Dec. 2017.

[24] G. Li, S. Yang, Y. Chen, and Z.-P. Nie, "A novel electronic beam steering technique in time modulated antenna array," *Prog. Electromagn. Res.*, vol. 97, pp. 391–405, 2009.

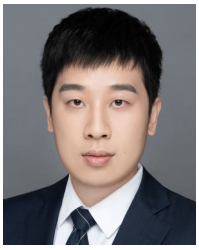
[25] A. Tennant, "Experimental two-element time-modulated direction finding array," *IEEE Trans. Antennas Propag.*, vol. 58, no. 3, pp. 986–988, Mar. 2010.

[26] Y. Tong and A. Tennant, "A two-channel time modulated linear array with adaptive beamforming," *IEEE Trans. Antennas Propag.*, vol. 60, no. 1, pp. 141–147, Jan. 2012.

[27] X. Lu, S. Venkatesh, B. Tang, and K. Sengupta, "4.6 space-time modulated 71-to-76 GHz mm-Wave transmitter array for physically secure directional wireless links," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2020, pp. 86–88.

[28] A. Ahmad, M. Amin, and M. Farooq, "Analyzing directional modulation techniques as block encryption ciphers for physical layer security," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2017, pp. 1–6.

[29] S. G. Lee and J. K. Choi, "Current-reuse bleeding mixer," *Electron. Lett.*, vol. 36, no. 8, pp. 696–697, Apr. 2000.
[30] X. Lu, C. R. Chappidi, X. Wu, and K. Sengupta, "Antenna preprocessing and element-pattern shaping for multi-band mmWave arrays: Multi-port receivers and antennas," *IEEE J. Solid-State Circuits*, vol. 55, no. 6, pp. 1455–1470, Jun. 2020.
[31] C. R. Chappidi, X. Lu, X. Wu, and K. Sengupta, "Antenna preprocessing and element-pattern shaping for multi-band mmWave arrays: Multi-port transmitters and antennas," *IEEE J. Solid-State Circuits*, vol. 55, no. 6, pp. 1441–1454, Jun. 2020.



Xuyang Lu (Member, IEEE) received the B.S. degree in electrical engineering from Rice University, Houston, TX, USA, in 2014, and the M.A. and Ph.D. degrees in electrical engineering from Princeton University, Princeton, NJ, USA, in 2016 and 2020, respectively.

In 2021, he joined the University of Michigan–Shanghai Jiao Tong University Joint Institute, Shanghai Jiao Tong University, Shanghai, as an Assistant Professor. He was dually appointed to the Department of Electronic Engineering, Shanghai Jiao Tong University, in October 2021. He is currently with the State Key Laboratory of Radio Frequency Heterogeneous Integration and the Department of Electronic Engineering, Shanghai Jiao Tong University. His research spans high-speed programmable RF and millimeter-wave (mmWave) integrated systems, integrated terahertz systems, integrated photonics, on-chip antenna optimization, and the intersection of machine learning with analog circuit design.

Suresh Venkatesh (Senior Member, IEEE) received the M.S. degree in electrical and computer engineering from North Carolina State University, Raleigh, NC, USA, in 2010, and the Ph.D. degree in electrical and computer engineering from The University of Utah, Salt Lake City, UT, USA, in 2017.

He was an Associate Research Scholar at the Department of Electrical and Computer Engineering, Princeton University, Princeton, NJ, USA, and a Lead Antenna Technology Consultant for Massachusetts-based start-ups, namely, Wafer LLC and E-Space, Beverly, MA, USA, where he developed SATCOM technologies for high-speed low-latency communications. He was a Research Project Assistant at the Molecular Astronomy Laboratory, Raman Research Institute, Bengaluru, India, from 2007 to 2008, where he worked on a millimeter-wave radio telescope. He is currently an Assistant Professor at the Department of Electrical and Computer Engineering, North Carolina State University. He has authored or coauthored more than 60 journal and conference publications. His research interests are in electromagnetics, metamaterials, antenna design, integrated circuits, computational imaging, and transformation optics design.

Dr. Venkatesh is an Affiliate Member of the MTT-23 Wireless Communication and MTT-21 Terahertz Technology and Applications committees. His Ph.D. dissertation received the ECE Outstanding Dissertation Award in 2016.

Bingjun Tang (Member, IEEE) received the M.S. degree in integrated circuits from Xi'an Jiaotong University, Xi'an, China, in 2014, where he is currently pursuing the Ph.D. degree in electrical engineering.

He joined Prof. Sengupta's laboratory in October 2018 as a Visiting Student. His research area is mainly about CMOS active circulators, and self-interference cancellation for full-duplex, phase-locked loop (PLL), voltage-controlled oscillators (VCOs), and terahertz (THz) oscillators.

Kaushik Sengupta (Senior Member, IEEE) received the B.Tech. and M.Tech. degrees in electronics and electrical communication engineering from IIT Kharagpur, Kharagpur, India, in 2007, and the M.S. and Ph.D. degrees in electrical engineering from California Institute of Technology (Caltech), Pasadena, CA, USA, in 2008 and 2012, respectively.

In 2013, he joined the Department of Electrical and Computer Engineering, Princeton University, Princeton, NJ, USA, as a Faculty Member, where he is currently a Professor and the Director of the Integrated Microsystems Research Laboratory. His current research interests include high-frequency integrated circuits (ICs), electromagnetics, and optics for various applications in sensing, imaging, and high-speed communication.

Dr. Sengupta received the DARPA Young Faculty Award in 2018, the Bell Labs Prize in 2017, the Young Investigator Program Award from the Office of Naval Research in 2017, the E. Lawrence Keys, Jr. Emerson Electric Co. Junior Faculty Award from the Princeton School of Engineering and Applied Science in 2018, and the Excellence in Teaching Award in 2018 nominated by the Undergraduate and Graduate Student Council in the Princeton School of Engineering and Applied Science. He received the Outstanding Young Engineer Award from IEEE Microwave Theory and Techniques in 2021, and the IEEE Solid-State Circuits New Frontier Award in 2022. He was a recipient of the Charles Wilts Prize in 2013 from Electrical Engineering, Caltech, for the best Ph.D. thesis, the Caltech Institute Fellowship, the Prime Minister Gold Medal Award of IIT in 2007, and the inaugural Young Alumni Achievement Award from IIT Kharagpur. He was a co-recipient of the IEEE Radio Frequency Integrated Circuits (RFIC) Symposium Best Student Paper Award in 2012, multiple best student paper awards in IEEE IMS, and the 2015 Microwave Prize from the IEEE Microwave Theory and Techniques Society. He is on the Technical Program Committee of International Solid-State Circuits Conference (ISSCC) in the Technology Directions Sub-Committee. He has served as the Chair for Emerging Technologies for IEEE Custom Integrated Circuits Conference (CICC) in 2022. He currently serves as a co-chair of Chair of the IEEE Solid-State Circuits Directions Committee, and as a technical advisor for the wireless startup Guru Inc., based in Pasadena. He served as a Distinguished Lecturer for the IEEE Solid-State Circuits Society from 2019 to 2020, and as Distinguished Lecturer for the IEEE Microwave Theory from 2021–2023.