New Frontiers in Silicon Terahertz Electronics: Wirelessly Powered THz-ID and Secure THz Links

by

Muhammad Ibrahim Wasiq Khan

B.E., National University of Science and Technology (2012)
MSc., Korea Advanced Institute of Science and Technology (2016)

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Electrical Engineering and Computer Science

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

May 2022

Author .....
Department of Electrical Engineering and Computer Science
May 13, 2022

Certified by .....
Ruonan Han
Associate Professor of Electrical Engineering and Computer Science
Thesis Supervisor

Accepted by .....
Leslie A. Kolodziejski
Professor of Electrical Engineering and Computer Science
Chair, Department Committee on Graduate Students

New Frontiers in Silicon Terahertz Electronics: Wirelessly Powered THz-ID and Secure THz Links

by

Muhammad Ibrahim Wasiq Khan

Submitted to the Department of Electrical Engineering and Computer Science
on May 13, 2022, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy in Electrical Engineering and Computer Science

Abstract

Advances in silicon integrated electronics have enabled many significant systems and applications in the terahertz (THz) band over the last decade. However, ultra-low-power ($<25\mu$W) or battery-less THz transceivers have not been explored yet due to the stringent challenges posed by them. Likewise, the notion of wireless power transfer at THz frequency is non-existence. There is a growing demand for low-power mm-size transceivers in supply chain management, assets tracking, authentication, micro-robotics, on-skin or close-to-skin implants, etc. With these ubiquitous THz-links, the security of the wireless channels is another emerging challenge. Advanced digital encryption techniques are computationally intensive, power-hungry, and not suited for these low-power applications. This thesis explores the challenges and novel approaches to realizing ultra-low-power/battery-less and physically secure THz transceivers. Specifically, it demonstrates three new frontiers in standard CMOS technologies that will open up the THz band. The first is a mm-size 0.26 THz identification tag (THz-ID) enabling μW level THz link by exploiting back-scattering and beam-steering functionalities. It is the smallest, package-less, monolithic ID chip with far-field communication capability and asymmetric cryptography. The second is the optimization based on dual-antenna architecture for 0.26 THz energy harvesting with $\sim$25μW harvesting capability. It is the highest frequency of CMOS harvester by $\sim$3x and has the highest RF-to-DC conversion efficiency at low input power. And the third is developing an orbital-angular-momentum (OAM) wave-based transceiver with bits-to-OAM modes mapping for secret key distribution at 0.31 THz frequency. It is the first chip-based demonstration (at any frequency) of a transceiver front-end that transmits and receives OAM waves. It is also the smallest, least power consuming OAM transceiver and it can dynamically switch among OAM modes. The thesis concludes with potential improvements and prospects for the future work.

Thesis Supervisor: Ruonan Han
Title: Associate Professor of Electrical Engineering and Computer Science

Acknowledgments

Foremost, I would like to express my utmost gratitude to my thesis supervisor, Prof. Ruonan Han, for his continuous support of my Ph.D. study and research, and his patience, guidance, encouragement, and mentorship. His vision, enthusiasm, and insightful knowledge helped me a lot with my research work. He has been more than a technical supervisor to me and I have learned a lot from him throughout my Ph.D.

I would also like to thank my Ph.D. committee members Prof. Anantha P. Chandrakasan and Prof. Qing Hu. I was fortunate to work with Prof. Anantha P. Chandrakasan through collaborations on many projects notably THz-ID and THz-OAM transceiver. I am thankful to him for all his ideas and technical pieces of advice. His insightful feedback helped me improve my work and make career decisions. His support during the chip measurement was also crucial in the timely completion of many projects.

Special thanks to my colleague and friend Mohamed I. Ibrahim who has worked closely with me for over three years on THz-ID and THz-OAM projects. I am very fortunate to have him as a close friend and coworker in other projects as well. I would also like to thank Chiraag Juvekar for working with Mohamed and me on THz-ID project. The discussions with him were very helpful. I am grateful for the technical advice and contributions from Rabia T. Yazicigil and Wanyeong Jung in the THz-ID project. This work would not be completed without their help.

I would like to especially thank Xiang Yi for his designs and recommendations for the THz-OAM chip as well as his help in the measurements. I would like to acknowledge the contributions of Jongchan Woo and Rabia T. Yazicigil to the THz-OAM project and their help with the chip measurements. I want to thank Nathan N. Monroe for helping me in setting up Intel's PDK and Eunseok Lee for his contribution to the THz energy harvesting project.

Furthermore, thanks for the technical discussions and assistance from the rest of my labmates at the THz integrated electronics group including but not limited to: Cheng Wang, Zhi Hu, Mina Kim, Mohamed Elsheikh, Xibi Chen, and Jinchen Wang.

Last but not least, I would like to thank my family and friends. Especially, my parents for their love, care, and support during my studies and research. There are no words that can express my appreciation for them. In addition, I would also like to thank my wife for her patience. She has been the best partner, friend, and supporter. I cannot express my gratitude to her.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Exploring terahertz (THz) gap on-chip has gained significant interest over the past decade to enable new opportunities in imaging, radar, and broadband communications [11–14]. However, utilizing the overlooked aspect of THz systems, which is the ability to shrink the communication node size with the challenge of keeping low-power operation, can pave the way to new paradigms for wireless sensing and IoT systems, especially with the advances in 6G and beyond. One potential application is in the miniaturization of far-field Radio Frequency Identification (RFID) tags which are widely used for counterfeit mitigation, authentication and supply chain management. Small form factor, power efficiency and cost are the important requirements of these tags which are often limited by off-chip antenna and packaging. Operating at THz frequency removes these limitations by enabling on-chip antenna array within mm-size with sufficient gain. In this thesis, we present an ultra-small identification tag that is entirely built in a CMOS chip without external components. The usage of back-scatter communications at 260 GHz enables full integration of a 2×2 patch antenna array. For chip compactness and minimum interference caused by direct wave reflection, the back-scatter signal is frequency-shifted by 2 MHz and radiated with cross-polarization from the same antenna array. Such a configuration also, for the first time for RF tags, enables beam-steering for enhanced link budget. The presented tag has a peak power consumption of 21 μW and can be powered by a chip-wide array of photodiodes. Using a low-cost 65-nm bulk CMOS technology, the

THz-ID chip has an area of only 1.6 mm^2 and demonstrates a measured downlink speed of 100 kbps and upload speed of 2 kbps across 5 cm distance from the reader. The tag-reader authentication/communication protocol is fully demonstrated using external tag power and partially demonstrated using the tag-integrated photo-voltaic powering. The photo-voltaic powering limits the applications of THz-ID to optically-transparent packaging and there is a need for THz energy harvester. Therefore, this thesis next explores the challenges of wireless power transfer at THz frequency for ultra-miniaturized and battery-less platforms. A CMOS energy harvester, which operates at so far the highest reported frequency (263 GHz) is presented. To maximize the THz-to-DC conversion efficiency at low available radiation power, the harvester not only utilizes a high-speed 22-nm FinFET transistor but also achieves the optimal operating conditions of the device. In specific, the circuit enables self-gate biasing; and through a dual-antenna topology, it drives the transistor drain and gate terminals with both optimal voltage phase difference and power ratio simultaneously and precisely. With a low input power of -8 dBm, the harvester achieves 13.6% measured conversion efficiency and delivers 22 μW to a 1-kΩ load. Without relying on any external component, the harvester chip occupies an area of 0.61×0.93 mm^2. This is a breakthrough for THz circuits that will enable many new technologies and open new research directions.

Large antenna arrays at the sub-THz/THz bands are basic building blocks for 6G networks. An emerging challenge is the security of these ubiquitous THz-links, which are susceptible to eavesdropping at unintended positions, due to beam divergence and antenna sidelobes. Traditionally, wireless communication is secured at network and application layers using digital encryption techniques which rely on trustworthy secret key distribution. Such security architectures are becoming computationally intensive and are not scalable with THz-links operating at multi-Gbps with strict energy constraints and latency requirements. Physical-layer security (PLS) significantly relaxes the requirements for security at other layers. Orbital-angular-momentum (OAM) is a potential candidate that can physically secure the one-way transmission of secret keys in such networks and is easily generated from planar antenna arrays. In or-

der to demonstrate the above-mentioned security application this thesis reports the first chip-based THz-OAM transceiver. The chip consists of eight 0.31-THz modulator/detector units, with integrated patch antenna, which are placed in a uniform circular pattern with a diameter of one free-space wavelength. The chip transmits OAM modes that are digitally switched among the m=0 (plane wave), +1 (left-handed), -1 (right-handed) and (+1)+(-1) (superposition) states. The chip is also reconfigurable into a receiver mode that identifies different OAM modes with >10 dB rejection of mismatched modes. The array, driven by only one 310 GHz signal generation path, has a measured EIRP of -4.8 dBm. Using a 65-nm bulk CMOS technology, the THz-OAM chip has an area of only 2.1×2.6 mm^2, which is the smallest among all prior OAM prototypes. The output OAM beam profiles and modes' orthogonality are experimentally verified. The dynamic mode switching capability of the chip is also verified in time domain across a 1 m distance and a full-silicon OAM link is demonstrated. Robustness of OAM-PLS using the presented chip is also analyzed through different threat models.

1.1 Thesis Organization

This thesis is organized as follows:

1. **Chapter 2** presents the motivation for the THz-ID, some related works and critical innovations. Next, the overall architecture of the chip is presented. Details of the THz front-end i.e., downlink and uplink circuits are also given. Then, the security protocol and the photo-voltaic powering scheme are discussed. Finally, the experimental demonstrations and comparisons with the prior state-of-the-art are presented.

2. **Chapter 3** presents the motivation and potential applications for wireless power transfer at THz frequency and the challenges that need to be overcome. It presents a step-by-step optimization for efficient THz harvester design. The measurement results are presented and compared with the prior state-of-the-

art. Next, this work is extended to the second prototype of THz-ID that harvests power from the THz signal as well as uses it for back-scatter communication.

3. **Chapter 4** introduces the concept of orbital-angular-momentum (OAM) and presents its applications. Next, the system architecture for the THz-OAM transceiver chip is presented. Details of the transmitter and receiver circuits integrated into the THz pixels are also given. The experimental demonstrations and comparisons with the prior state-of-the-art are presented. Finally, certain threat models are also discussed for OAM-based security.

4. **Chapter 5** presents the motivation and limitations of ingestible electronics. Next, the stringent requirements for a Bluetooth Low Energy (BLE) compatible wake-up receiver are presented. Then, the overall system design and circuit details are given.

5. **Chapter 6** provides a conclusion for the projects presented in this thesis. It also points out some potential improvements and the future research directions.

1.2 Publications

Much of the work presented in this dissertation has been previously published or submitted for publication. The main works contributing to this thesis are as follows.

- [15] M. I. Ibrahim, **M. I. W. Khan**, C. S. Juvekar, W. Jung, R. T. Yazicigil, A. P. Chandrakasan, and R. Han, "THzID: A 1.6mm^2 Package-Less Cryptographic Identification Tag with Backscattering and Beam-Steering at 260GHz," *IEEE International Solid-State Circuits Conference - (ISSCC)*, San Francisco, CA, Feb. 2020.

- [16] **M. I. W. Khan**, M. I. Ibrahim, C. S. Juvekar, W. Jung, R. T. Yazicigil, A. P. Chandrakasan, and R. Han, "CMOS THz-ID: A 1.6-mm^2 Package-Less Identification Tag Using Asymmetric Cryptography and 260-GHz Far-Field

Backscatter Communication," *IEEE Journal of Solid-State Circuits*, vol. 56, no. 2, pp. 340-354, Feb. 2021.

- [17] **M. I. W. Khan**, J. Woo, X. Yi, M. I. Ibrahim, R. T. Yazicigil, A. P. Chandrakasan, and R. Han, "A 0.31-THz CMOS Uniform Circular Antenna Array Enabling Generation/Detection of Waves with Orbital Angular Momentum," *IEEE Radio Frequency Integrated Circuits Symposium (RFIC)*, 2021, pp. 203-206. **(Best Student Paper Award – First Place)**

- [18] **M. I. W. Khan**, J. Woo, X. Yi, M. I. Ibrahim, R. T. Yazicigil, A. P. Chandrakasan, and R. Han, "A 0.31-TTHz Orbital-Angular-Momentum (OAM) Wave Transceiver in CMOS with Bit-to-OAM Mode Mapping," *IEEE Journal of Solid-State Circuits, RFIC Special Issue,* vol. 57, no. 5, pp. 1344-1357, May 2022. **(Invited)**

- (Accepted) **M. I. W. Khan**, Eunseok Lee, Nathan M. Monroe, A. P. Chandrakasan, and R. Han, "A Dual-Antenna, 263GHz Energy Harvester in CMOS for Ultra-Miniaturized Platforms with 13.6% RF-to-DC Efficiency at -8dBm Input Power," *IEEE Radio Frequency Integrated Circuits Symposium (RFIC)*, 2022.

Chapters 2 and 4, reproduce and adapt material from previously published works. Chapter 2 is adapted from Ref. [15], and [16], while Chapter 4 being adapted from Ref. [17], and [18].

1.3 Co-worker Contributions

The collaborative work presented in this thesis would not have been possible without the valuable contributions of my research colleagues. I would like to acknowledge my thesis supervisor Prof. Ruonan Han, who guided me through all the projects presented in this thesis. The substantial guidance and technical inputs of Prof. Anantha P. Chandrakasan to the work presented here were also crucial. The rest of my co-workers' contributions are summarized below:

- The THz-ID system design presented in Chapter 2 was led in a collaboration with Muhammad I. Ibrahim and assisted by Chiraag S. Juvekar, Rabia Tugce Yazicigil, and Wanyeong Jung. Mohamed and I were responsible for the THz/analog front-end. I designed the THz square-law detector, coupler, SSB mixer and matching network in the back-scattering module and the base-band amplifier. Mohamed constructed the multi-feed patch antenna and was responsible for the co-design of the antennas and the photodiode array. Wanyeong designed the DC-DC converter. Chiraag and Rabia designed the cryptographic processor. I designed the THz reader using off the shelf components for the chip measurements. Chiraag did the coding for the communication protocol. Mohamed, Chiraag, and I performed the experiments.

- THz energy harvesting presented in Chapter 3 is entirely led by me. In this effort, I tested many devices and topologies, and also tape out a chip based on a custom-designed Schottky diode in 65-nm CMOS process. The chip didn't work properly due to lack of accurate simulation models for the custom diodes. Finally, I found Intel's 22-nm FinFET to be a good candidate and optimized the harvester circuit design. Eunseok Lee contributed to the DC-DC converter design for the second prototype of THz-ID and Nathan M. Monroe helped me with setting up Intel's 22FFL PDK and associated DRC, LVS, and QRC scripts. I conducted the chip measurements.

- I also led the THz-OAM system design presented in Chapter 4. Prof. Ruonan Han initially explored the idea of OAM and we jointly came up with system architecture. I designed all the THz front transmitter and receiver circuits as well as the baseband circuits. The multiplier-amplifier chain circuits were modified from the design of Xiang Yi. Jongchan Woo and Rabia T. Yazicigil designed the controller. I designed the measurement setup including spiral-phase plates and 3D printed fixtures. Mohamed did the chip wire-bonding and he helped me with some experiments.

- The BLE-compatible wake-up receiver presented in Chapter 5 is led by Yeseul

Jeon. I designed the RF front end including LNA, mixer, and custom-design antenna as well as the baseband circuits. I presented the idea of air-gap for mitigating the shift in antenna resonance frequency. I also improved the FSK demodulator circuit previously designed by Mohamed Radwan. Yeseul and I designed the impedance sensor and tunable matching network and did the FBAR measurements. Pierce oscillator is designed by Saebyeok Shin.

Chapter 2

CMOS THz-ID: A 1.6mm^2 Package-less Identification Tag using 260-GHz Far-Field Back-scatter Communication

2.1 Motivation

Radio-frequency identification (RFID) tags have been widely adopted in tracking, authentication, localization, supply-chain management, health care, and so on [19]. They are filling the information gap between the physical world and the digital world, maximizing efficiency and improving quality of life. For example, inside a hospital, a fine-grained localization and authentication technology can help doctors and nurses keep track of assets and medicines, and thus, reduces operational cost while increasing the quality of patient care [20,21]. In retail, locating items on shelves and tracking the movement of goods improves customer experience and provides valuable analytics for store owners [22, 23]. In the supply chain, such capability can optimize pallet loading and quality control processes, in which a lot is done manually today [24,25]. According to Semiconductor Industry Association "Counterfeiting costs US-based semiconductor

companies more than $7.5 billion per year" [26]. Therefore, there is a growing need for ultra-miniaturized far-field tags that can even be embedded inside integrated chips for authentication throughout their lifetime.

At present, commercial RFID chips rely on an external antenna or inductor packaging to facilitate efficient coupling of the RF waves. That, however, significantly increases the overall size of the tag, making it impossible to be attached to small objects such as medical pills, tooth implants, and semiconductor chips. The associated authentication and recording of manufacturing data, therefore, can only be realized indirectly through special treatments (e.g., holographic patterns) on the goods packages, which leave loopholes for counterfeiting. Another barrier for RFID applications is the additional cost associated with chip packaging, which takes up to two-thirds of the total tag cost [27, 28]. That makes RFID technologies much less competitive than optical identification systems (based on barcodes or QR-codes), for example, printed barcodes for low-cost products (e.g., a 50-cent candy bar) [19]. Lastly, it is noteworthy that pervasive electronic tagging raises serious privacy concerns related to inadvertent and malicious tracking of the tagged assets. Other sensitive data related to, for example, finance and personal health, are also increasingly generated by RFIDs. However, high-security encryption and authentication protocols normally require intensive computing, making reliable data protection difficult to realize in power/hardware-constraint RFID operation environments.

2.2 Related Works

To enable secure and ubiquitous asset tagging, fully-passive, particle-sized identification chips without external packaging are highly desired. However, the recently demonstrated prototypes [29–34] that took the above path face either size, energy, communication, or security limitations (summarized in Fig. 2-1). In [29], a 9-mm^2 sensor node (volume=27 mm^3) is implemented at 915MHz out of a stacked packaging of multiple functionality layers for photo-voltaic powering, battery, antenna, etc. This increases the overall size and cost of the sensor node. In [30], a 116×116 μm^2

monolithic radio chip is demonstrated, that relies on near-field inductive coupling at 5.8 GHz with an on-chip coil antenna, which severely limits the operation range to ∼1 mm. In comparison, far-field tag interrogation using resonant antennas effectively increases the range. Using this principle, a pad-less chip with 24-GHz downlink and 60-GHz uplink boosts the range to 50 cm [31,35], but the chip-integrated transmitter (Tx) and receiver (Rx) antennas at two different frequencies also increase the chip size to 3.7×1.2 mm^2. While this is already an impressive form factor, to fully enable the applications described previously, further miniaturization is desired. In [33], a mm-Wave power-harvesting RFID tag is presented where the chip size is 1.3×0.95 mm^2 without including the antenna. The off-chip 60 GHz antenna increases the size and requires special packaging. A bidirectional 0.32 THz radio is presented in [34] with a size of 0.57 mm^2 because of on-chip Tx and Rx antennas. However, this work doesn't involve power harvesting and requires a separate battery for its 49.3 mW peak DC power consumption. The additional battery increases the size of the whole package. It is also noteworthy that all the above works [29–31, 33, 34] also do not support cryptographically secure identification. To this end, [32] demonstrates a secure authentication tag, but the chip requires an 8-mm^2 433MHz external antenna and works by inductive coupling which limits its operation range.

2.3 Innovations

The major challenge of tags' physical size is dominated by the size of resonant antenna which is important for efficient far-field communication. The size of a resonant antenna is of the order of $\sim \lambda_o/2$ where λ_o is the wavelength. This indicates that operating at THz frequency will drastically reduce the antenna size enabling the mm-size form-factor for the tags. Fig. 2-1 compares the size of previously reported work with the proposed THz-ID emphasizing size scaling with frequency. The aggressive CMOS scaling allows for THz tags but THz circuits (e.g., oscillators) consume a large DC power making them incompatible with field-deployable applications. This hurdle is overcome through photovoltaic energy-harvesting and back-scattered communication

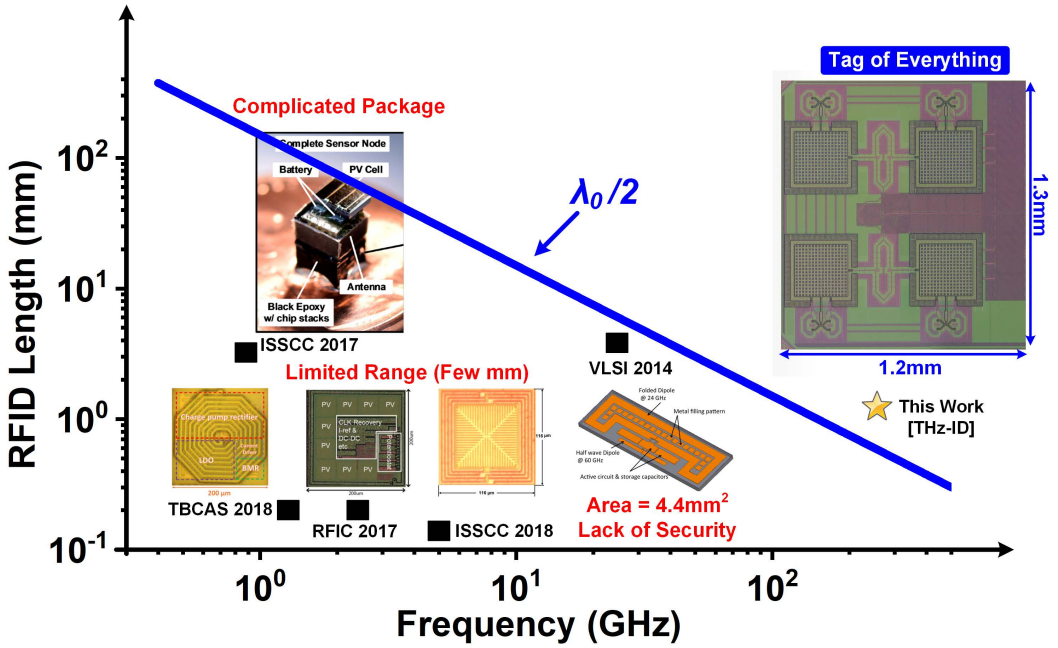
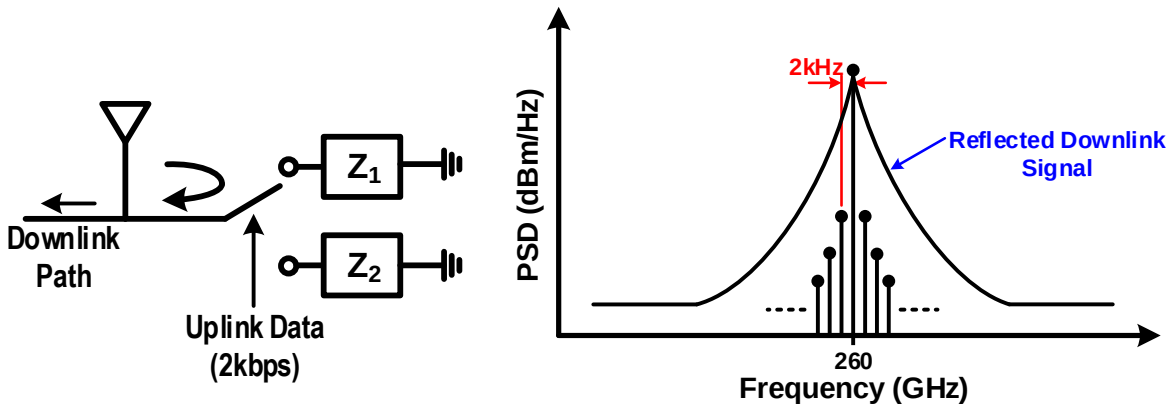


Figure 2-1: Size comparison of previous works. Blue line indicates the reduction in the size of a resonant antenna with frequency.

in the proposed design.

Conventional RFIDs are based on antenna impedance modulation to back-scatter the tag's data (Fig. 2-2a), i.e. by changing the antenna impedance, the amplitude or the phase of the reflection coefficient is changed. To enable THz operation, the carrier frequency of conventional RFIDs (few GHz) increases by ∼100×. Consequently, the phase noise also increases by ∼40-dB. Therefore, the above-mentioned back-scattering technique doesn't work at THz frequency as the weak back-scattered signal will be submerged in the phase noise of the strong reflected signal, making it impossible to recover the uplink data. A conceptual plot of the spectrum of ON/OFF-shift-keying (OOK) back-scattered signal with a data rate of 2 kbps is shown in Fig. 2-2b.

In this thesis, we propose a novel architecture to avoid the previously mentioned limitations. As shown in Fig. 2-3a, the downlink continuous-wave (260 GHz) from the reader is received using one polarization (Pol. 1). Then, this signal is frequency-shifted by 2 MHz using a single-sideband mixer (SSB). Finally, the back-scattered signal is transmitted back on the orthogonal polarization (Pol. 2). As it can be seen in Fig. 2-3b, the proposed architecture helps in boosting the SNR, since the wanted

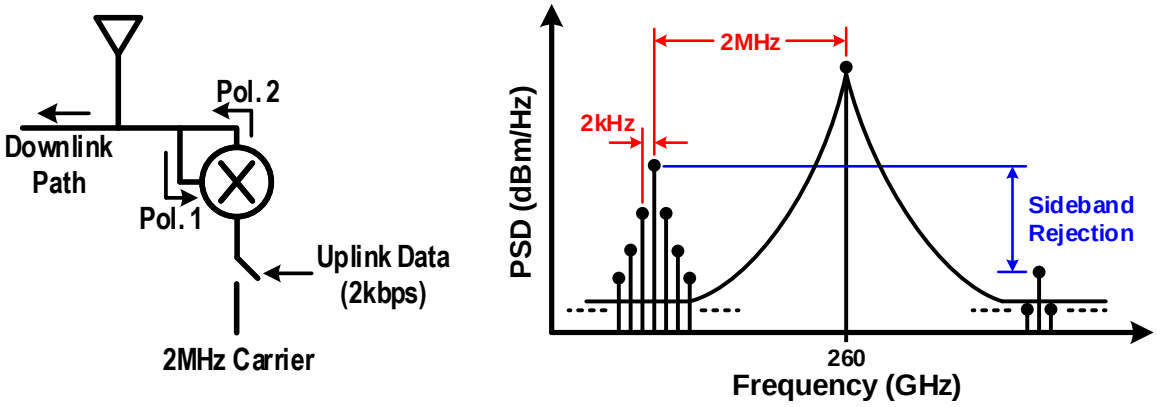


(a) (b)

Figure 2-2: (a) Conventional RFID back-scattering architecture. (b) A conceptual spectrum of OOK modulated back-scattered signal with data rate of 2 kbps.

modulated signal is pushed away from the high phase noise. In addition, the carrier phase noise is further reduced by ∼20 dB due to the cross-polarization rejection.

This thesis presents a package-less, monolithic tag chip in CMOS, that has a size of 1.2×1.3 mm^2 (shown in Fig. 2-4) [15, 16]. To enable far-field operation with such a small form factor, the downlink/uplink carrier frequency is pushed into the low THz regime (260 GHz). That, along with a Tx-Rx antenna sharing technique, allows for on-chip integration of a 2×2 antenna array and a tag-side, beam-steering capability. An operation range of 5 cm is demonstrated, which makes barcode-reader-like applications possible. A frequency-shifted back-scattering technique with orthogonal radiation polarization is employed which helps in distinguishing weak back-scattered signal from strong reflection of the incident wave. Meanwhile, an ultra-low-power elliptic-curve-cryptography (ECC) dedicated processor is integrated in the THz-ID chip, which provides high-security compact asymmetric encryption. The whole chip consumes a peak power of 21 μW, which is provided by an array of chip-integrated photodiodes.



(a) (b)

Figure 2-3: (a) Proposed frequency-shifted back-scattering with orthogonal polarization. (b) A conceptual spectrum of OOK modulated back-scattered signal with a data rate of 2 kbps and a frequency shift of 2 MHz.

2.4 THz-ID Hardware Architecture

The architecture of the tag chip is shown in Fig. 2-5. The incident 260-GHz wave (red) from the reader is coupled to a 2×2 array of on-chip patch antennas. The THz signal with a particular linear polarization received by each antenna is extracted from two sets of antenna feeds with a power-splitting ratio of ∼1:1. Half of this power, used for the downlink, is rectified to baseband via four THz square-law detectors. The other half of the input power is used for the back-scatter uplink communication. It is noteworthy that a strong, direct reflection of the incident downlink wave, due to the large surface of the object to be tagged, is inevitable. It is, therefore, critical to eliminate the interference of such reflected waves to the actual data-modulated signal, which is back-scattered by the chip. To this end, single-sideband (SSB) frequency mixing is added to the back-scattering process, so that the final carrier frequency for the uplink (f_{UL}) is ∼2 MHz below that for the downlink (f_{DL}). Meanwhile, the chip is designed so that the polarization of the back-scattered wave (blue in Fig. 2-5) is also rotated by 90°, so that the tag reader's receiver antenna with a linear polarization aligned with the back-scattered wave can further suppress the directly

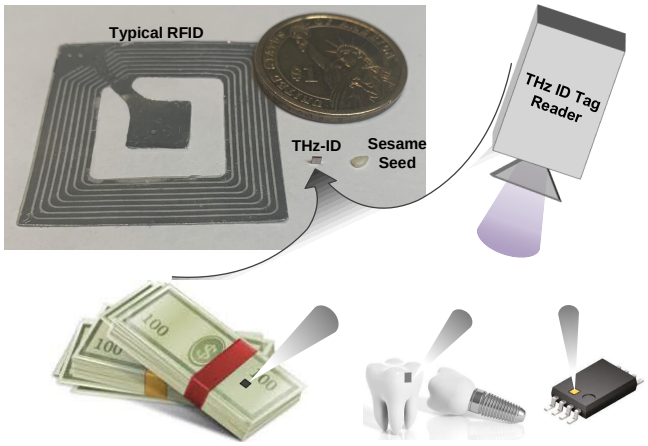


Figure 2-4: THz-ID tag: a size comparison and its potential applications.

reflected wave by >20 dB. The cross-polarization scheme also allows for re-using the downlink antennas for uplink antennas, which reduces the tag area by ∼2x. More details of the antennas will be given in Section 2.5.1.

Both the downlink and the uplink utilize ON/OFF-shift-keying (OOK) modulation, and offer data rates at 100 kbps and 2 kbps, respectively. The THz SSB mixers for the frequency shifting of the uplink carrier are driven by four 2-MHz local-oscillator (LO) signals generated by an integrated processor. With independent, digital control of the phase in each LO, beam-steering for the THz uplink wave is achieved. That enhances the link budget when the tag is not perpendicularly facing the tag reader. Moreover, without the beam-steering capability, the tag would act as a mirror and make the back-scatter communication more prone to eavesdropping.

In our protocol, the cryptographic processor first sweeps the uplink beam direction until reliable communication is established. Then it will work with the reader to perform a narrow-strong private identification protocol [36] under a public-key cryptography scheme (specifically elliptical-curve cryptograhy). It guarantees that any eavesdropper who does not possess the readers' private key cannot identify which tag participates in the protocol by merely monitoring the wireless link.

The photo-voltaic powering of the tag is realized through a large array of P-N photodiodes placed under and beside the antennas. To allow the incident light to reach the photodiodes, the patch and the ground plane of the antenna possess a

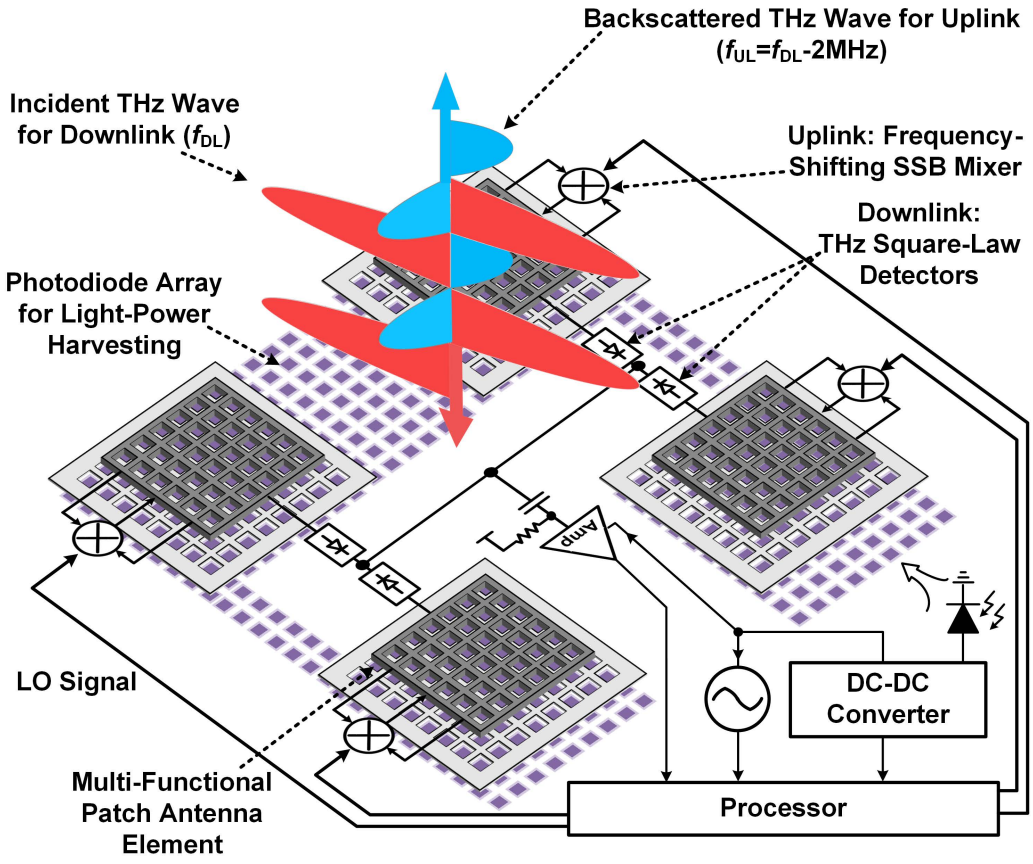


Figure 2-5: Overall architecture of the THz-ID tag.

fishnet pattern (Fig. 2-5). A DC-DC converter is implemented in order to boost the photodiode output voltage to ∼1 V. A 8-MHz oscillator is integrated to provide the LO signal for the THz SSB mixers, as well as the clock signals for the DC-DC converter and the cryptographic processor.

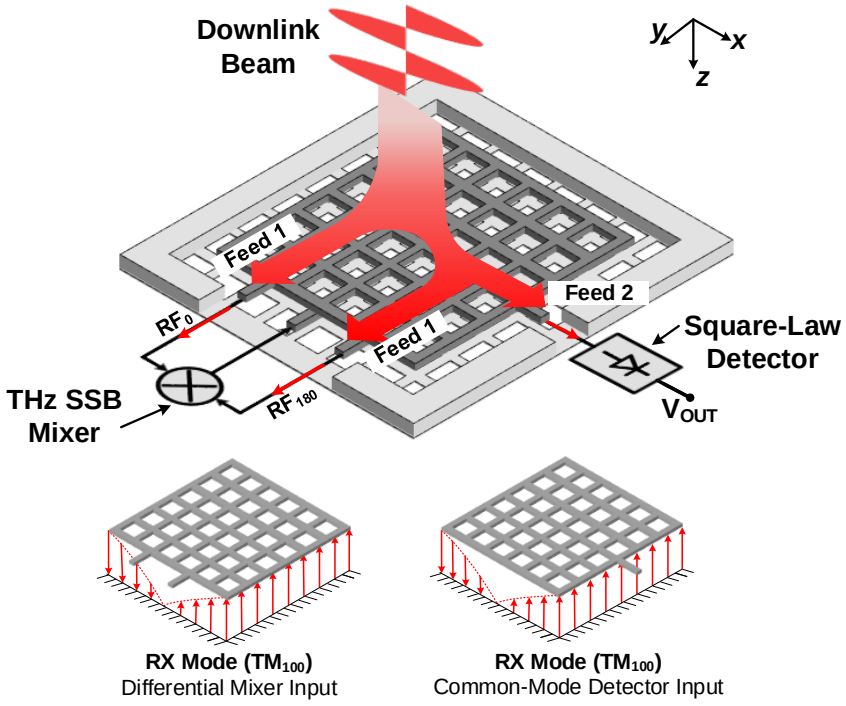
2.5 THz Downlink and Uplink

In this section, I describe the design of various tag components that enable 260-GHz communication with very small power consumption and chip area.

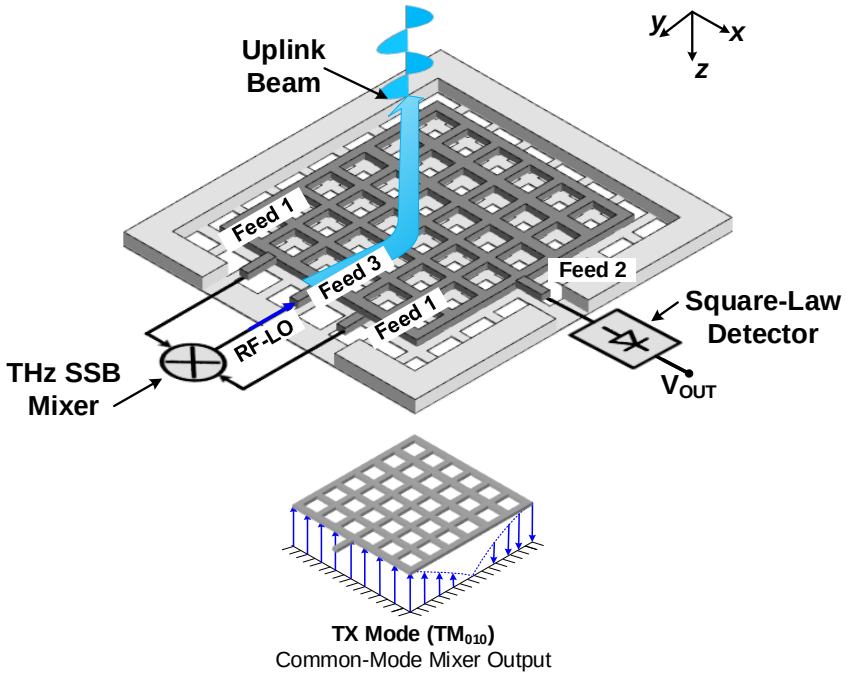
2.5.1 Multi-Functional On-Chip Patch Antenna

To enable front-side radiation, the tag integrates 2×2 patch antennas that are shared between the downlink and uplink. To realize such sharing, a near-square shape is adopted for the patch, so that its two dominant excitation modes i.e. TM_{100} and TM_{010} with orthogonal polarizations have the same resonance frequency (∼260 GHz). As Fig. 2-6a indicates, to excite a certain mode (TM_{100} in this case), we can either use a differential feed symmetrically connected to the patch edge along the x-direction (i.e. Feed 1), or a single-ended feed connected to the center of the patch edge along the y-direction (i.e. Feed 2). Therefore, when both feeds are used and the downlink wave aligns with the TM_{100} mode of the antenna, the received power is split into the two feeds for back-scatter (Feed 1) and downlink demodulation (Feed 2), respectively. Accordingly, the THz SSB mixer has a differential input, while the THz square-law detector for the OOK demodulation of downlink has a single-ended input (Fig. 2-6a).

Next, to radiate the uplink signal with orthogonal polarization, the TM_{010} mode of the same antenna is used (Fig. 2-6b) and is excited by a single-ended feed (Feed 3) at the center of the patch edge along the x-direction. Accordingly, the THz SSB mixer provides a single-ended output, as described later in Section 2.5.2. Note that the electrical field distribution of the associated TM_{010} mode has a null at Feed 2, so the leakage of the uplink signal to the THz square-law detector is very small. Similarly, the received downlink signal does not leak into the SSB mixer output either (Fig. 2-



(a)



(b)

Figure 2-6: Schematic of the multi-port patch antenna with excited (a) TM_{100} for downlink and (b) TM_{010} for uplink.

7a). Note that the uplink signal injected at Feed 3 can *couple back* to the SSB mixer through a *common-mode* leakage in Feed 1. Techniques to prevent such leakage are described in Section 2.5.2.

To ensure the reliability of both the downlink demodulation and the back-scattering, the power splitting ratio in Fig. 2-6a is set to about 1:1. The value of the ratio is controlled by the termination impedances at Feed 1 and Feed 2 (i.e. Z_1 and Z_2 in Fig. 2-7a). To determine the optimal values of Z_1 and Z_2, we first derive the desired ratio of $K{=}Z_2/Z_1$. Note that for the TM_{100} resonance mode, the distribution of the electrical field (hence the local voltage with respect to the ground) along the x-direction approximately follows an anti-symmetric sinusoidal pattern (Fig. 2-7a), and can be expressed as [37]:

$$V(x) = V_0 \cdot \sin \frac{\pi x}{2L_{ANT}}, \tag{2.1}$$

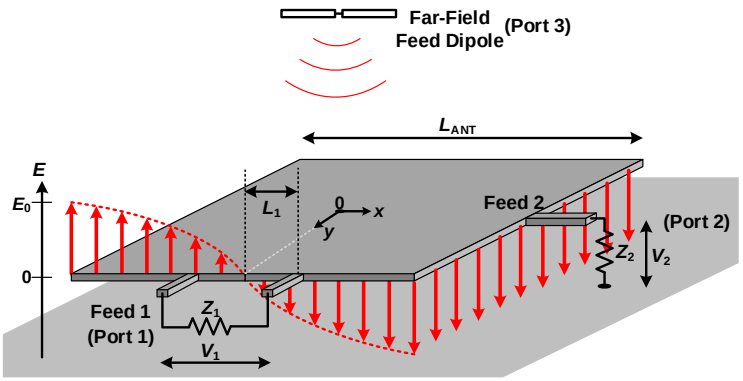
where V_0 is the maximum RMS voltage at the edge of the antenna, and L_{ANT} is the dimension of the antenna. Therefore, the power injected into Z_1 and Z_2, respectively, is:

$$P_1 = \frac{4V_0^2}{Z_1}(\sin \frac{\pi L_1}{2L_{ANT}})^2 \quad \text{and} \quad P_2 = \frac{V_0^2}{Z_2}, \tag{2.2}$$

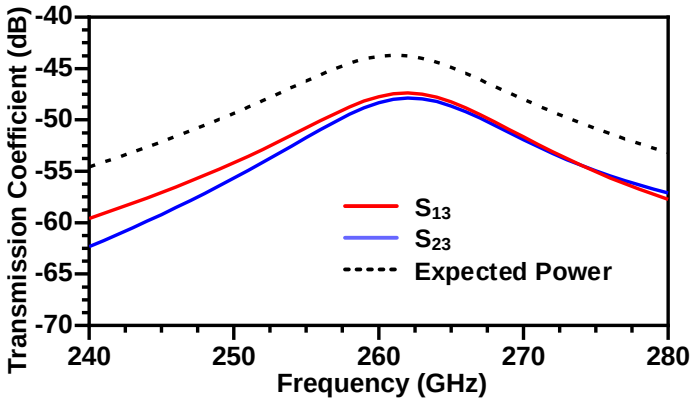
where L_1 is the distance of each Feed 1 wire from the antenna edge center (Fig. 2-7a). For equal power splitting (i.e. $P_1{=}P_2$), the required ratio K is derived:

$$K = \frac{Z_2}{Z_1} = \frac{1}{4(\sin \frac{\pi L_1}{2L_{ANT}})^2}. \tag{2.3}$$

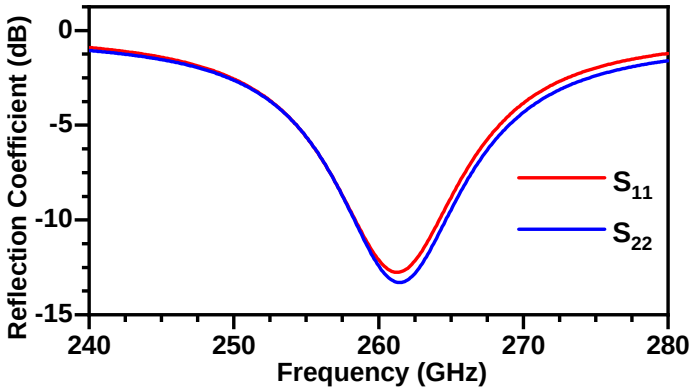
In our design, the value of L_1/L_{ANT}, limited by the circuit floorplan, is about 0.18, which leads to $K{\approx}3$. Next, to further determine Z_1 and Z_2, we note that their optimal values should provide matching between the entire downlink structure and the incident plane wave. This scenario is emulated in a full-wave electromagnetic simulator, HFSS [38], with a far-field half-wave dipole antenna (Port 3 in Fig. 2-7a). The dipole has a gain of 2 dB and is located at 2 cm from the on-chip patch antenna. The absolute values of Z_1 and Z_2 are then swept (while keeping their ratio



(a)



(b)



(c)

Figure 2-7: (a) The electrical-field distribution of the TM_{100} mode in the multi-port antenna. (b) The simulated power transmission coefficients from a far-field feed dipole (2 cm away) to the two ports associated with the downlink, when they are terminated by Z_1=150 Ω and Z_2=450 Ω, respectively. The dotted line shows the expected total received power, which includes the free-space propagation loss and the gains of two antennas. Ideally, it should be 3-dB higher than S_{13} and S_{23} when the power transmissions to Port 1 and 2 are equal and maximized. (c) The simulated reflection coefficients show impedance matching at both ports.

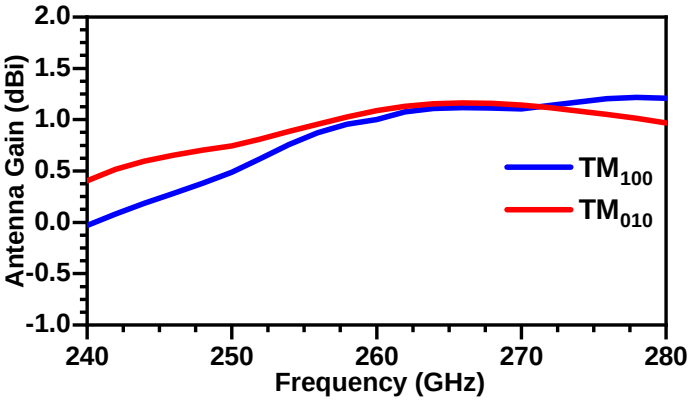
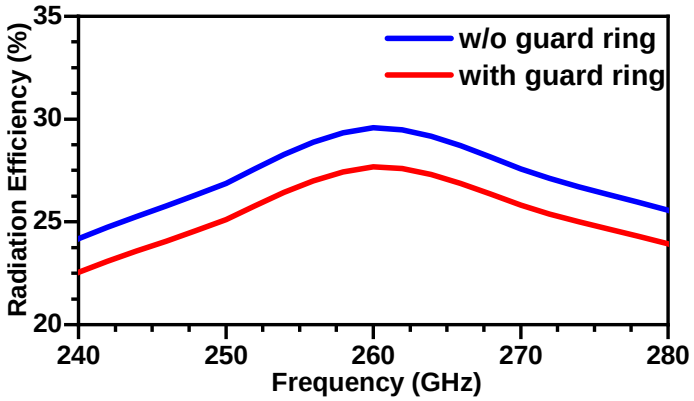


Figure 2-8: Simulated gains for both TM_{100} and TM_{010} modes of the patch antenna.

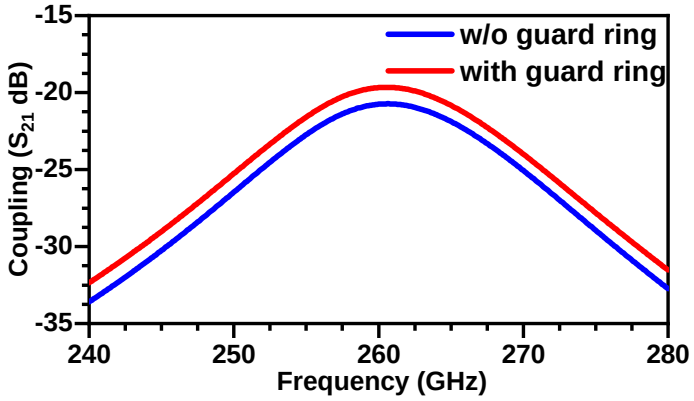
of K=3). When Z_1=150 Ω and Z_2=450 Ω, maximum total power transfer from the feed dipole to the two patch antenna ports (S_{13} and S_{23}) is obtained, meaning that the wave reflection on the antenna is minimum. Fig. 2-7b shows the simulated power transmission co-efficient (including free-space propagation loss) when the above optimal impedance values are applied.

Regarding the implementation of the patch antenna, its radiator uses the top aluminum (Al-pad) layer of the CMOS process and has a size of 271 μm in the x-direction and 235 μm in the y-direction. These dimensions, along with the additional feed ports, lead to the same resonant frequency for both TM_{100} and TM_{010} modes. The patch would have a square shape if only Feed 2 and Feed 3 were present but the differential Feed 1 necessitates a non-square shape. The simulated antenna gains for both the TM_{100} and TM_{010} modes are almost the same as shown in Fig. 2-8.

The patch radiators and the ground planes of the antennas are implemented with a fishnet pattern to allow the transmission of light through them for photovoltaic harvesting. The ground plane of the antenna is made out of the M3 layer. The antenna is also enclosed by a ground wall (M3 to top aluminum layer), which is 20-μm away from the patch on all sides. That reduces the coupling with neighboring electronics and antennas while its effect on the antenna performance is negligible as shown in Fig. 2-9. Using HFSS the peak directivity and radiation efficiency of the antenna in the simulation are 6.7 dBi and 27%, respectively, in both resonant modes.



(a)



(b)

Figure 2-9: (a) Effect of the guard ring on the simulated radiation efficiency of the patch antenna. (b) Simulated coupling (S_{21}) between two antennas with and without guard ring.

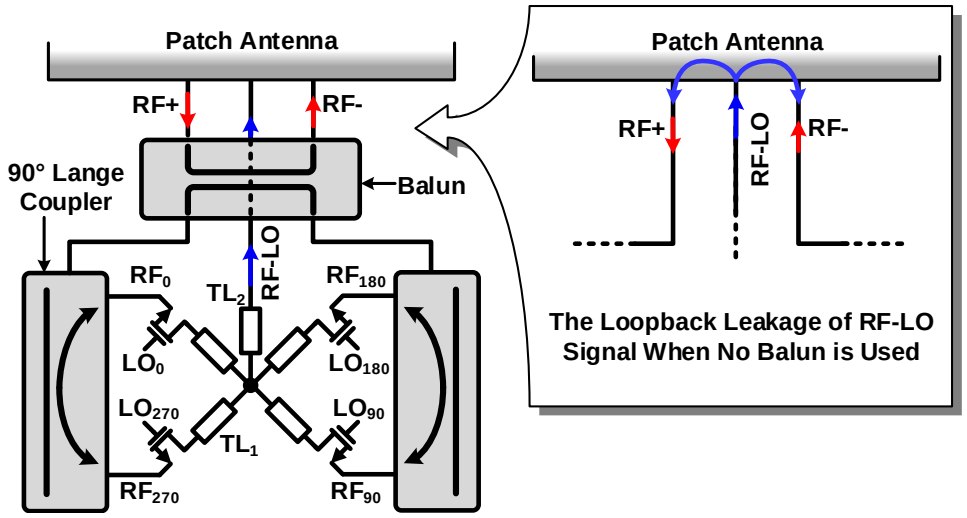


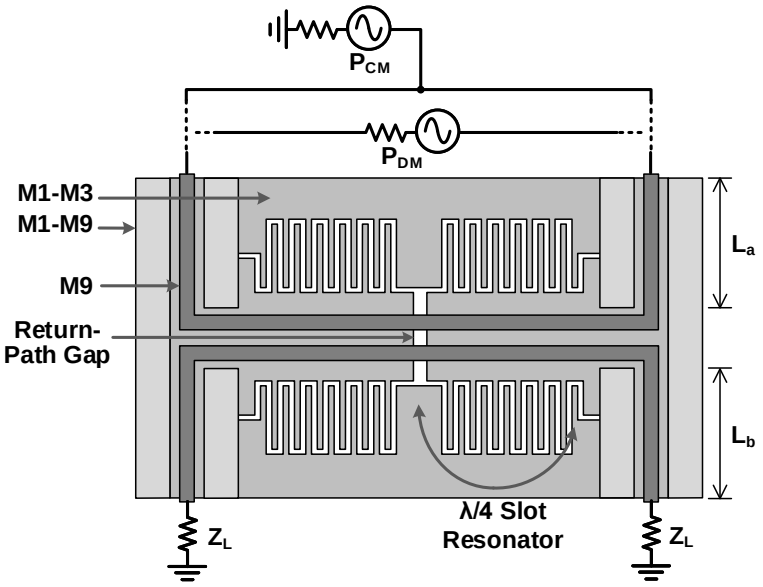
Figure 2-10: Schematic of the back-scattering module consisting of a passive SSB mixer, a balun, and two 90° Lange couplers. The loopback effect with the absence of the input balun is also shown.

2.5.2 THz Frequency-Shifting Back-scatter Module

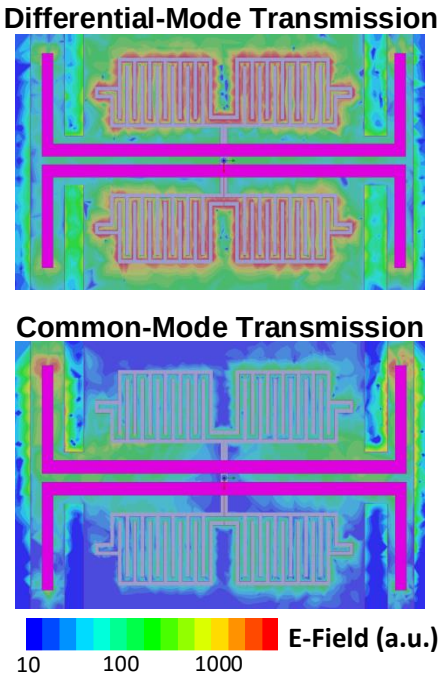
Instead of using a dedicated Tx signal source on a tag [31], which is too power hungry to be practical for THz-IDs, our uplink adopts an energy-efficient back-scatter scheme for the incident wave. As described in Section 2.4, the back-scatter module applies a frequency shifting to the THz signal. Shown in Fig. 2-10, the back-scatter module consists of a passive SSB mixer, two 90° Lange couplers, and a balun. It takes the differential RF signal from the antenna, generates its quadrature phases, and then mixes it with a set of 2-MHz quadrature LO signals. The mixer output is finally injected back to the antenna through Feed 3. Next, details of the components in the back-scatter module are given.

Input Balun

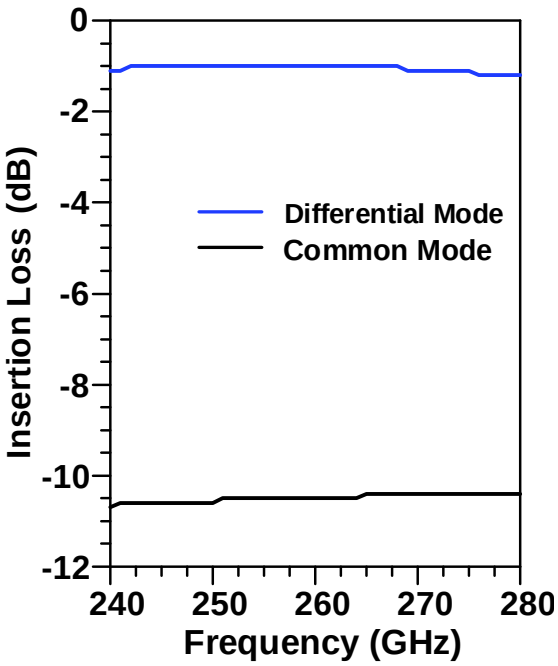
In Fig. 2-6b, the TM_{010} mode excited by the SSB mixer output presents a common-mode electrical field at the two wires of Feed 1. As a result, the mixer output will be fed back to the mixer and undergoes an extra down-shift by f_{LO} in each round trip. Such loopbacks, therefore, cause excessive signal loss and undesired LO harmonic spurs. To avoid it, between Feed 1 of the antenna and the SSB mixer input, a balun



(a)



(b)



(c)

Figure 2-11: 260-GHz balun based on a return-path gap: (a) structure, (b) simulated electrical-field distribution, and (c) simulated insertion loss from the input to one load Z_L.

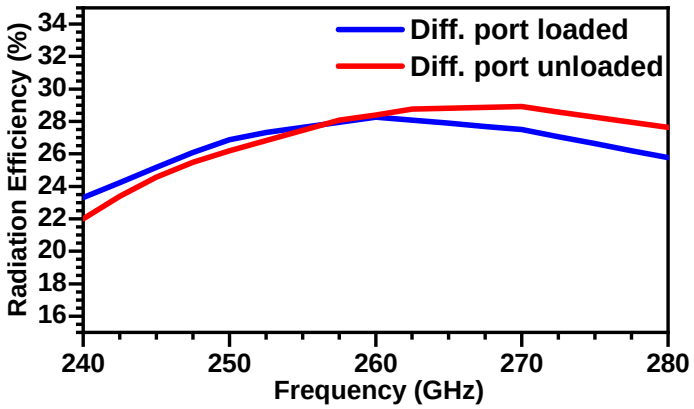


Figure 2-12: Simulated radiation efficiency of the antenna for Feed 3 with and without connecting balun to the differential Feed 1.

is inserted, which only allows the transmission of differential signal from the antenna, and blocks the common-mode leakage from the mixer output. A return-path-gap-based balun introduced in [39] is used, which consists of two microstrip lines coupled via a slot in the ground plane (i.e. return-path gap or RPG, see Fig. 2-11a). The RPG slot, closed by four quarter-wavelength slot resonators in the ground plane, only allows transmission (hence input-output coupling) of quasi-TE-mode wave, which is excited by a differential signal in the input microstrip lines. That is illustrated in the electromagnetic simulation shown in Fig. 2-11b, and we can see that the common-mode signal is effectively rejected. The simulated insertion loss for the differential mode is $\sim$1 dB and the rejection for the common mode is $>$10 dB from 240 to 280 GHz. The balun is implemented using 2-μm-wide M9 microstrip lines and slots in a shunted M1-M3 ground. Note that a wire placed along the central line of the balun connects the SSB mixer output (f_{RF}-f_{LO}) and the antenna (Fig. 2-10); since the balun central line can be treated as the virtual ground for the differential-mode transmission, the above wire does not interfere with the balun operation. The radiation efficiency of the antenna for Feed 3 is not effected by the balun connected to Feed 2 as shown in Fig. 2-12.

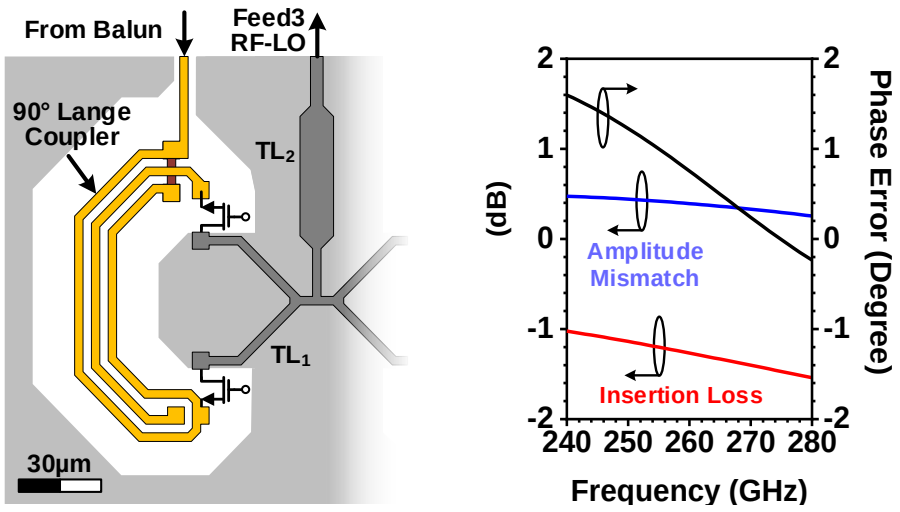


Figure 2-13: (a) The structure of the 260-GHz Lange coupler in the back-scatter module. (b) Simulated insertion loss and output mismatch of the coupler.

Coupler

The Lange coupler that generates the quadrature phases for the input 260-GHz signal is shown in Fig. 2-13a. The electromagnetic simulation results are shown in Fig. 2-13b; at 260 GHz, the simulated insertion loss excluding the ideal 3-dB power splitting factor is 1.2 dB, and the amplitude/phase mismatches at the two output ports are 0.5 dB and 0.5°, respectively. The couplers are implemented using the M9 layer, with 3-μm-wide lines and 3-μm spacing among the lines. The couplers are also enclosed by a ground plane (with a spacing of 15 μm) to provide the signal's return path and to minimize the coupling to surrounding structures.

2.5.3 Passive Single-Sideband (SSB) Mixer

Although a double-sideband (DSB) mixer involves simpler hardware implementation, we note that the generated upper and lower sidebands are applied with opposite phases from the LO; in our tag, therefore, their associated uplink beams would point to different directions in the beam-steering. That lowers the security and causes signal loss and interference. In our design, a SSB mixer based on passive quad switches is adopted to not only suppress the upper-sideband of the output, but also to minimize

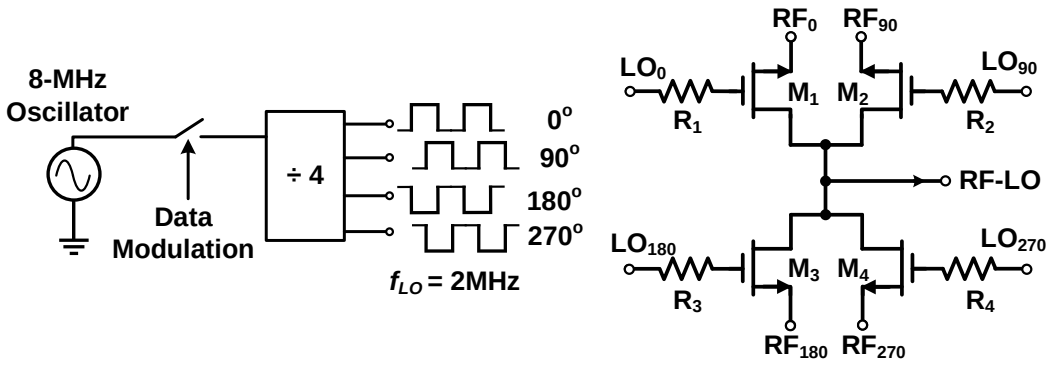


Figure 2-14: Schematic of the 260-GHz passive SSB mixer.

the power consumption. Shown in Fig. 2-14, the 2-MHz quadrature LO signals of the mixer are from an 8-MHz on-chip oscillator cascaded by a divide-by-4 static frequency divider. Although a divide-by-2 operation for a 4-MHz signal also provides the 2-MHz quadrature LO signal, the additional availability of LO phases (e.g., 45°, 135°, 225°, 315° in Fig. 2-14) provided in our divide-by-4 scheme is utilized to demonstrate the beam-steering of the uplink wave. The phases of the RF and LO signals of the MOSFETs are arranged in the way that at the central current-summing node, the lower-sidebands of all branches add up constructively, while the upper-sidebands cancel. MOSFETs in 65-nm bulk CMOS process have poor switching performance at THz; although a wider channel provides smaller ON-resistance, there is also a stronger coupling of THz signal from the channel to the LO wire through the gate-channel capacitance. To block such coupling, a set of 1.5-kΩ resistors ($R_1 \sim R_4$ in Fig. 2-14) are added in series with the transistor gates, which improves the mixer insertion loss from 15.5 dB to 13.5 dB in the simulation. Lastly, the OOK uplink modulation is realized by a data-controlled gating of the LO signals.

Shown in Fig. 2-13a, microstrip TL_1 lines combine the drain nodes of the MOSFETs and TL_2 is used to assist the impedance matching to Feed 3 of the antenna. But TL_2 falls short to provide ideal transformation and the limited space (due to the presence of the balun) hinders the placement of additional matching network components. This impedance mismatch leads to an insertion loss of 2 dB from the mixer to antenna Feed 3.

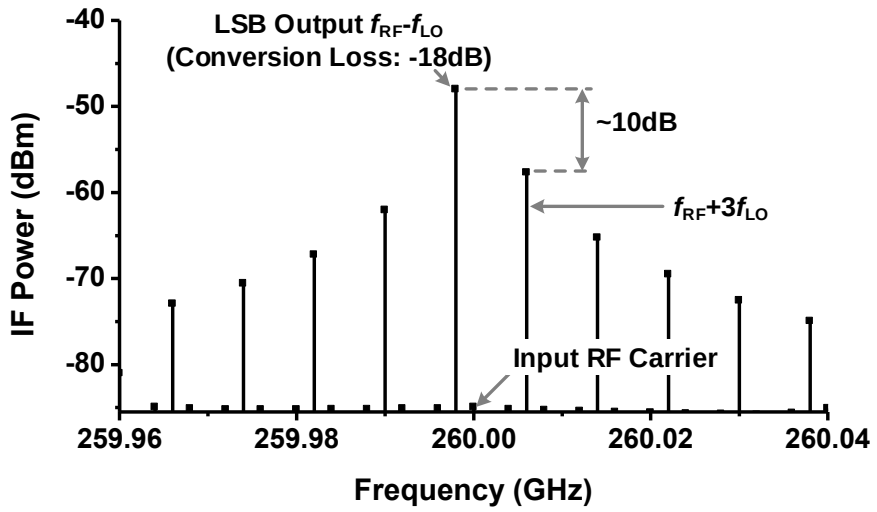


Figure 2-15: Simulated output spectrum of the THz back-scattering module with a -30-dBm RF input (f_{RF}=260 GHz) and quadrature LO signals at f_{LO}=2 MHz.

The simulated differential impedance of the whole back-scattering module is very close to the desired 150 Ω (see Section 2.5.1) without any additional matching network. If necessary, the impedance matching can be fine tuned by controlling the lengths (L_a and L_b, see Fig. 2-11a) of the transmission lines connecting the balun to the antenna and coupler, respectively. The simulated common-mode impedance of the back-scattering module is largely capacitive (4.2-347.4j Ω). The small real impedance ensures that the radiation efficiency for the uplink signal is not affected by the loading at Feed 1.

In Fig. 2-15, we show the eletromagnetic-circuit co-simulation results of the entire back-scattering module. An overall conversion loss of 18 dB (including the 2-dB impedance mismatch loss) is achieved at f_{RF}=260 GHz, at the expense of zero static DC power. The conversion loss should be improved with more advanced CMOS technologies. The module also effectively suppresses the components at $f_{RF}+f_{LO}$ and $f_{RF}\pm 2f_{LO}$. The component at $f_{RF}+3f_{LO}$, due to its constructive summation at the mixer output node, appears at the output spectrum, with a 10-dB rejection ratio. In the future, this may be improved by adopting a polyphase N-path mixer structure. Also note that the phase noise of the back-scattered signal, being the sum of the RF and LO phase noise, is not deteriorated by the ultra-low-power tag LO; because the

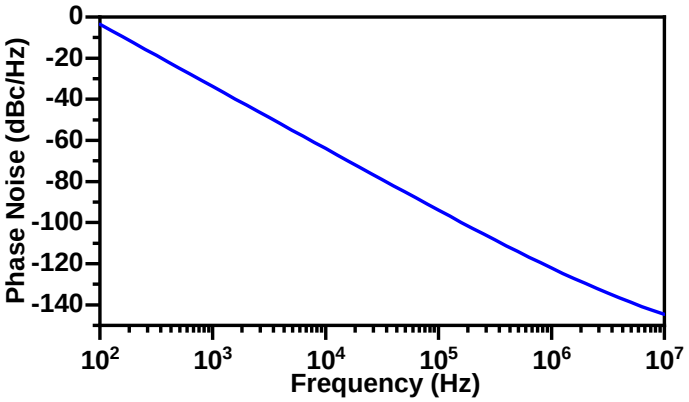


Figure 2-16: Simulated phase noise of the on-chip 8 MHz oscillator.

simulated tag LO phase noise is still smaller than that of the RF signal, due to the large difference between the two signal frequencies (i.e. 2 MHz versus 260 GHz). The simulated phase noise of the on-chip oscillator is ∼20 dB better than the 260 GHz signal as shown in Fig. 2-16.

2.5.4 THz Downlink Circuits

For the demodulation of the 260-GHz OOK downlink signal, a THz square-law detector is used to first rectify the input to baseband, then a low-power amplifier is used to boost the baseband signal to a few hundred mV, so that the subsequent digital circuits can operate reliably (Fig. 2-5).

THz Square-Law Detector

To achieve zero DC power and low flicker noise, our 260-GHz square-law detector is based on a 2.4μm/65nm NMOS device with zero drain bias. Similar to other FET-based THz detectors [40, 41], the optimal responsivity and noise-equivalent power (NEP) occur at a gate bias around the threshold voltage V_{th} of the transistor. Conventional VDD-powered circuits, due to the tag's energy harvesting operation, has large bias voltage fluctuation. Fortunately, in our CMOS process, the threshold voltage (V_{th}≈0.4 V) is close to the light-insensitive, open-circuit voltage of a P-N photodiode (V_{PD}≈0.47 V). Therefore, a simple photovoltaic-biasing circuit shown in Fig. 2-17 is

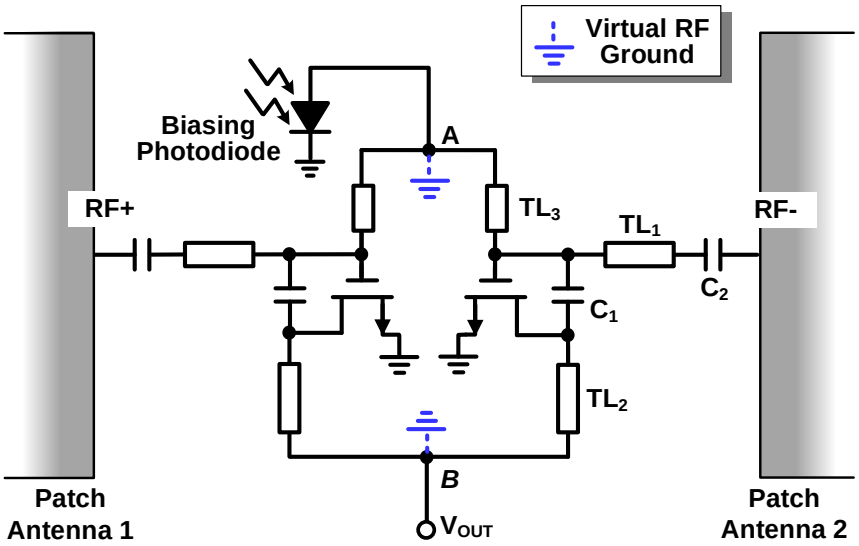
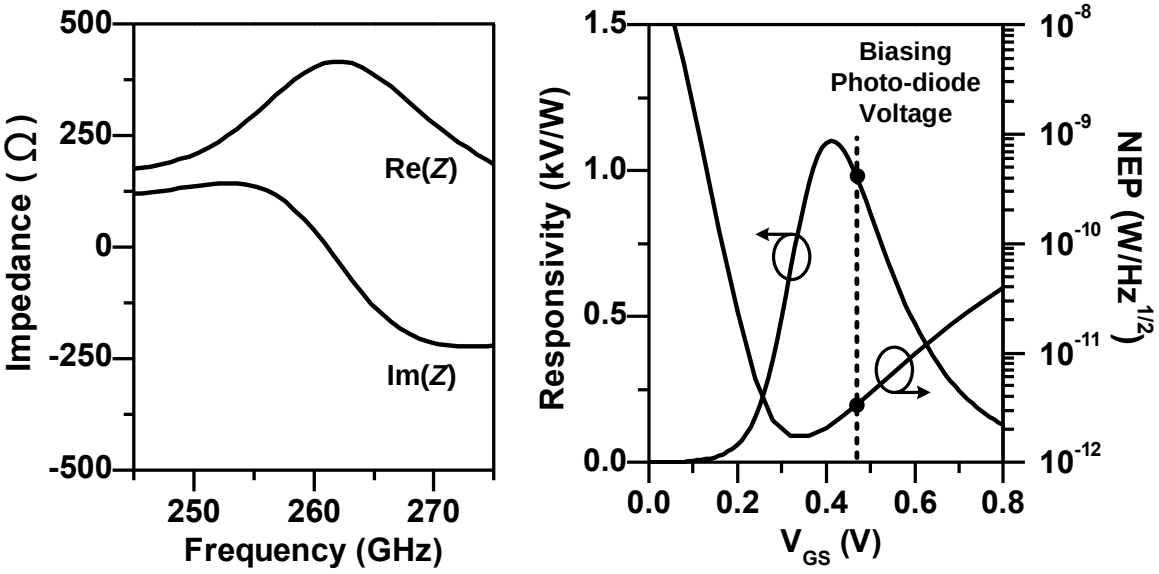


Figure 2-17: Schematic of a photovoltaically-biased THz square-law detector pair.

adopted. Next, we note that any THz-power leakage to the biasing photodiode and detector baseband output should be avoided. To this end, a dual-detector scheme shown in Fig. 2-17 is used, which utilizes the property that the THz downlink signals extracted respectively from the adjacent edges of two patch antennas (see Fig. 2-5) are differential. As a result, in the symmetric circuit topology in Fig. 2-17, virtual RF grounds are formed at Node A and B. Furthermore, TL_2 and TL_3 are quarter-wavelength transmission lines; they transform the virtual ground to high impedances at the drain and gate of the MOSFET and therefore, highly confine the THz wave within the device. It is noteworthy that since the two differential THz inputs carry the identical OOK envelope, the baseband output from the two MOSFETs is in-phase, and is therefore combined and extracted at Node B.

In Fig. 2-17, C_1 ($\sim$50 fF) creates an AC short and therefore facilitates THz self-mixing in the diode-connected MOSFET. C_2 ($\sim$15 fF) provides DC isolation from the uplink back-scatter module, and together with TL_1 (0.35λ) forms a matching network to present an impedance that is derived in Section 2.5.1 for equal power splitting. The insertion loss of the matching network is 1 dB. $\mathrm{TL}_1$$\sim$$\mathrm{TL}_3$ are 75 Ω coplanar-waveguide (CPW) transmission lines implemented using the M9 layer. As shown in Fig. 2-18a, the simulated overall impedance of the detector circuit is close



(a) (b)

Figure 2-18: (a) Simulated impedance of the detector presented to Feed 2 of the antenna. (b) Simulated responsivity and NEP of the detector.

to the desired impedance value of 450 Ω. Lastly, Fig. 2-18b shows that, at the photodiode bias voltage of ∼470 mV, the simulated responsivity and noise equivalent power (NEP) are 1 kV/W and 32 pW/Hz$^{1/2}$, respectively. Note that the NEP is limited by the channel thermal noise of the transistor. The noise voltage from the photodiode, calculated in APPENDIX, is small and does not transfer to the transistor output, given that the transistor is in the triode mode.

Ultra-Low-Power Amplifier

Shown in Fig. 2-19a, the demodulated signal from the detector is injected into a chain of amplifiers through a high-pass filter. The filter, consisting of a 5 pF capacitor and a 5.7 MΩ resistor, has a low cut-off at 5 kHz and provides not only the input bias of the amplifier but also DC isolation from the THz detector. The amplifier consists of three stages and two inverting buffers, and are separated by the same high-pass filters; this way the inevitable amplifier offset due to PVT variations and layout asymmetry is not amplified and saturates the circuits near the amplifier output.

Each amplifier stage consists of an input NMOS differential pair, which is preceded

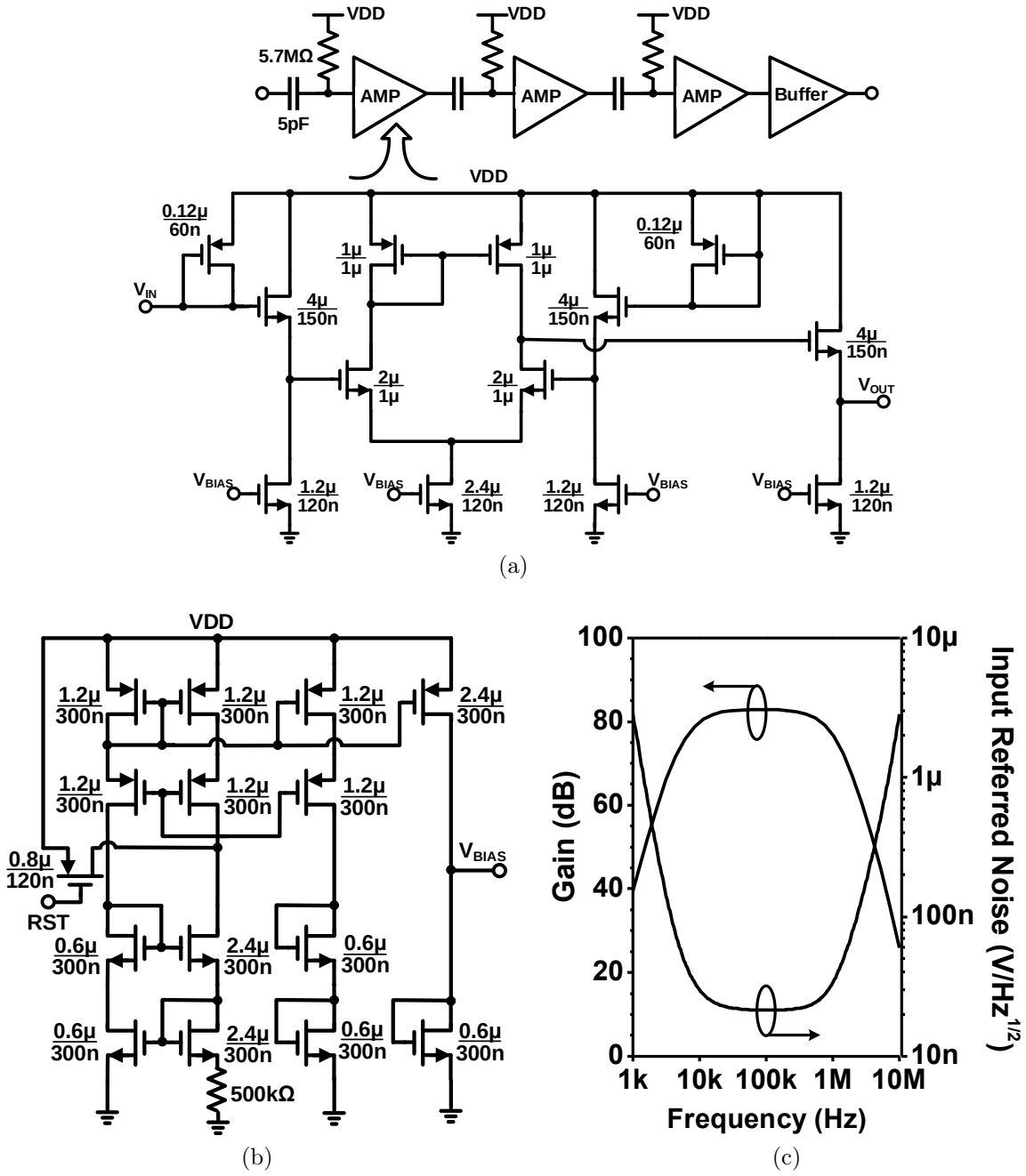


Figure 2-19: The ultra-low-power amplifier in the tag downlink: (a) the schematic of the main amplifier chain, (b) the cascode constant-g_m bias generation circuit, and (c) the simulated voltage gain and input referred noise.

and followed by source-follower stages acting as voltage shifters. To save power, all amplifier stages are biased in the sub-threshold regime. The bias voltage V_{BIAS} in Fig. 2-19a is generated from a cascode constant-g_m circuit (Fig. 2-19b). A reset signal RST from the tag's DC-DC converter is used to ensure that the biasing circuit jumps from an undesired meta-stable state to the normal state when VDD ramps up to $\sim$1 V. As shown in Fig. 2-19c, the simulated gain and the input-referred noise of the amplifier chain are 80 dB and 21 nV/Hz$^{1/2}$, respectively. The whole amplifier-buffer chain, including the biasing circuit, consumes only 1.5 μW.

The high gain is to ensure reliable toggling of subsequent digital circuits. It, however, also amplifies the noise, so when the THz detector is idle, the amplifier output has a low but non-zero probability of falsely toggling the succeeding digital buffer. To mitigate its impact, before taking any downlink message, the on-chip processor always first validates a 16-bit preamble in front of the message. When the THz detector outputs normal data in the downlink mode, the amplifier output level is sufficiently far away from the digital trigger threshold, and the noise impact is suppressed.

2.6 Cryptographic Security Processor

Fig. 2-20 shows the cryptographic processor which implements a 128-bit secure ECC-based private ID scheme [36, 42]. The scheme is a 3-move protocol where the tag chip uses its private key and the reader's public key in order to identify itself to the valid readers. The scheme guarantees that any eavesdropper who does not possess the reader's private key cannot identify which tag participates in the protocol by merely monitoring the wireless link.

An important consideration in the choice of the authentication protocol was the need to co-design it with the cryptographic accelerators to ensure a low footprint. Firstly, we narrowed the choice of authentication protocols, to those that did not require any hash functions to reduce die-area. Secondly, a protocol using x co-ordinate only arithmetic was chosen to enable a compact architecture for the ECC hardware

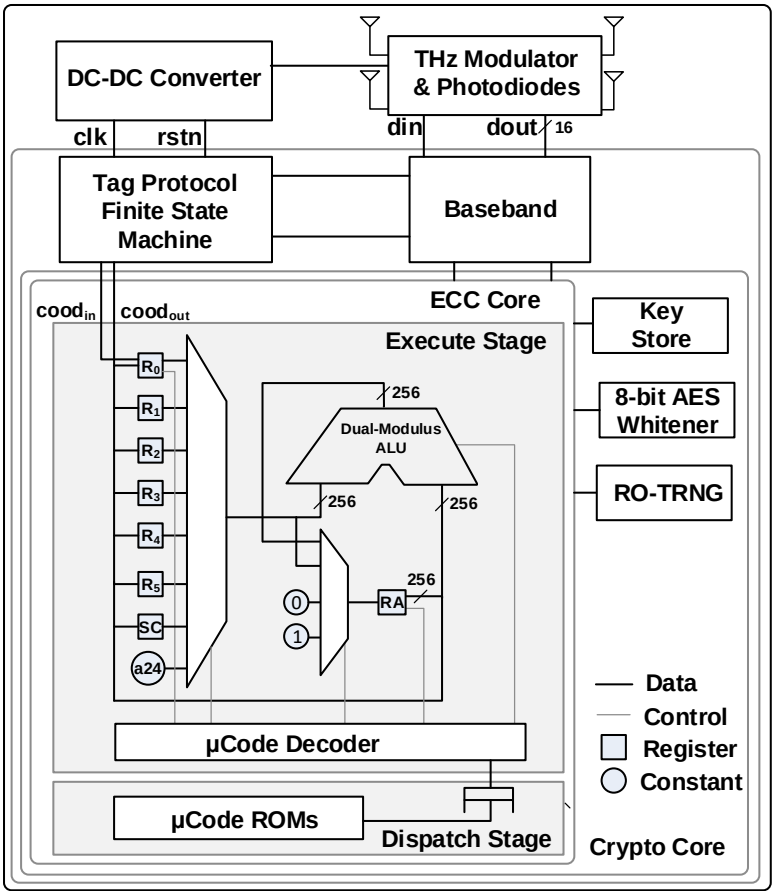


Figure 2-20: Block diagram of the processor on the THz-ID.

accelerator (ECHA). Finally, Curve25519 was chosen since it allowed for an especially efficient x co-ordinate only Montgomery Ladder [43]. Since the authentication protocol requires a secret-scalar multiplication, using the Montgomery Ladder has the added benefit of providing side-channel resistance [44].

The chip has a ring-oscillator-based true-random-number generator (RO-TRNG) with a 3.3kGE[1] 8-bit advanced encryption standard (AES) whitener and a compact 25kGE Curve25519 ECHA to provide the randomness and cryptographic primitives used in the protocol. The ECHA is a very long instruction word (VLIW) machine with a 2.8kGE microcode ROM that implements the ID scheme. Our chosen authentication protocol needs to support arithmetic over both the base field as well as the scalar field. A dual-modulus ALU with a 256-cycle multiplier was chosen to allow sharing the entire datapath between both moduli. As explained above, the Elliptic curve scalar multiplication (ECSM) is implemented using a constant time 650k-cycle projective coordinate Montgomery ladder that is secure against simple power analysis. Register savings in the ECHA design and optimized ECSM microcode results in 22% lower area and 18% lower cycle count compared to [45]. Storing the entire ECSM state in registers allows for low voltage operation down to 0.85V and improves the energy efficiency of the core to 14.4μJ/ECSM.

Fig. 2-21 shows the flow of the direction optimization and the authentication protocol between a THz secure tag and the THz tag reader. When powered using light, the tag wakes up and signals the same to the reader via a beacon. The beam direction is optimized by adjusting two antenna parameters, azimuth angle (ϕ) and elevation angle (θ), to maximize the link budget for data transmission. To this end, the whole space is divided into 25 possible angular positions: five in each azimuth and elevation directions with a step size of 45° from 0° to 180°. The tag wakes up with ϕ=0° and θ=90° by default, and then starts scanning. It takes ∼20 ms (limited by uplink data rate of 2 kbps) to complete the exchange of one beam direction message between the reader and tag. The total time for the beam search is therefore ∼500 ms.

[1]kGE represents a technology normalized area metric equivalent to the area of a thousand minimum-sized NAND gates

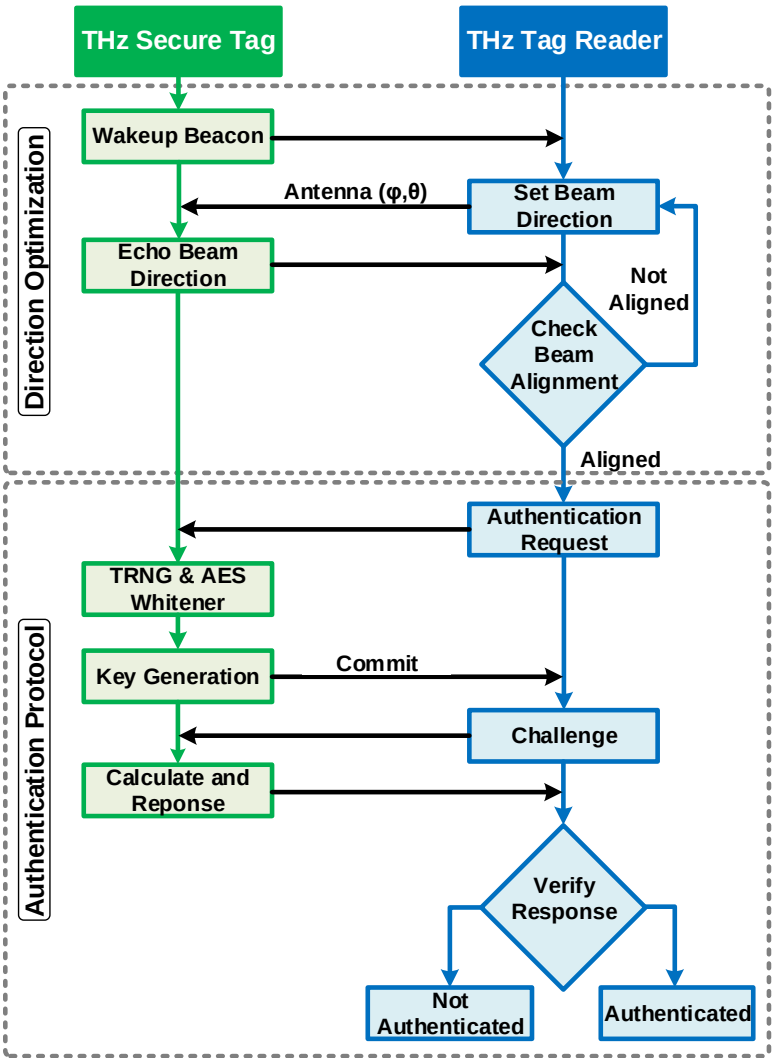


Figure 2-21: The security protocol between the THz secure tag and the tag reader.

All THz tags are initialized with a unique private and public key pair (t, T=tP) and the reader has the tag's public key (T) registered in its database. The reader also has a private and public key pair (y, Y=yP) and the reader's public key Y is known to all tags. If the reader requests authentication of the THz tag, the tag commits a fresh random value (R_1=r_1P) where the randomness (r_1) is generated using the RO-TRNG and the 8-bit AES whitener. The reader responds to the tag's commit message with a random challenge ($R_2 = r_2P$) that is utilized by the tag to compute a Diffie-Hellman share (r_1r_2P). The tag then applies a one-way function to this share and calculates its response. This response is then verified on the reader side through a similar computation to authenticate the tag.

2.7 Integrated Photo-voltaic Powering

The antenna array, when incorporated on the tag chip, occupies most of the die area. In this section, we describe how the silicon under the antennas, along with an integrated DC-DC converter, are exploited to perform photo-voltaic powering for the tag.

2.7.1 Photodiodes

The CMOS technology used for the chip provides a Deep N-well structure, normally for increased isolation between analog and digital circuits. This feature is utilized in the THz-ID tag, where silicon photodiodes are built based on a vertical stack of N+, P-well, Deep N-well, and P-substrate, as shown in Fig. 2-22. As a result, three P-N junctions are formed, which maximize the absorption of incident light. For chip compactness, an array of shunted photodiodes is placed both beside and underneath the antennas. Correspondingly, the patch radiators and the ground planes of the antennas are implemented with a fishnet pattern (Fig. 2-22). A simulation tool based on a finite-difference time-domain (FDTD) method, Lumerical [46], is used to examine the hole size of the fishnet pattern. The simulation results in Fig. 2-23a assume that 25% area of the antenna are holes to allow light transmission (refereed as fill factor

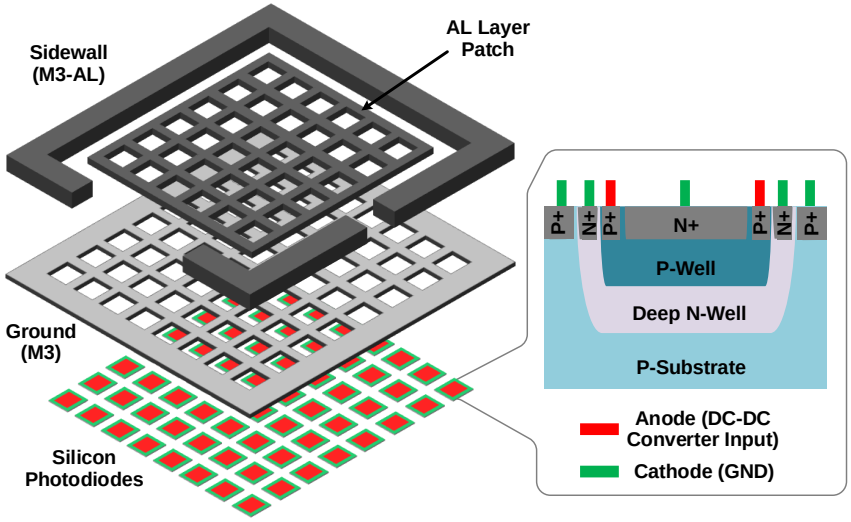
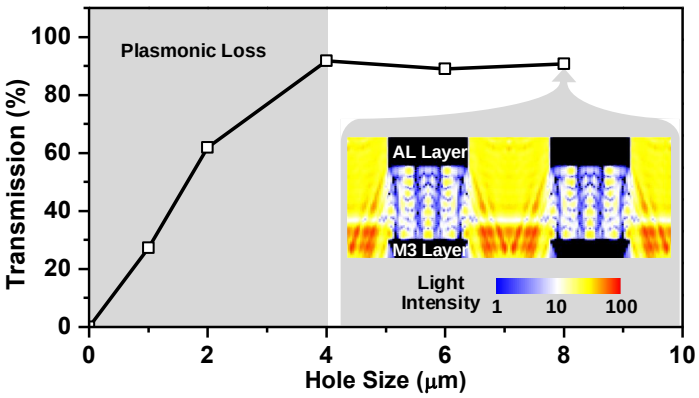


Figure 2-22: Photodiodes placed below patch antenna with fishnet pattern.

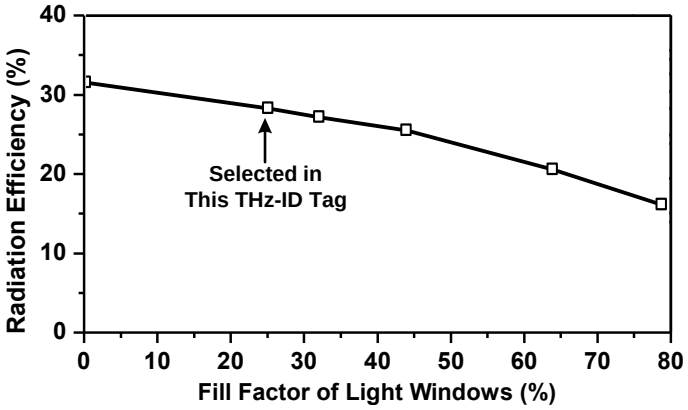
of holes henceforth), and show that the through-hole light transmission for hole size smaller than 4 μm undergoes significant plasmonic and scattering loss. On the other hand, the hole size should remain a small fraction of the THz wavelength, so that the THz-field distribution over the antenna is not affected. As a result, hole size of 8 μm, which leads to a through-hole light transmission rate of 92% is selected. For a larger effective illumination area, the fill factor of the holes should increase. That, however, decreases the equivalent conductivity of the antenna metal layers, and lowers the radiation efficiency, as is shown in the HFSS simulation in Fig. 2-23b. In the tag chip, a fill factor of 25% is used, which slightly degrades the antenna efficiency from 31% to 27%.

2.7.2 DC-DC Converter

This component is needed to convert the loaded photodiode output voltage at about 0.3 V to the chip supply at 1 V. It consists of two converters (start-up and main converters) that are connected between V_{IN} and $V_{OUT,I}$ in parallel, switching clock generators, and other small blocks for control (Fig. 2-24). When the converter is powered by the photodiode from the cold state, the start-up converter (Fig. 2-25a)



(a)



(b)

Figure 2-23: (a) FDTD-simulated light (λ=700 nm) transmission through different hole size. The cross-sectional view of intensity distribution for the hole size of 8 μm is also shown. (b) Simulated antenna radiation efficiency with different hole opening fill factor while keeping 8-μm hole size.

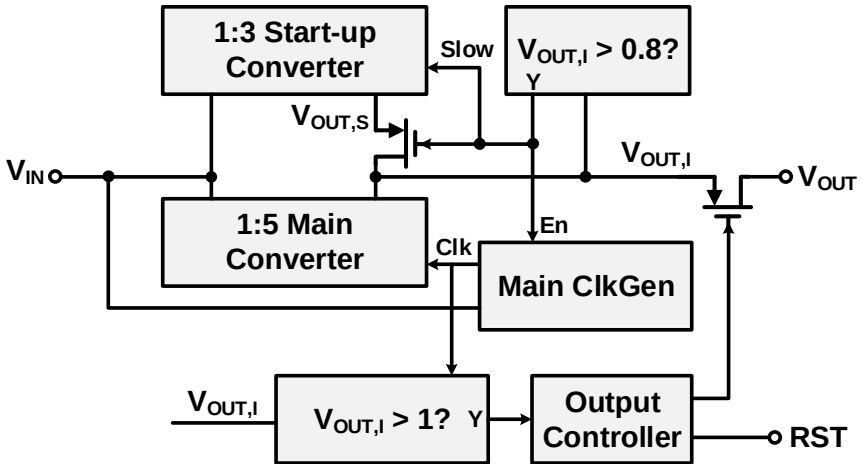
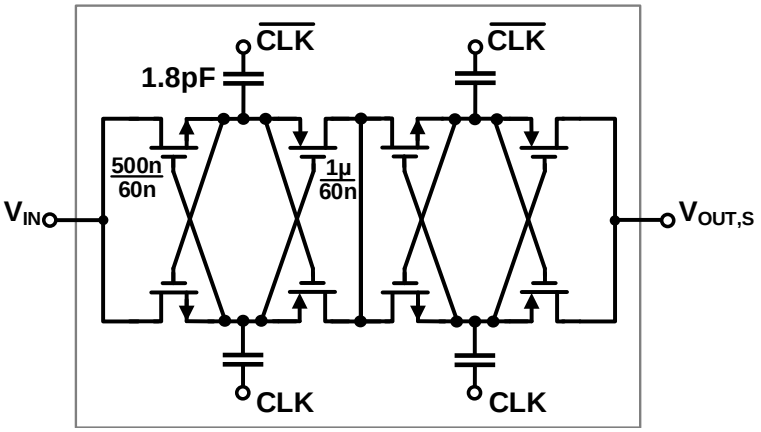


Figure 2-24: Block diagram of the on-chip DC-DC converter.

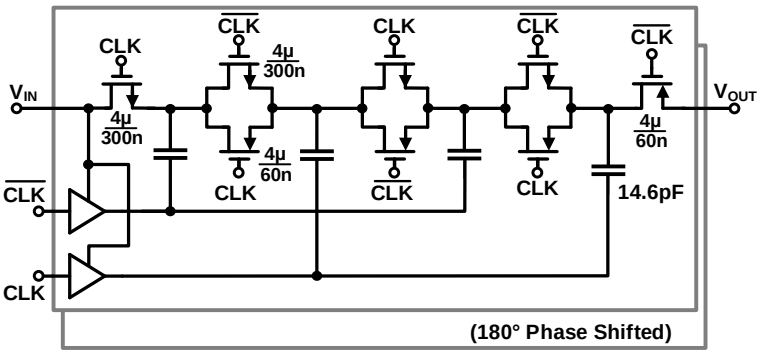
is first turned on and generates 3x up-converted voltage at $V_{OUT,I}$. When $V_{OUT,I}$ exceeds 0.8 V, it triggers the main converter to generate the 1 V output. If the main converter raises $V_{OUT,I}$ over 1 V, the output controller is triggered and turns on the output switch that connects $V_{OUT.I}$ and V_{OUT}, starting power supply to load circuits. The output controller also provides a reset signal (RST in Fig. 2-24) to load circuits so as to initialize them properly during start-up. RST is being asserted during the whole start-up process, and is de-asserted after the output switch is on and V_{OUT} is stabilized at 1 V.

For cold start, the start-up converter always operates whenever photodiode power is available, but after triggering the main converter, its switching frequency is minimized for minimum power waste (Signal *Slow* in Fig. 2-24). According to post-layout simulation results, the switching frequency changes from 8 MHz to 16 kHz (around 500× frequency reduction) and the waste from switching loss is also proportionally reduced.

The main converter (Fig. 2-25b) is optimized for the power conversion of the peak system power, which can be estimated during the design time by simulation. It has a higher conversion ratio of 1:5 to provide a high enough voltage and current to the load. For efficient power conversion during operation, it uses transmission gate switches instead of cross-coupled ones for better conductance, and most of the available capacitors for the converters are allotted to the main converter. For stable



(a)



(b)

Figure 2-25: Schematics of (a) DC-DC converter startup circuit and (b) main DC-DC converter.

and efficient power output, a feedback loop controls the switching frequency of the main converter, so that the photodiode output voltage V_{OUT} stays at the maximum power point under the light intensity that is capable of providing the peak system power.

After the main converter's operation is stabilized, V_{OUT} output switch is turned ON to connect the converter's V_{OUT} to the supply voltage of other blocks. For regulating the output voltage at 1 V, another control loop is attached at V_{OUT} for excess output power from the converter to bypass the load. Design optimization specialized for the tag enables the main converter to achieve a simulated conversion efficiency of 60% during peak power conversion, only using a tiny space (0.096 mm^2) between two patch antennas.

2.8 Experimental Results

The tag chip is fabricated using a TSMC 65-nm bulk CMOS process. The micrograph of the chip is shown in Fig. 2-26. The chip has an area of 1.3×1.2 mm^2. The two rows of pads, which can be cut, are for debugging purposes. In our testing, the chip is mounted and wire-bonded on a PCB.

2.8.1 Measurement Setup

First, a custom-designed THz-ID reader is constructed, as shown in Fig. 2-27a. It communicates with the chip at a distance of 5 cm using two WR-3.4 horn antennas. The antennas are placed in a way that their *E*-planes are orthogonal to each other, in order to match the cross-polarizations of the THz-ID antennas (Fig. 2-6). For the reader-to-tag downlink, an amplifier-multiplier chain (AMC) from Virginia Diodes Inc. (VDI) is used, which converts a 10.9414-GHz input signal to a 20-dBm output at 262.5936 GHz. The input of the VDI AMC is OOK modulated by the 100-kbps data generated from a FPGA board (XEM 7001). According to the Friis formula [47], the power impinging on the THz-ID chip is about -5 dBm.

For the tag-to-reader uplink, a VDI spectrum analyzer extender (SAX) mixes

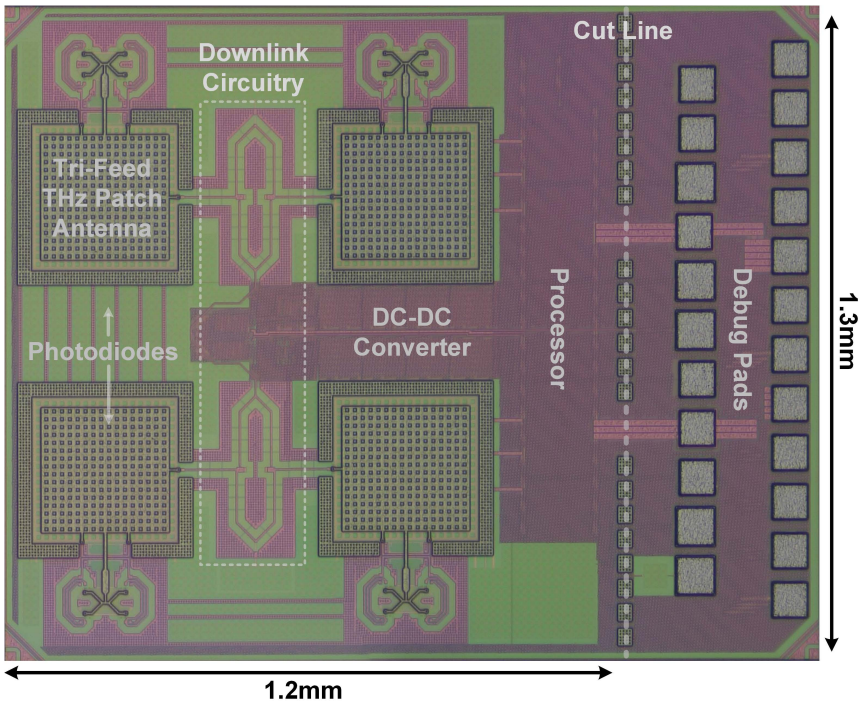
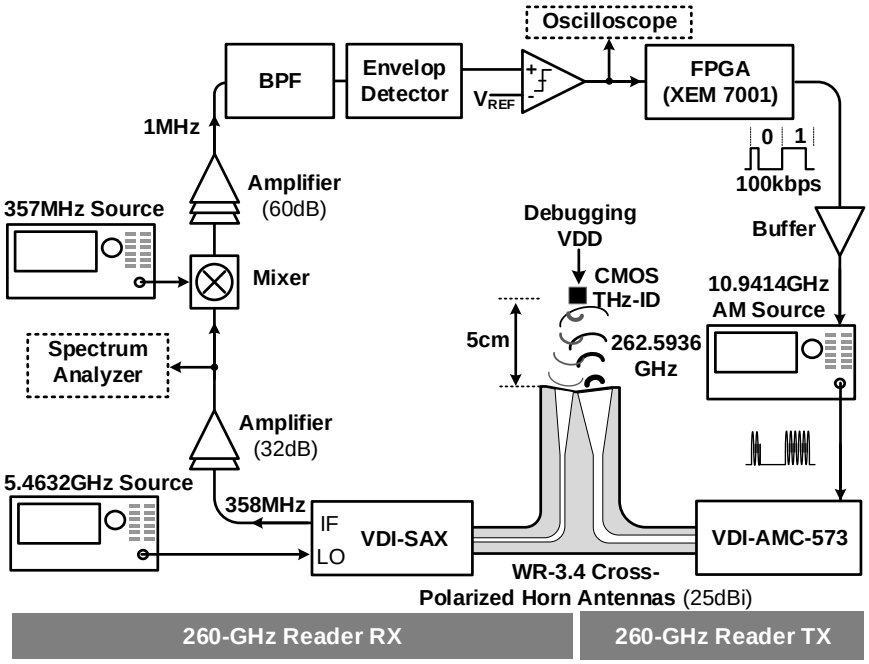
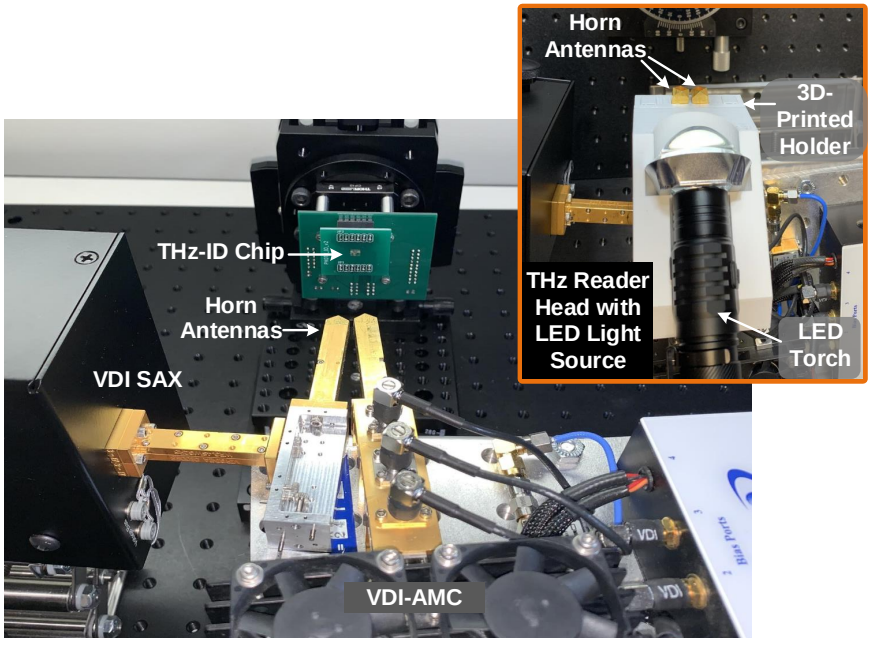


Figure 2-26: Chip micrograph of THz-ID.

the tag's back-scattered signal with the 48^{th} harmonic of its 5.4632-GHz LO, and down-converts to 358 MHz. The signal is then amplified by 32 dB and observed on a spectrum analyzer. To close the communication loop, the signal is also further down-converted to 1 MHz, amplified by 60 dB and bandpass filtered. Finally, an envelop detector cascaded by a comparator recovers the 2-kbps data and feeds it to the FPGA (Fig. 2-27a). Fig. 2-27b shows the photograph of the setup. The THz-ID reader head also includes an illumination source, which consists of a CREE XP-L-V6 LED and a lens that converges the light to a $\sim$1 cm^2 spot on the PCB. The chip PCB is mounted on a rotational stage, which is used for the beam-steering measurement. In the uplink and downlink modes, the tag consumes 13 μW of power; which includes 4 μW of static leakage power of the digital circuits. In the most power-hungry security mode, when the cryptographic processor is running RO-TRNG and AES, the power consumption rises to 21 μW.



(a)



(b)

Figure 2-27: (a) Diagram of the testing setup. Note that when light powering is used, the debugging VDD is disconnected. (b) Photos of the testing up with and without a LED torch for photovoltaic powering of the CMOS chip. The power electronics inside the LED torch, which generates large switching noise, is by-passed in the setup.

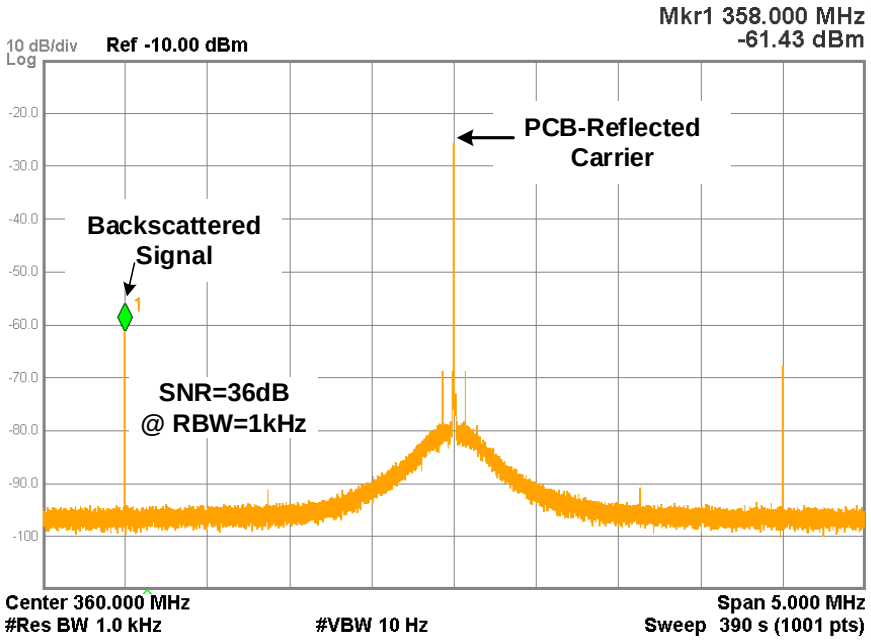


Figure 2-28: Measured spectrum of the back-scattered signal.

2.8.2 Characterization of the Circuits

Back-scatter Module

First, to characterize the 260-GHz back-scatter module in a basic continuous-wave mode, the chip is externally powered and clocked (at f_{LO}=2 MHz) via the debugging pads. With the incident wave generated by the VDI AMC, a down-converted spectrum shown in Fig. 2-28 is obtained from the VDI SAX. The tone at 358 MHz is the expected signal back-scattered by the THz-ID. It has a *SNR* of 36 dB at 1-kHz bandwidth, indicating the feasibility of an uplink with the designed 2-kbps data rate. The tone at 362 MHz is the upper-sideband image due to the limited image rejection (∼10 dB) of the SSB mixer in the tag. The central tone at 360 MHz is the reader-generated 262.5-GHz signal directly reflected from the chip and its surroundings. Note that although this signal is already attenuated by ∼25 dB due to the cross-polarization of the reader antennas, it is still >30 dB higher than the tag-back-scattered signal in Fig. 2-28. That in turn justifies our back-scatter scheme using cross-polarization and frequency shifting. The scheme ensures that the phase noise of the directly-reflected signal is below the reader's thermal noise floor, hence does

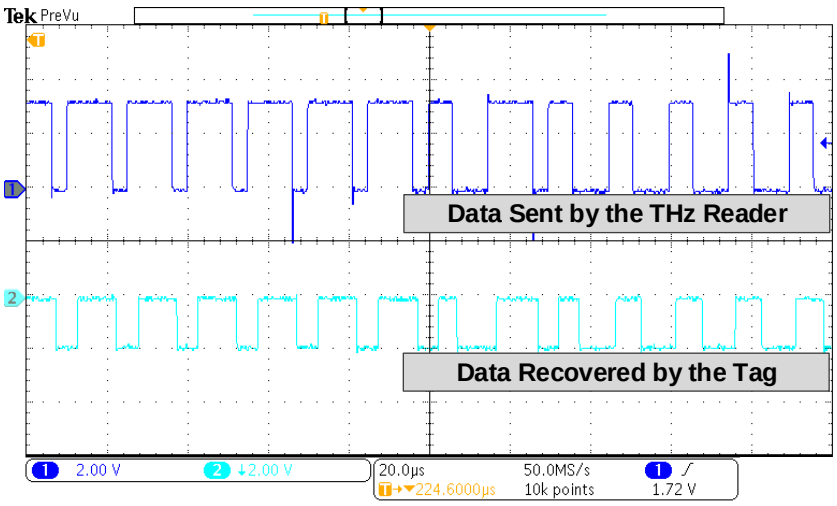


Figure 2-29: Measured downlink waveform from the tag.

not degrade the uplink *SNR*. The scheme also avoids the saturation of the reader's baseband amplifier caused by the undesired reflected tone with large power.

Downlink circuits

With OOK modulation to the VDI AMC, the tag downlink output is measured via a debugging pad. Pulse-width modulation is adopted for the encoding of the system, where duty cycle <45% represents bit 0 and >55% represents bit 1. In our measurement setup, the reader uses 40% duty cycle for bit 0 and 75% for bit 1. The results in Fig. 2-29 indicate that the tag downlink correctly recovers the original data created by the FPGA in the THz reader (Fig. 2-27a). To achieve the gate bias of the downlink MOSFET detector, ambient lighting is found to be sufficient in the testing.

Tag's beam-steering

Next, we test the beam-steering capability of the THz-ID chip. Note that it is different from conventional beam-steering of phased arrays, due to the unique back-scattering operation of the chip, and the co-location of the reader's transmitter and receiver. Shown in Fig. 2-30a, the goal of the beam-steering of this tag is to ensure that when the chip does not face the reader perpendicularly, its back-scattered wave can still be re-directed towards the reader. Fig. 2-30a indicates that, with a chip tilting angle of

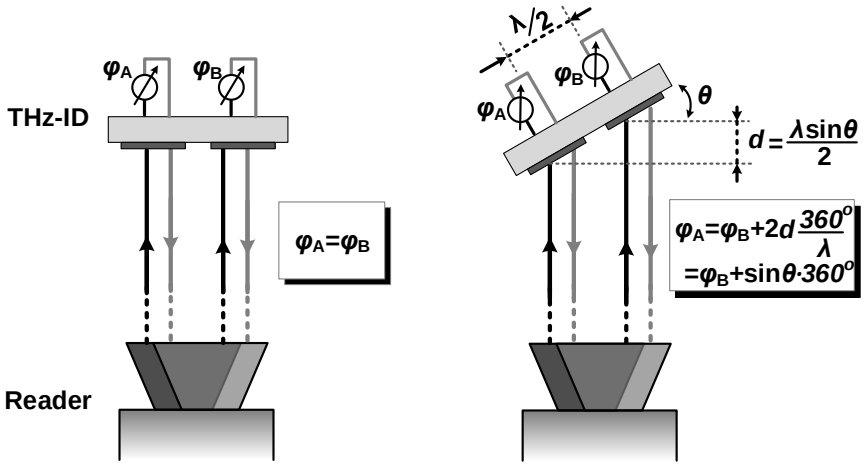
θ and on-chip antenna spacing of $\lambda/2$, the following phase gradient (in degree) should be applied in order to compensate for the total propagation-path difference related to the waves handled by the two patch antennas:

$$\varphi_A - \varphi_B = 2 \cdot (\frac{\lambda}{2} \sin\theta) \cdot \frac{360^\circ}{\lambda} = (\sin\theta) \cdot 360^\circ \tag{2.4}$$

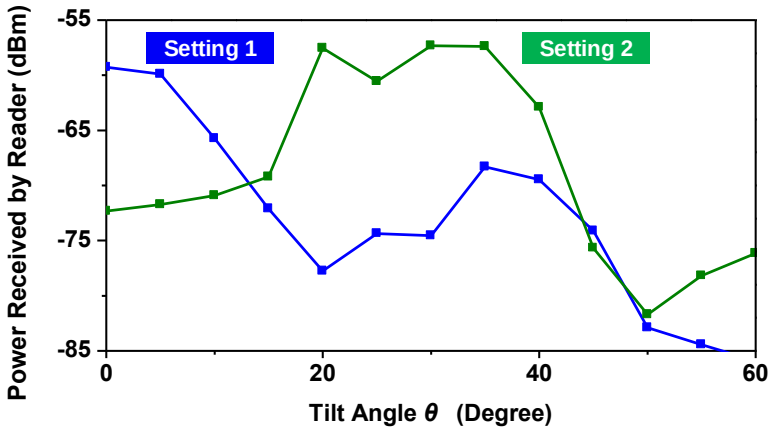
This is verified in our experiment, where the LO phase of each THz SSB mixer is digitally controlled by the on-chip processor. Fig. 2-30b shows the back-scatter-wave power, which is received by the reader in the measurement, at varying chip tilting angles θ. Two tag phase-gradient settings requested by the reader, φ_A=φ_B and φ_A-φ_B=180°, are tested. The measured peak responses of the reader occur at θ=0° and θ=30°, respectively, which agrees well with (2.4). This also shows that the maximum beam-steering angle (in both azimuth and elevation directions) is ±30°. It should be noted here that, when an antenna is tilted, the effective aperture decreases by a factor of $\cos\theta$. At θ=30°, ∼1.2 dB two-way power loss should occur. However, in the measurements, we received almost the same peak power in both settings. This can be attributed to either a better alignment in Setting 2 or a measurement error.

Protocol and Energy-Harvesting

We also verified the protocol and the cryptographic function with external power and the tag internal clock (Fig. 2-31a). When the reader receives the tag's beacon message, the FPGA starts a feedback loop to request a change of uplink beam angle until the *SNR* is maximized. The measured waveforms associated with this operation are shown in Fig. 2-31b. Then the reader sends a trigger to the chip to start the authentication process described in Section 2.6. Fig. 2-31c shows the measured waveforms of the challenge-response protocol that the tag takes towards the end of the authentication process, in order to identify itself to the valid reader. In Fig. 2-31b, when the THz reader is transmitting data, tag's downlink circuit recovers the exact same data and during idle time random output pulses are observed, as explained in Section 2.5.4. Due to the preamble validation in the processor, those random pulses are rejected.

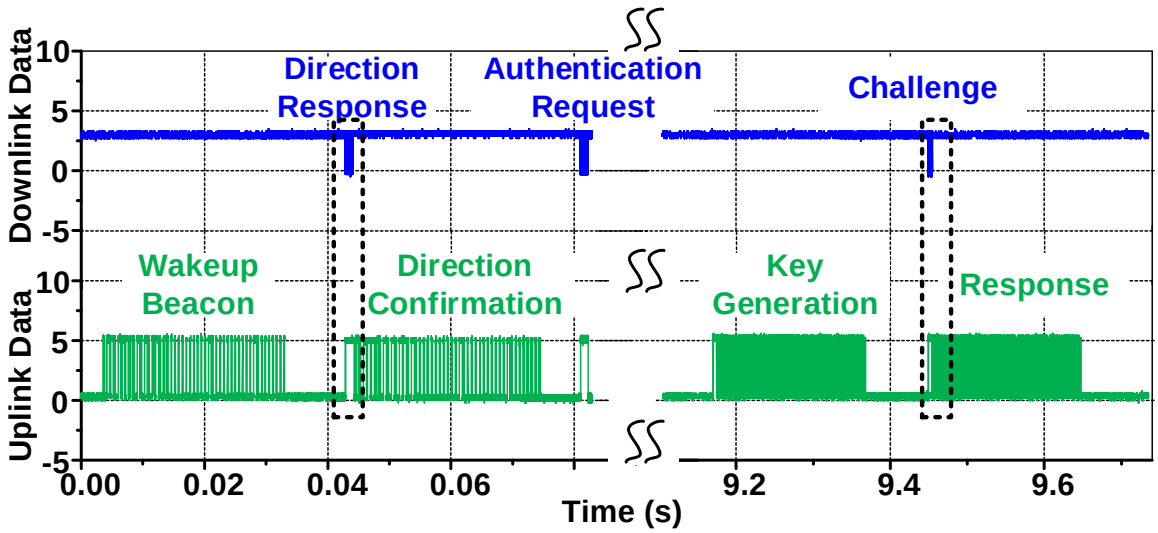


(a)

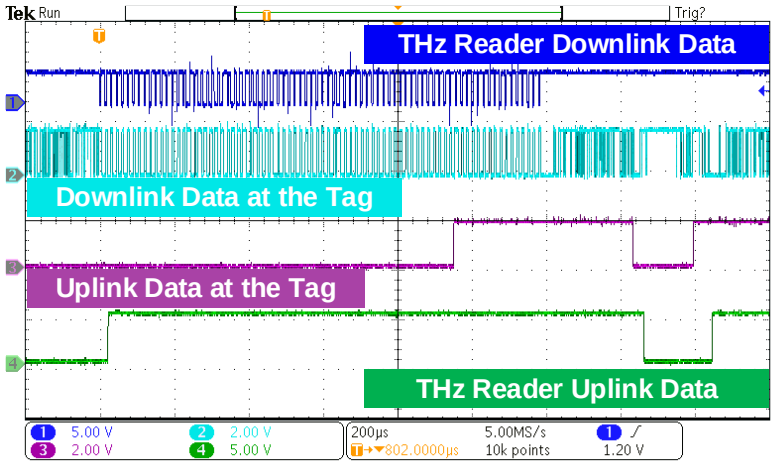


(b)

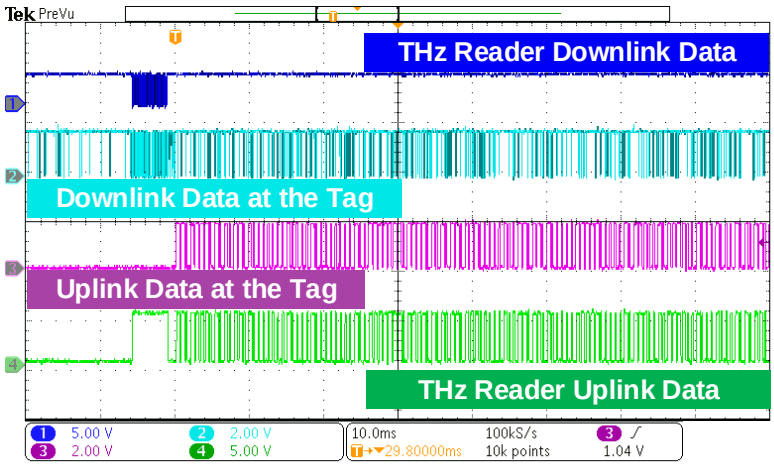
Figure 2-30: (a) Phase-shifting (φ_A-φ_B) conditions in the tag to ensure that the back-scattered wave points to the reader when the tag is tilted by θ. (b) Measured back-scattered-wave power, which is received by the reader, at different chip tilting angles θ. Here, two digital settings of φ_A-φ_B are applied.



(a)



(b)



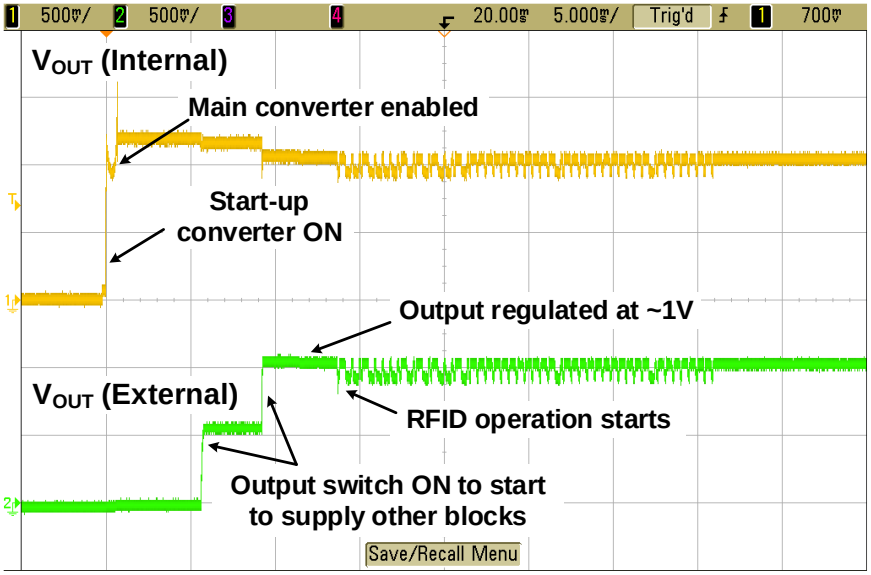
(c)

Figure 2-31: (a) Measured downlink and uplink data in the protocol. Zoom-in views of dotted regions representing the phases of (b) direction response and confirmation, and (c) challenge and response messages.

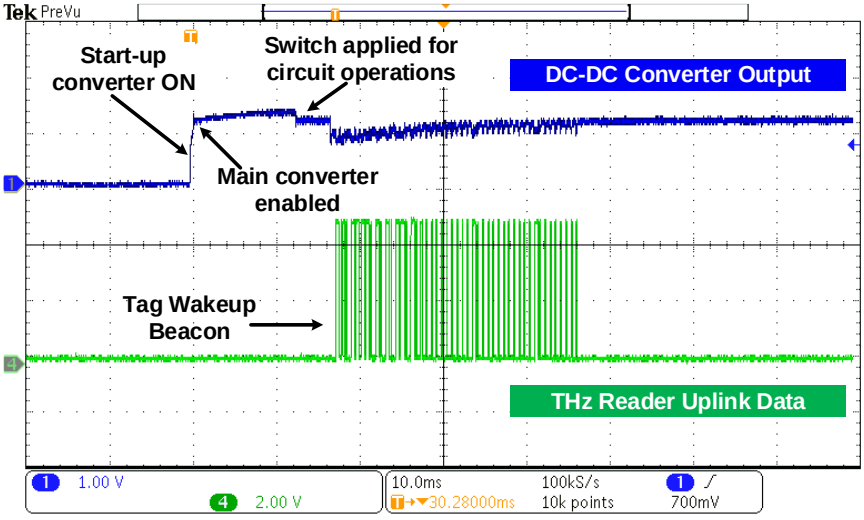
Lastly, with external LED illumination and photodiode powering, the time-domain behavior of the DC-DC converter, measured via the tag's power supply pads, is shown in Fig. 2-32a. The first waveform presents the operations of the DC-DC converter, where the first peak shows the operation of the start-up converter, and the second peak shows that the main converter is activated once the internal voltage of the circuit rises to 0.8 V. Subsequently, the output switch loads the main converter output V_{OUT} (external) with other circuit blocks of the tag, which is shown by the second waveform. The high-frequency fluctuations on V_{OUT} lines after the output voltage reaches ~ 1 V indicate that the on-chip processor is activated. In Fig. 2-32b, the chip is entirely power-autonomous and interrogated by the THz reader. It can be seen that, when the converter startup is completed, the on-chip processor sends a tag-wakeup beacon signal through its 260-GHz back-scatter uplink, and the signal is successfully received and recovered by our reader. Since the downlink amplifier consists of transistors operating in the sub-threshold regime, the large photoelectric effect causes bias drift of the amplifier and excessive noise, which prevents the completion of the entire security protocol in the test. The static current of the processor also increases with the illumination. In future development iterations, we should be able to optically power the complete protocol by enclosing the downlink and processor circuitry with a cover formed by the Al-pad layer and sidewalls formed by the M1-to-Al stack.

2.9 Comparison with the State-of-Art

A comparison of our work with the prior state-of-the-art is given in TABLE 2.1. Our presented tag is built entirely on a low-cost CMOS chip and is around 3× smaller than the smallest package-less, far-field chip reported previously [31]. It also offers multi-antenna beam-steering functionality for the first time in RFIDs. It uses pulse-width modulation (PWM) and amplitude shift keying (ASK) with a 100% modulation index. The uplink and downlink data rates are 2kbps and 100kbps, respectively, and have been demonstrated at a distance of 5cm. The tag employs a security processor with a peak power consumption of 21μW. Compared to [32], the asymmetric public-



(a)



(b)

Figure 2-32: (a) Measured startup behavior of the DC-DC converter. (b) Measured startup behavior of THz-ID with optical powering.

key cryptography provides higher-level security and makes the THz-ID tag suitable for privacy-sensitive applications. TABLE 2.2 compares the proposed ECC hardware accelerator with prior work implementing prime-field ECC at a 128-bit security level. The proposed design consumes the least energy per ECSM and occupies a minimum normalized area.

Table 2.1: Summary of the THz-ID Performance and Comparison with Other State-of-the-Art RFIDs in CMOS

References	CMOS Process	Carrier Freq. (GHz)	Modulation	Data Rate	Peak Power	Security	Range	Beam-Steering	Area (mm^2)
This Work	65 nm	260	PWM 100% ASK	DL: 100kbps UL: 2kbps	21μW	Yes (Elliptic Curve)	5cm	Yes	1.6
[29]† ISSCC'17	180 nm	0.915	PPM	DL: 62.5kbps UL: 30.3kbps	2mW	No	20m	No	9†
[30] ISSCC'18	65 nm	5.8	DL: <4% ASK UL: HIMIL	DL: 5Mbps UL: 4kbps	10μW	No	1mm	No	0.01
[31] VLSI'14	65 nm	DL: 24 UL: 60	DL: 75% ASK UL: PPM	DL: 6.5Mbps UL: 1.2Mbps	11mW‡	No	50cm	No	4.4
[32]§ ISSCC'16	130nm	0.433	DL:PPM UL:PWM	125kbps	16μW	Yes (Symmetric)	5mm	No	64§

†Assembly of multiple functional layers (photo-voltaic powering, battery, antenna, etc.) is used.

‡The calculated value in [29] is cited.

§PCB-level components including off-chip coupler are required.

Table 2.2: Comparison of Elliptic Curve Hardware Accelerators

Reference	**CMOS Process**	**Technology Normalized Area**	**Cycle Count**	**ECSM Energy**
[48] CRASH'05	350 nm	31kGE	1.1M	550μJ
[45] CHES'15	130 nm	33kGE	811.2k	56μJ
[49] ISSCC'18	65 nm	65.5kGE+ 4kB SRAM	496k	17.6μJ
This Work	65 nm	25kGE	650k	14.4μJ

Chapter 3

A Dual-Antenna, 263-GHz Energy Harvester in CMOS with 13.6% THz-to-DC Conversion

3.1 Motivation

Pushing the wave frequency of far-field wireless power transfer (WPT) to the terahertz regime is essential for ultra-miniaturized, battery-less platforms, which currently can only be powered through light or ultra-sound (Fig. 3-1). As an example, the mm^2-size THz identification tag (THz-ID) in [1, 16] relies on integrated photo-diodes, and THz WPT will allow embedding the tags into optically-opaque packages of small-size goods (e.g., semiconductor chips) for authentication and logistic tracking. Similarly, micro-robots and sub-mm^3 wireless sensor nodes are also optically-powered through integrated photo-diodes [2, 50]. Light powering limits their application only to optically transparent mediums and most of the silicon chip area is also taken by the photo-diodes for sufficient energy harvesting which leaves little room for adding advanced functionality in the sub-mm form factor. Previously, the highest harvesting frequency in silicon was only 94 GHz [51, 52]. These harvesters require off-chip antennas which increases the total size and packaging cost, hence are not suitable for

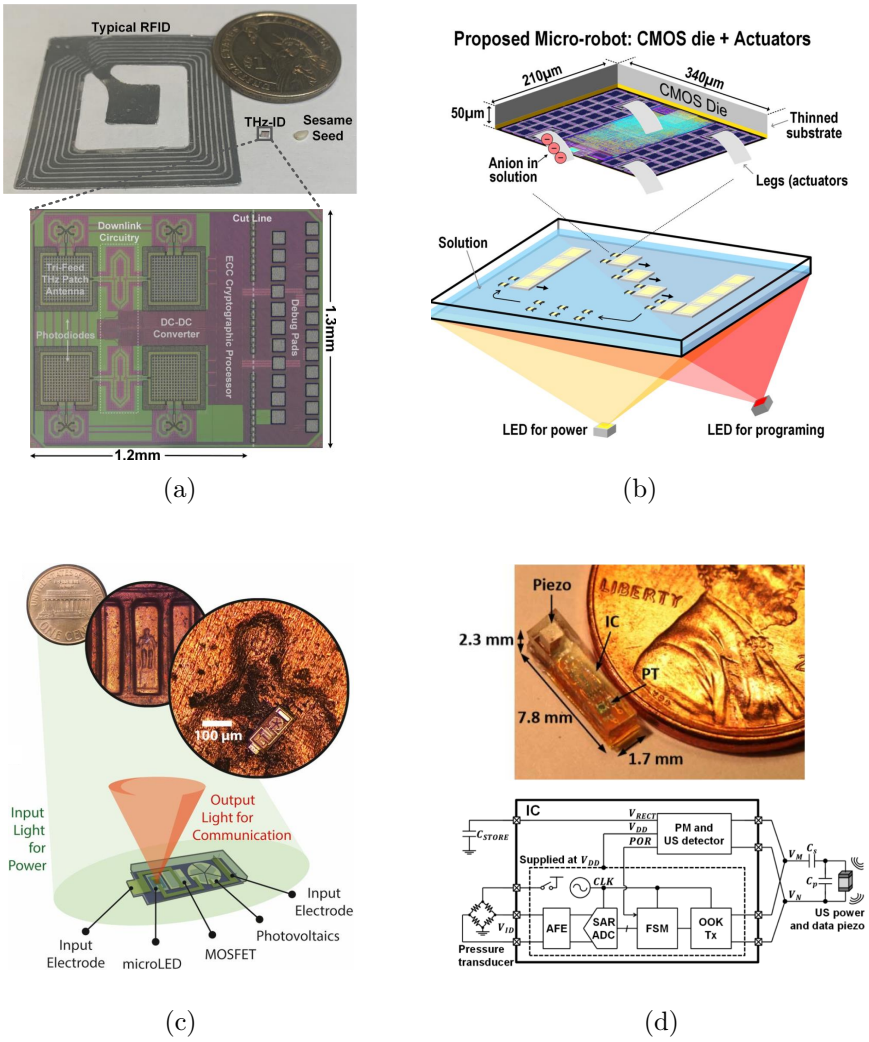
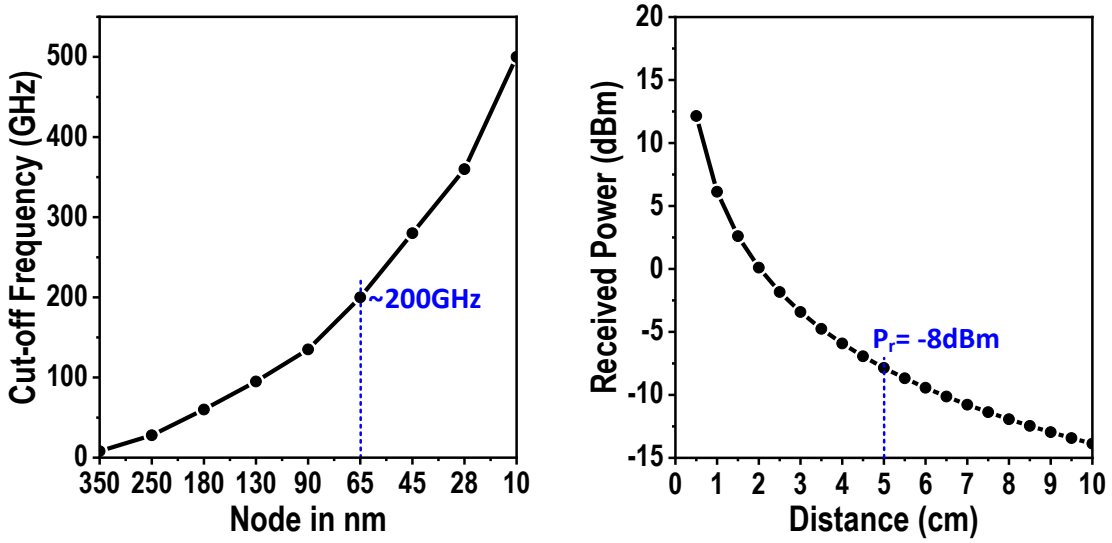


Figure 3-1: Potential applications of THz wireless powering in ultra-miniaturized systems: (a) THz-ID [1], (b) Micro-Robot [2], (c) Micro-sensors [3] and (d) Micro-implants [4].

ultra-miniaturized applications.

3.2 Challenges of THz WPT

There are two main challenges in efficient THz WPT: limited cut-off frequency (f_t) of the CMOS device and the lack of high-power THz sources. As shown in Fig. 3-2a, the f_t of a 65-nm NMOS device is ≈200 GHz [5]. The device cannot fully respond to signals above f_t and hence the device doesn't operate as an efficient switching



(a) (b)

Figure 3-2: (a) Cut-off frequency of CMOS devices with technology node scaling [5]. (b) Calculated received power at varying distances from a 20-dBm 300-GHz source (G_T=26-dBi and G_R=2-dBi).

rectifier above 200 GHz. Therefore, it is important to use a technology node with f_t comparable to or higher than the frequency of the signal to be rectified. The implementation of on-chip THz harvesters requires not only high-speed nonlinear devices but also unconventional peripheral circuits that maximize the rectification efficiency, η, of the device near its speed limit. Secondly, the high-power source is typically infeasible in THz setups. For instance, from a state-of-the-art 0.3-THz III-V source with 20-dBm output and 26-dBi antenna gain, the power received by an on-chip antenna ($\sim$2-dBi gain) at 5-cm distance is only -8 dBm as shown in Fig. 3-2b. The corresponding reduced signal swing makes it difficult to fully utilize the device's nonlinearity for rectification. It is noteworthy that all prior mm-Wave harvesters [51–57] are designed to work with high input power of a few to tens of mW and at the sub-mW input level their efficiencies drop sharply.

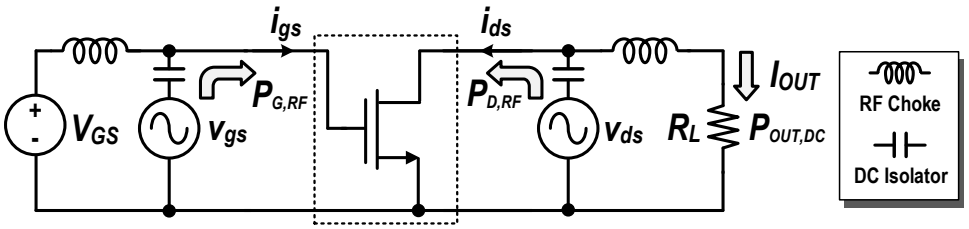


Figure 3-3: A generalized testbench for rectification performance test.

3.3 THz Energy Harvester Design

In this thesis, I present a 263-GHz energy harvester using Intel's 22-nm FinFET process, increasing the highest frequency of the CMOS harvester by ∼3x. To maximize the THz-to-DC conversion efficiency, η, at low available radiation power, the harvester achieves the optimal operating conditions of the device. In specific, the circuit enables self-gate biasing; and through a dual-antenna topology, it drives the transistor drain and gate terminals with both optimal voltage phase difference and power ratio simultaneously and precisely. The antenna integrated harvester is ultra-compact (∼0.5 mm^2) and does not rely on any external component. At -8-dBm input power level, 13.6% THz-to-DC efficiency is experimentally obtained, resulting in >20-μW harvested DC power – sufficient even for advanced, power-consuming functions, like cryptography in THz-IDs, and motion of micro-robots. The THz energy harvester design is presented next with two steps: (1) finding the conditions under which the FET conversion efficiency is maximized, and (2) designing a network around the FET to achieve the above conditions.

3.3.1 Optimum Conditions for η_{max}

Although the 22-nm N-FinFET possesses a f_t of 300 GHz [58], the closely-spaced thin interconnects connecting to the device inevitably and significantly increase the THz power loss. Efficient THz-to-DC conversion is then only obtained when stringent device operating conditions are met. Fig. 3-3 shows a generalized testbench to search for such conditions, where two arbitrary RF voltage sources v_{gs} and v_{ds} are driving the gate and drain nodes, respectively, and the rectified DC current I_{OUT} is extracted

to a load R_L. The THz-to-DC conversion efficiency is defined as

$$\eta = \frac{P_{OUT,DC}}{P_{in}} \tag{3.1}$$

where the net injected RF power

$$P_{in} = P_{G,RF} + P_{D,RF} = Re\left(v_{gs} i_{gs}^*\right) + Re\left(v_{ds} i_{ds}^*\right) \tag{3.2}$$

Note that a certain P_{in} corresponds to an infinite number of (v_{gs}, v_{ds}) value sets, and each set gives a different η. Our goal is to find the optimal device driving condition (v_{gs}, v_{ds}) for maximum η, specifically:

$$\Delta\varphi = \angle v_{ds} - \angle v_{gs} \quad and \quad A = |v_{ds}|/|v_{gs}| \tag{3.3}$$

In conventional low-frequency rectifiers, out-of-phase gate and drain voltages are applied (Fig. 3-4a), so that when v_{gs} turns on the channel, a negative v_{ds} reaches its peak simultaneously and creates the maximum i_{ds}, hence the maximum, positive I_{OUT} from the clipped i_{ds} waveform. At THz frequencies, the above conditions are no longer valid. As illustrated in Fig. 3-4b, the finite pico-second-level transit time of carriers causes a phase delay $\Delta\varphi$ between v_{gs} and the moment the channel is ON. Therefore, if v_{ds} is still out-of-phase with v_{gs}, the channel will be turned OFF prematurely, resulting in an under-driven i_{ds}. For low input THz power P_{in} (hence smaller v_{gs} swing), this under-drive problem is worsened due to shorter channel ON time. To improve rectification efficiency, the following optimizations can be applied.

1. A $\Delta\varphi$ delay can be applied to v_{ds} ("Step 1" Fig. 3-5a), so that peak v_{ds} and minimum channel resistance occur simultaneously, hence higher i_{ds}.

2. Next, the rectifier DC output voltage can be used to self-bias the transistor gate ("Step 2" Fig. 3-5b), so that the channel is turned ON for a longer duty cycle, further increasing I_{OUT}.

3. Self-biasing also relaxes v_{gs} swing requirement, allowing more P_{in} to be injected to the drain ("Step 3" Fig. 3-5c) and causing even higher i_{ds}.

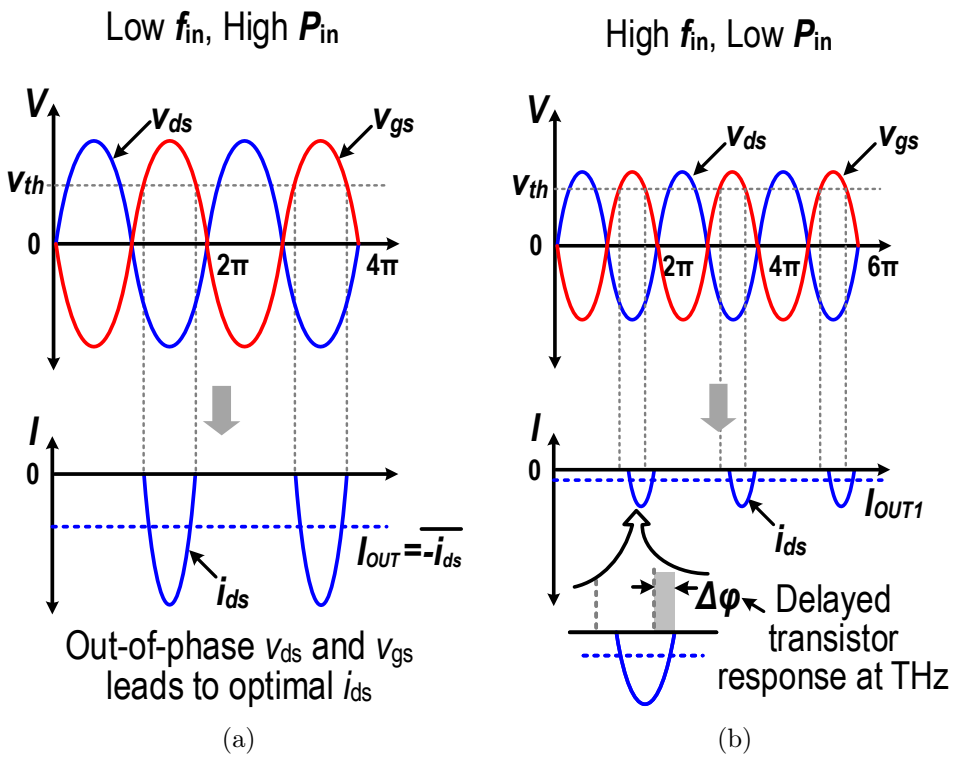


Figure 3-4: Rectifying operation of FET in a conventional harvester at (a) low f_{in} and high P_{in}, and (b) high f_{in} and low P_{in}.

The above optimum conditions give the maximum possible efficiency η_{max}. In Fig. 3-6, a self-biased N-FinFET is simulated with various (v_{gs}, v_{ds}) combinations while keeping P_{in}=-8 dBm. An η_{max} of 25.8% is obtained, under the following optimum conditions.

$$\Delta\varphi_{opt} = 45^{\circ} \quad and \quad A_{opt} = 3.75 \tag{3.4}$$

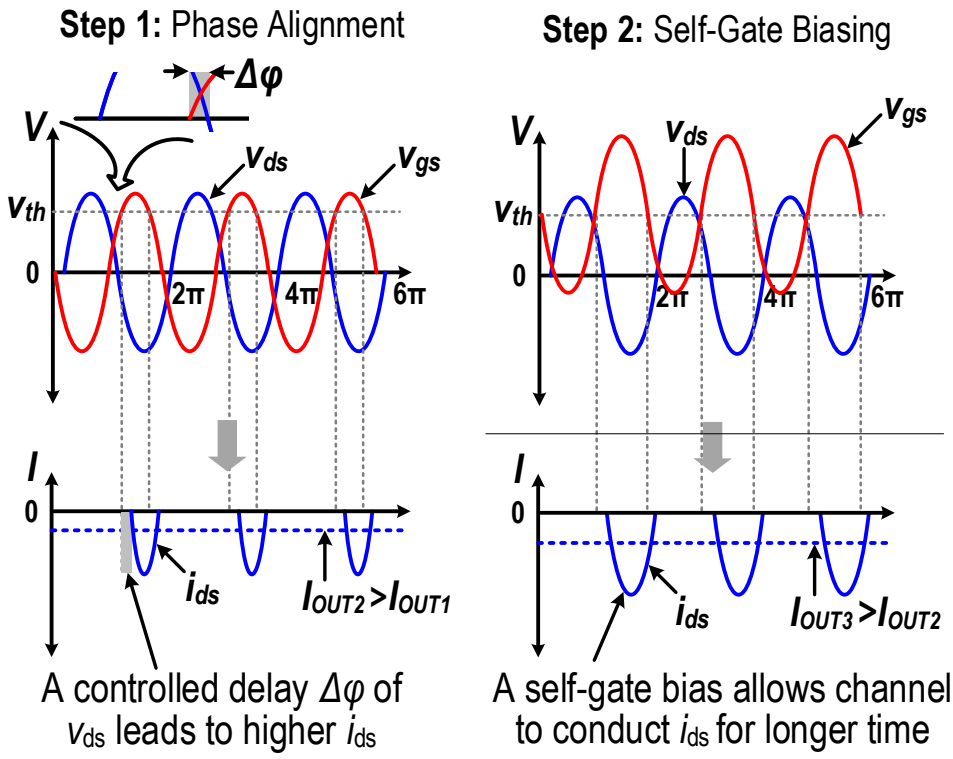
Amplitude ratio also corresponds to an input power ratio (m=$P_{D,RF}/P_{G,RF}$ in Fig. 3-3) of m_{opt}=2.2. Note that no prior reported energy harvesters meet all those conditions.

3.3.2 Circuit for Optimum Conditions: Dual-Antenna Design

Conventional harvester topologies adopting a single antenna or uniform antenna array (Fig. 3-7a) are not appropriate for THz operations; because it is difficult to create a passive network between the antenna and the transistor, which simultaneously achieves the above ($\Delta\varphi_{opt}, m_{opt}$) conditions and the conjugate matching at both the gate and drain nodes. The complexity of such a network also normally incurs large power loss. Our harvester adopts a compact scheme (Fig. 3-7b) involving two asymmetric patch antennas driving the gate and drain separately. This dual-antenna topology corresponds to a systematic design flow:

1. While the antenna length determines the resonance frequency, the width being proportional to the radiation aperture has a near linear relation with the antenna gain (see Fig. 3-8b). Given the uniform power density of the incident plane wave, the received power ratio of two antennas is then well controlled by the patch width ratio. In our design, by choosing W_G=230 μm and W_D=500 μm, the ratio (m) of power injected into the device nodes is readily fixed at m_{opt}=2.2.

2. Now, the matching networks for gate and drain are decoupled and only need to transform Z_G and Z_D in Fig. 3-7 to the two antenna impedances $Z_{ANT,G} = 173\Omega$



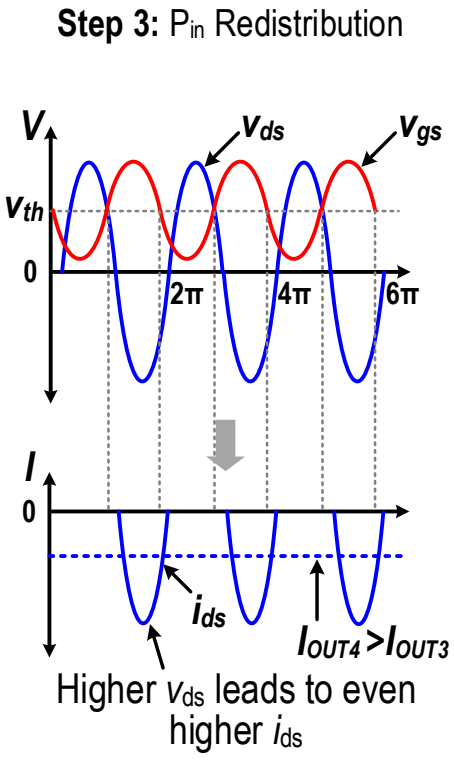


Figure 3-5: Rectifying operation of FET in our THz harvester with step-by-step optimizations.

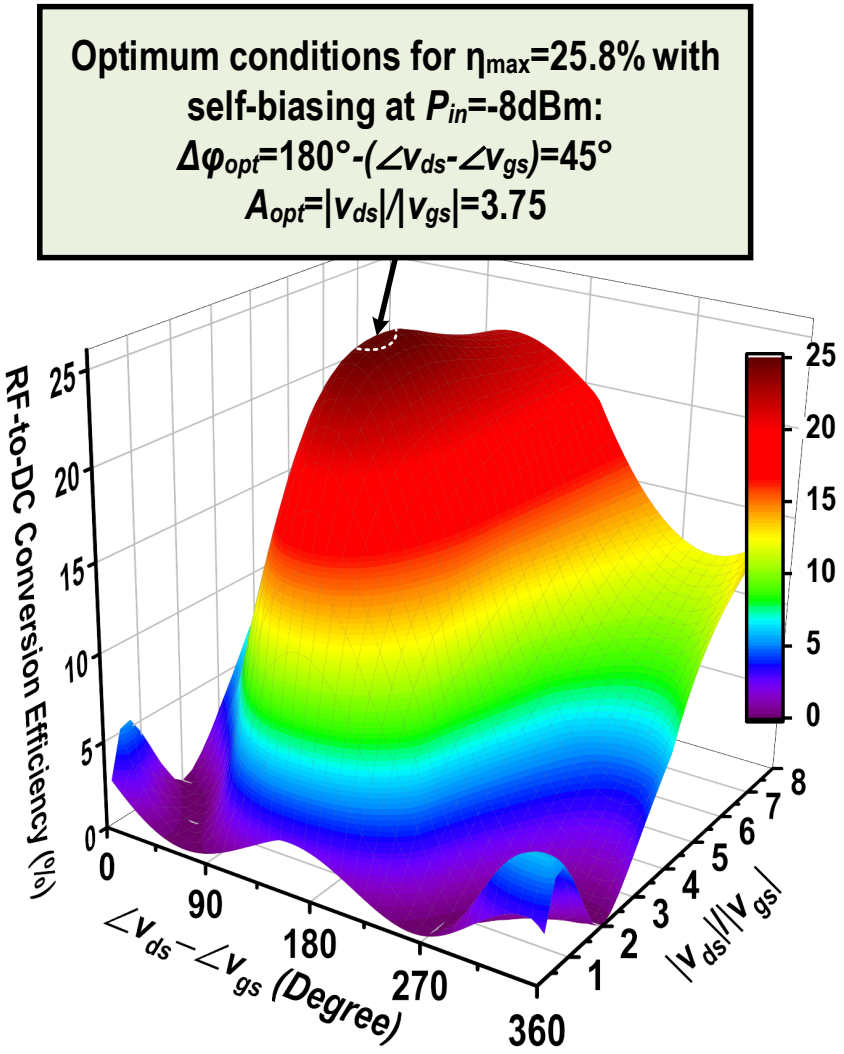
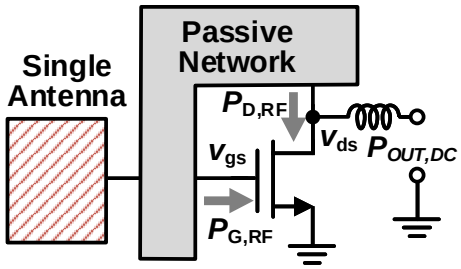
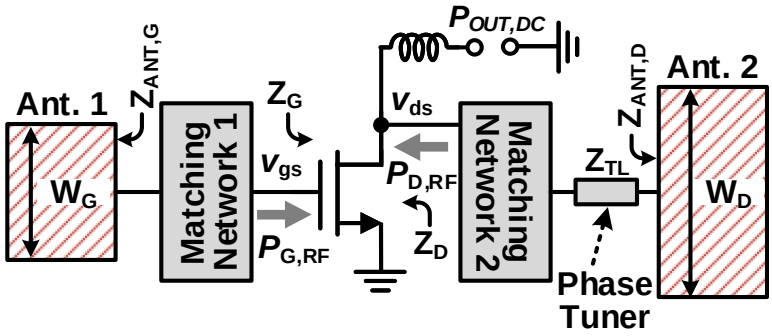


Figure 3-6: Simulated rectification performance of a N-FinFET (8×270nm/22nm) at various v_{ds} and v_{gs} ratio and phase difference.



(a)



(b)

Figure 3-7: Comparison between the (a) conventional single-antenna topology and (b) our dual-antenna topology.

and $Z_{ANT,D} = 128\Omega$, respectively, i.e.

$$Z_{ANT,G} = Z_G^* \quad and \quad Z_{ANT,D} = Z_D^* \tag{3.5}$$

Here, Z_G and Z_D are the *active impedances* of the gate and drain, in Fig. 3-3, valid only when the simulated device is driven under the optimal conditions and are derived as

$$Z_G = \frac{v_{gs}}{i_{gs}} = 33.5 - j25.7\Omega \quad and \quad Z_D = \frac{v_{ds}}{i_{ds}} = 24.6 - j117.8\Omega \tag{3.6}$$

Next, assuming lossless matching networks, the "maximum power delivery" requires the available power of the two antenna sources to be the same as $P_{G,RF}$ and $P_{D,RF}$ in ((3.2)):

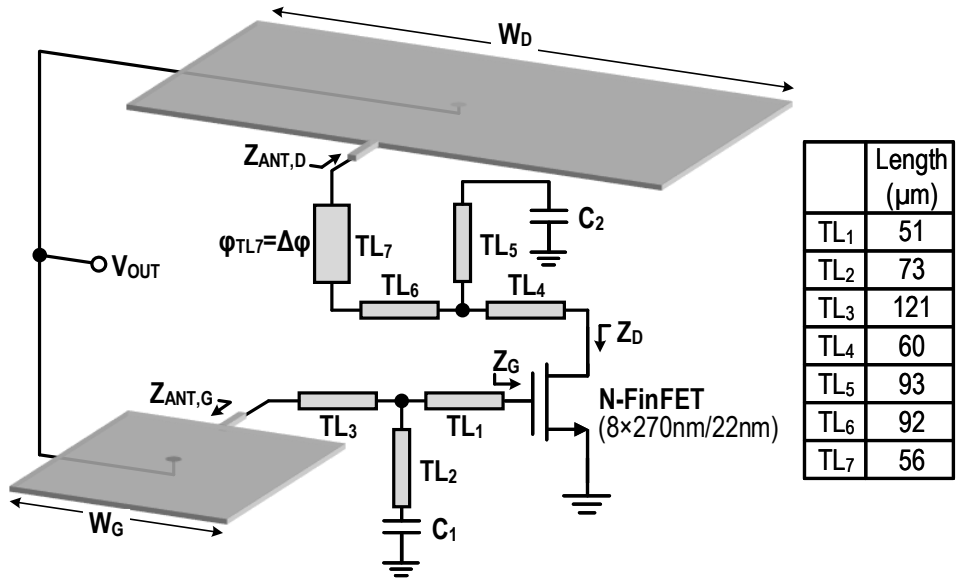
$$\frac{|V_{ANT,G}|^2}{4\,\mathrm{Re}\{(Z_{ANT,G})\}} = P_{G,RF} = \mathrm{Re}\left\{(v_{gs} \cdot (\frac{v_{gs}}{Z_G})^*)\right\} = \frac{|v_{gs}|^2 \cdot \mathrm{Re}(Z_G)}{|Z_G|^2} \tag{3.7}$$

$$\frac{|V_{ANT,D}|^2}{4\,\mathrm{Re}\{(Z_{ANT,D})\}} = P_{D,RF} = \mathrm{Re}\left\{(v_{ds}\cdot(\frac{v_{ds}}{Z_D})^*)\right\} = \frac{|v_{ds}|^2\cdot\mathrm{Re}(Z_D)}{|Z_D|^2} \tag{3.8}$$

3. Finally, to achieve $\Delta\varphi_{opt}$, a transmission line (TL) is inserted between the antenna and the matching network on the drain side. Note that the opposite orientations of the antennas provide an extra 180° phase between v_{gs} and v_{ds}; that eliminates the need for a lossy transformer or balun to approach $\angle v_{ds}$-$\angle v_{gs}$=180°-$\Delta\varphi_{opt}$=135° (Fig. 3-7). The length of the TL is then adjusted until $\Delta\varphi_{opt}$ is met at the device drain and gate. Ideally, the TL impedance Z_{TL} is set to be the same as $Z_{ANT,D}$, so that its length adjustment does not affect the matching from the previous step. But in our case $Z_{ANT,D}$ is too high for the phase-tuning TL to realize, so a TL with lower Z_{TL} is used and co-designed with Matching Network 2 in Fig. 3-7.

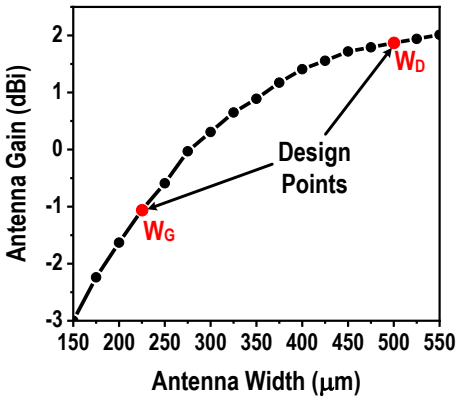
The schematic based on the above flow is shown in Fig. 3-8a. The adopted multi-stub matching networks ($TL_{1,2,3}$ and $TL_{4,5,6}$) along with the impedance transformation details given on a Smith chart are shown in Fig. 3-8c. The additional phase tuning is provided by TL_7. Lastly, connecting the central AC ground nodes of the patch antennas together enables the self-biasing of the transistor without interfering with antenna operations. Such a scheme also ensures that the self-bias voltage is close to the transistor V_{th}=0.18 V when driving an optimum load (see Fig. 3-12a). The same connection is also used to extract DC output power, thus avoiding lossy RF chokes.

Regarding the implementation of the patch antenna, its radiator uses the top copper (Cu-pad) layer of the CMOS process and has a length of 258μm. The ground plane of the antenna is made out of the M1-to-M6 layers and there is no dummy metal filling between the radiator and the ground. The antenna is also enclosed by a ground wall (M1-to-M8 metal stack), which is 20-μm away from the patch on all sides. The peak directivity and radiation efficiency of the drain side antenna in the HFSS simulation are 7.1 dBi and 39%, respectively, and for the gate side antenna are 4.4 dBi and 36%, respectively. $TL_{1,2,3}$ are grounded co-planar waveguides (GCPW) implemented using M8 with 2μm width and 8μm spacing from the ground. $TL_{4,5,6}$ are

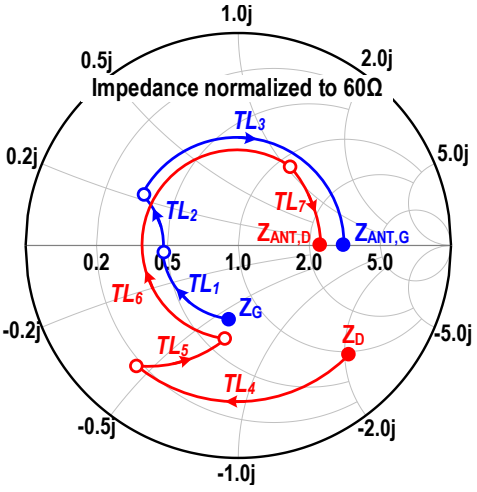


	Length (μm)
TL_1	51
TL_2	73
TL_3	121
TL_4	60
TL_5	93
TL_6	92
TL_7	56

(a)



(b)



(c)

Figure 3-8: (a) Schematic of the THz energy harvester. (b) HFSS-simulated antenna gains for different antenna widths. (c) Gate and drain impedance matching networks on a Smith chart.

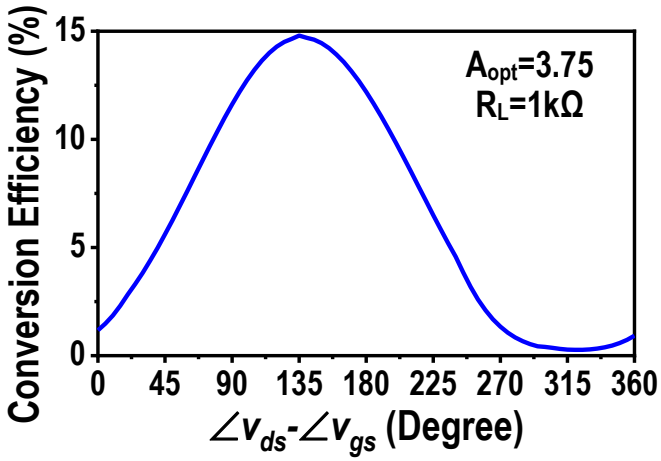
CPW implemented using M8 with 2μm width and 10μm spacing from the ground. TL_7 is implemented as a 12μm wide microstrip line on M8. C_1 and C_2 ($\sim$100fF) provide AC ground for the matching networks. Fig. 3-6 shows that even with losses of peripheral passives (device vias and matching networks), the above-mentioned optimum conditions still lead to η_{max}=15% with $P_{OUT,DC} \approx 24\mu W$.

3.4 Measurement Results

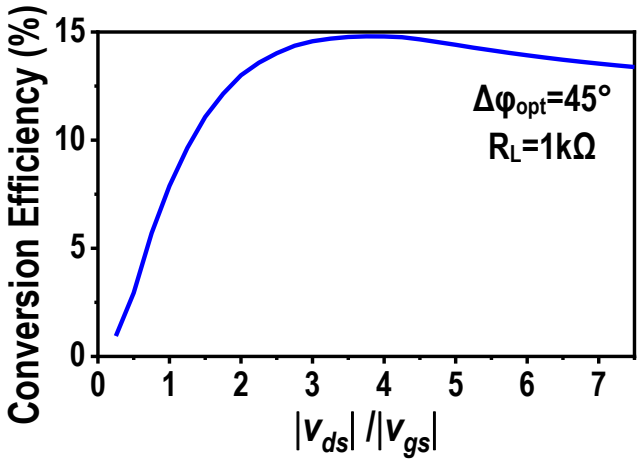
The chip is fabricated in a 22-nm FinFET process and has an area of 630×910 μm^2 as shown in Fig. 3-10. Most of the silicon and bottom metal layers under and around the antennas are unused and can be utilized for added functionality in future systems. The measurement setup is shown in Fig. 3-11, where a VDI amplifier-multiplier chain (AMC) radiates 90-mW 263-GHz signal with a 26-dBi horn antenna, and a digital multimeter measures the output voltage across a variable load resistor. The output power of AMC is measured using a PM5 Erickson power meter and is also verified with the manufacturer's calibration datasheet. The power received by the harvester is calculated using the Friis equation and the simulated gain of on-chip patch antennas as

$$P_R = P_T + G_T + G_R + 20\log_{10}\left(\frac{\lambda}{4\pi r}\right) \quad (dB) \tag{3.9}$$

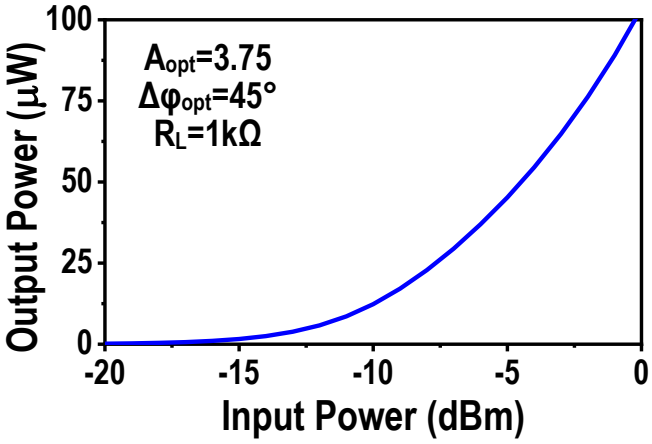
The measured load line performance of the harvester at 5-cm distance, shown in Fig. 3-12a, results in an optimum load of $\sim$1 kΩ. The measured output voltages at various distances are given in Fig. 3-12b. In Fig. 3-13, the measured incident angle sensitivity of the harvester is presented. The harvester is more sensitive in the E-plane than in the H-plane, because a non-zero incident angle in the E-plane introduces an additional phase shift between the two antenna outputs, causing deviation from the optimum device conditions. For angle-insensitive application scenarios, the two antennas should be closely placed, whereas when high angle sensitivity is desired (e.g., for robustness against undesired beam interrogation), the antennas should be separated apart. Fig. 3-14 shows the measured efficiency η and $P_{OUT,DC}$, excluding



(a)



(b)



(c)

Figure 3-9: Simulated rectification performance of a N-FinFET including losses from the device vias and matching networks.

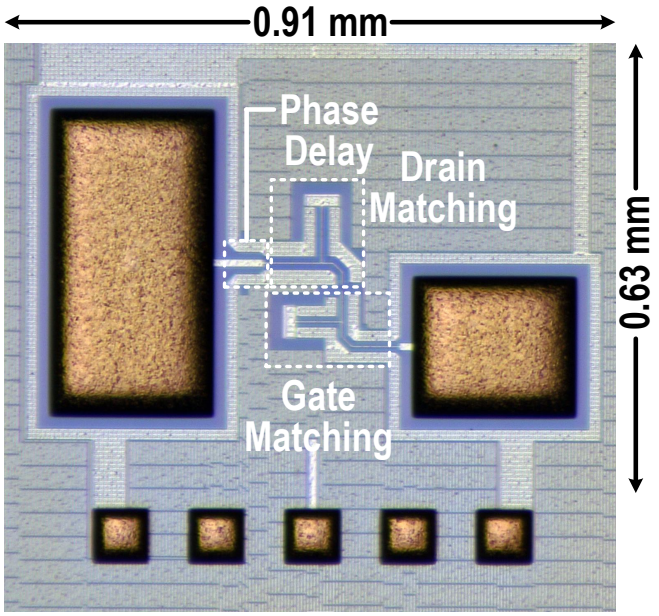


Figure 3-10: Chip micrograph of THz energy harvester.

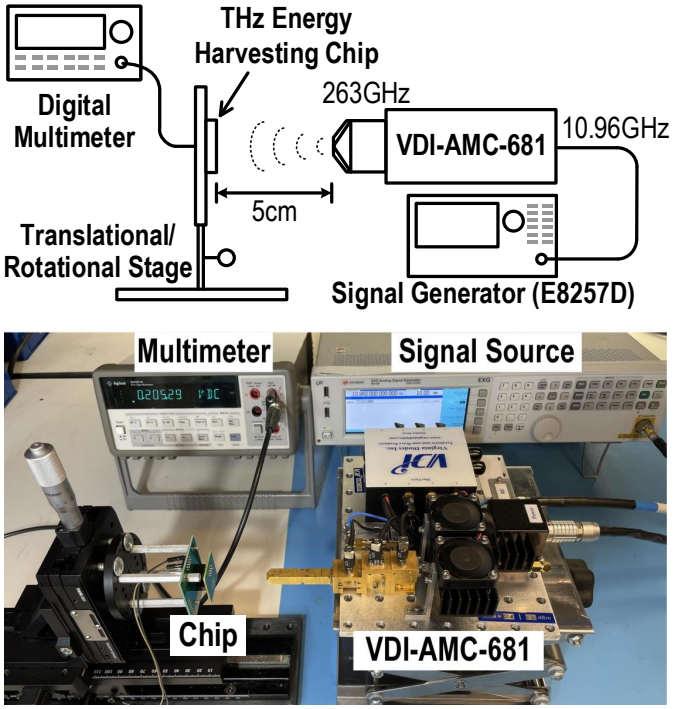
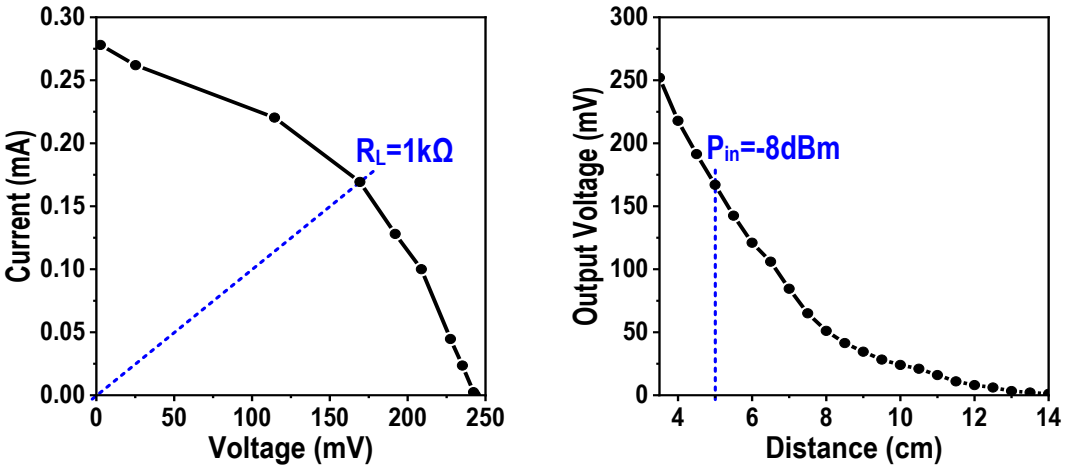


Figure 3-11: Diagram and photo of the test setup.



(a) (b)

Figure 3-12: Measured (a) load line and (b) open-circuit voltage of the harvester.

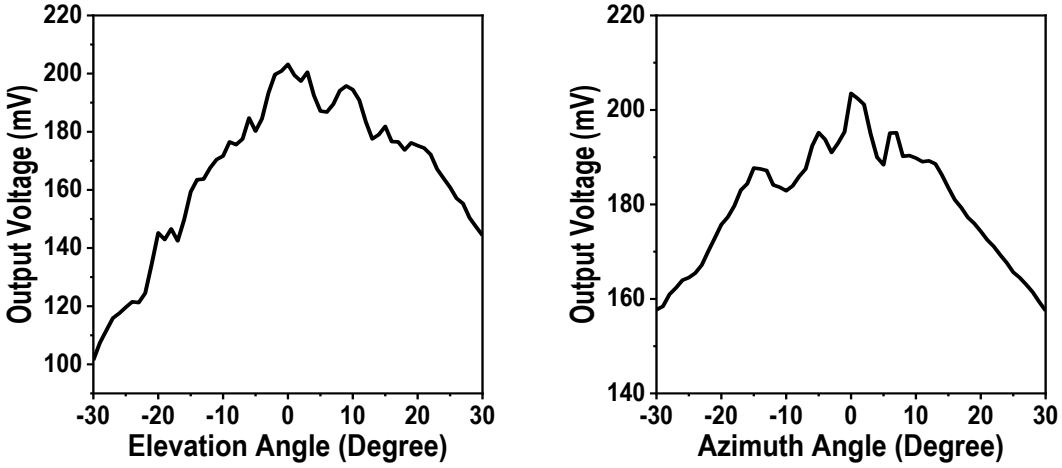
the antenna loss, at various attenuated input power levels. At P_{in}=-8 dBm, η_{max} of 13.6% and $P_{OUT,DC}$ of 22 μW are obtained.

3.5 Comparison with the State-of-Art

A dual-antenna based 263-GHz energy harvester in a 22-nm CMOS process is presented. This work is compared with the state-of-art mm-Wave harvesters in Fig. 3-15 and Table 3.1. It achieves not only the highest harvesting frequency but also a highly competitive conversion efficiency of 13.6% at low input power levels. This is enabled by an antenna-device co-design approach that simultaneously achieves the device's optimum conditions under self-gate biasing. The ultra-compact harvester ($\sim$0.5 mm^2) also demonstrates the feasibility of wirelessly powered, package/battery-less systems with the sub-mm^2 form factor.

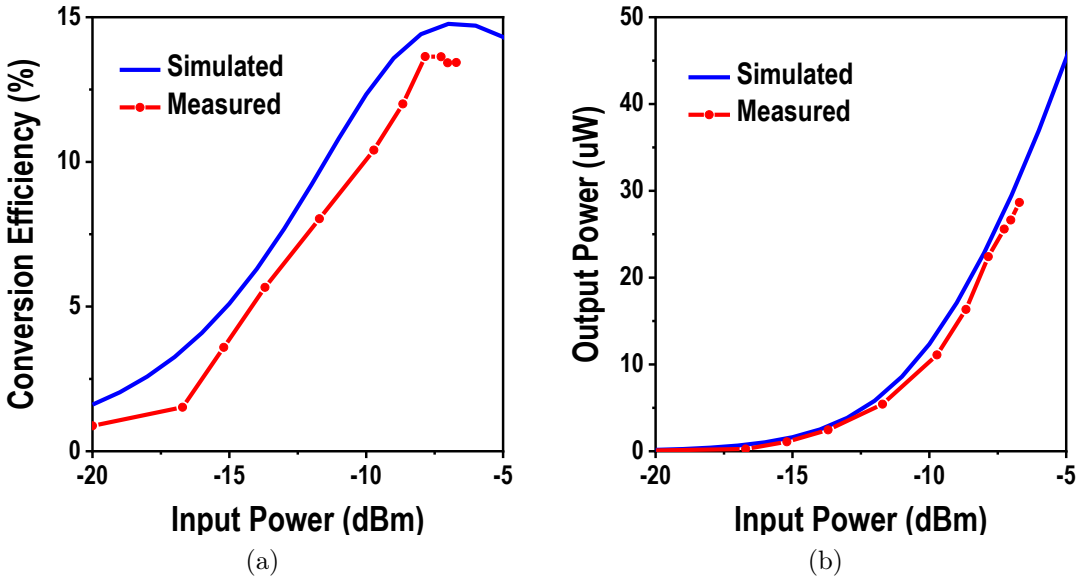
3.6 True THz-ID

Efficient THz energy harvesting has enabled a true THz-ID i.e. a tag that entirely operates with THz signal without requiring any optical component. It is powered by



(a) (b)

Figure 3-13: Measured angle sensitivity in (a) E- and (b) H-planes.



(a) (b)

Figure 3-14: Comparison of simulated and measured (a) THz-to-DC conversion efficiency (η), and (b) output power ($P_{OUT,DC}$) with a 1-kΩ load.

Table 3.1: Comparison with State-of-Art mm-Wave Energy Harvesters

	CMOS Technology	**Freq. (GHz)**	**Peak Efficiency η_{max}† and Related P_{in}**	**η at Reduced P_{in} ($\leq$0 dBm)†**	**Area (mm^2)**
This Work	22nm FinFET	263	13.6% at -8dBm	13.6% at -8dBm	0.57
T-MTT'21 [51]	40nm Bulk	94	45.8% at 10dBm	5% at 0dBm*	0.08#
T-MTT'19 [52]	65nm Bulk	94	24% at 16dBm	2% at 0dBm*	0.09#
		35	36.5% at 15dBm	10% at 0dBm*	0.12#
T-MTT'16 [53]	40nm Bulk	60	32.8% at 5.7dBm	10% at -3dBm*	15600‡
T-MTT'14 [54]	65nm Bulk	24	20% at 6.4dBm	2% at -3dBm*	0.27#
		35	18% at 6.6dBm	4% at 0dBm*	
		60	11% at 3dBm	6% at 0dBm*	
IMS'17 [55]	65nm Bulk	89	21.5% at 12.7dBm	1% at 0dBm*	0.12#
IMS'14 [56]	65nm Bulk	94	10% at 4.5dBm	4% at -2.3dBm*	0.48
RFIC'13 [57]	65nm Bulk	71	8% at 5dBm	-	1.8

†Without antenna loss

*Estimated from the plots in the literature

#Area without antenna

‡Area including a grid antenna

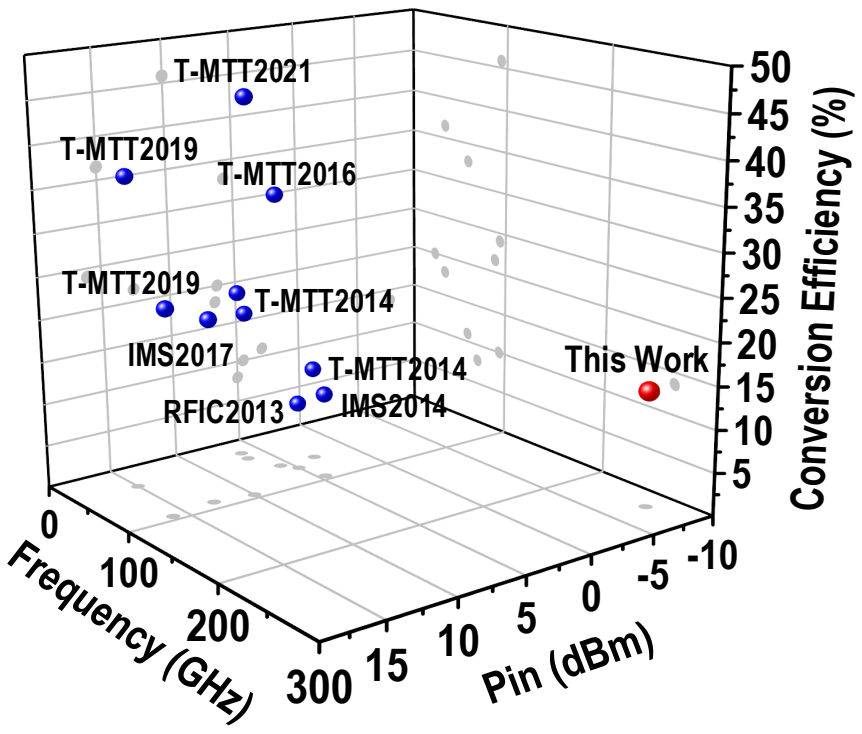


Figure 3-15: Comparison of 0.26-THz energy harvester with the state-of-art mm-Wave energy harvesters.

a THz signal and back-scatters using the same signal. Fig. 3-16 shows the schematic for such a tag where two antennas are used for energy harvesting and the other two antennas back-scatter the signal for transmitting the tag's data.

3.6.1 DC-DC Converter

A DC-DC converter up-converts the harvester output voltage (∼150mV) to ∼0.8V (nominal voltage in the 22-nm process). It consists of two Dickson charge pumps with six stages each, a tunable ring oscillator, and a storage capacitor (C_{store}=3.6nF) as shown in Fig. 3-17a. A feedback loop controls the frequency of the ring oscillator to regulate the output voltage under different loading conditions. The loop compares the output voltage ($V_{OUT,HIGH}$) with the reference voltage and a charge pump generates the control signal (V_{CTRL}). Fig. 3-17b shows the schematic of the Dickson charge pump. The first stage is driven by the clock signal from the ring oscillator which ensures that it works with input voltage (V_{IN}) as low as 100mV. The rest of the

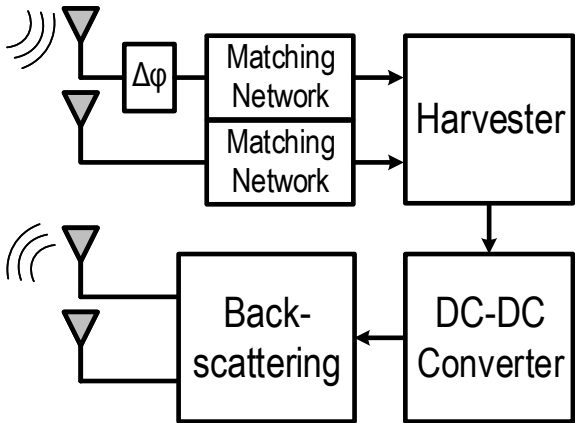


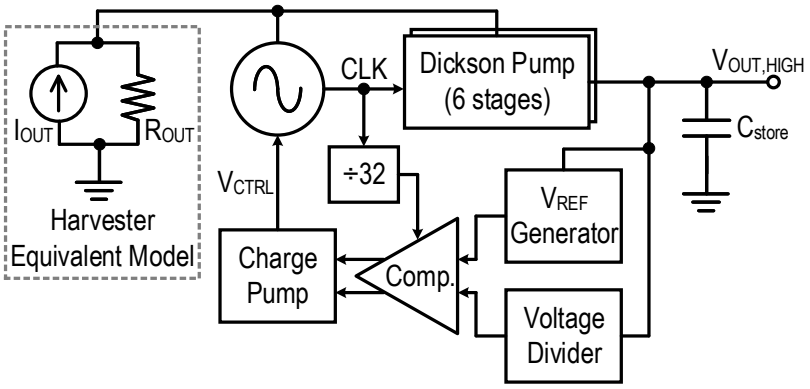
Figure 3-16: Block diagram of THz-ID with harvesting and back-scattering at 263 GHz.

stages have self-adaptive thresholds through diode-connected devices. The inter-stage capacitors (C_{fly}) are ∼100 pF. The ring oscillator employs leakage-based delay cells for frequency tuning in a range of 0.3-5 MHz as shown in Fig. 3-17c. In the post-layout simulation, the DC-DC converter has 46% power efficiency.

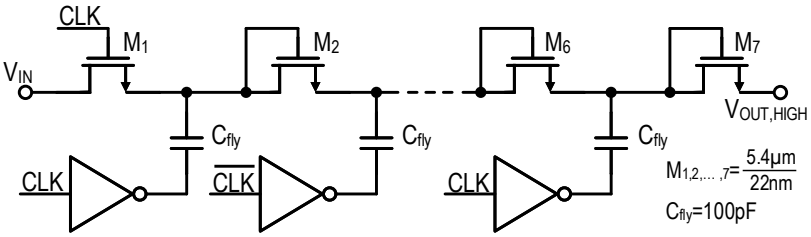
3.6.2 Back-scattering Module

The back-scattering module consists of two dual-feed patch antennas: single-ended (Feed1) and differential (Feed2) feeds as shown in Fig. 3-18b. The downlink incident signal with linear polarization along y-direction excites the TM_{010} mode of the patch antenna. It is extracted through the single-ended feed of the patch antenna and then mixed with data-modulated 8 MHz LO signals from the control circuit (Fig. 3-18a). The switches also direct the mixed signal to the differential ports of the antennas which excite the TM_{100} mode of the patch antenna. Consequently, the uplink radiated signal has orthogonal polarization to the downlink signal (i.e. linearly polarized along x-direction). In half of the LO cycle (when LO=1 and $\overline{LO}$=0) the signals are directed as shown in Fig. 3-19a and in the other half (when LO=0 and $\overline{LO}$=1) the signals are directed as shown in Fig. 3-19b. In this way, the back-scattered signal is BPSK modulated with LO signals. This is essential to filter out the weak back-scattered signal at the reader from the strong reflected signal.

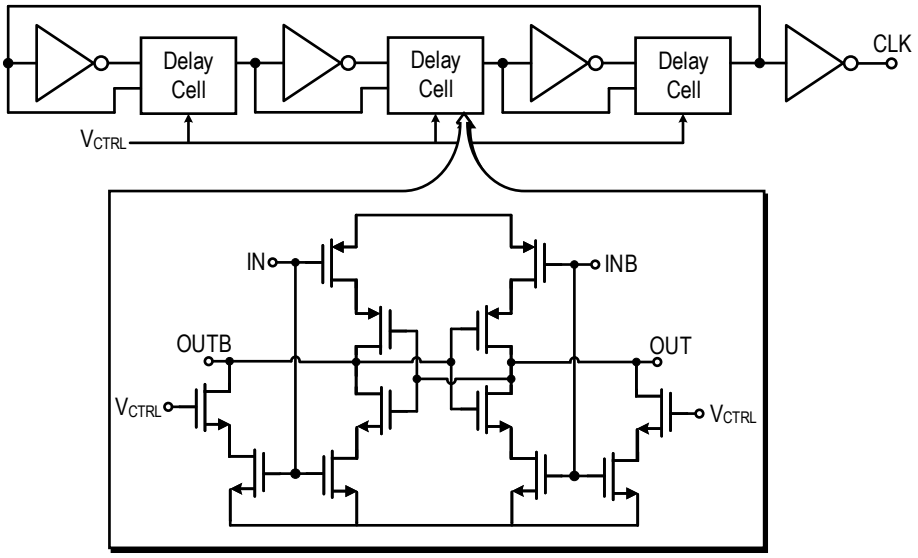
The radiator of the patch antenna uses the top copper (Cu-pad) layer of the CMOS



(a)

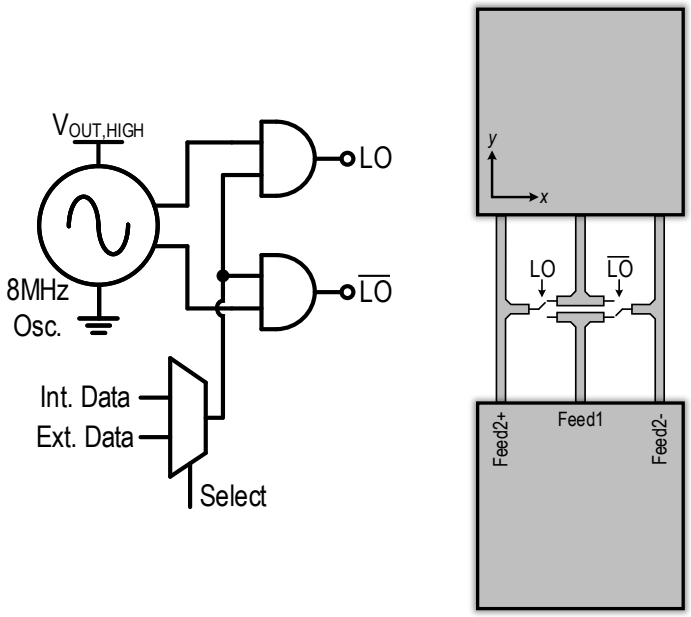


(b)



(c)

Figure 3-17: The schematic of the (a) DC-DC converter, (b) ring oscillator with delay cell, and (c) Dickson charge pump.

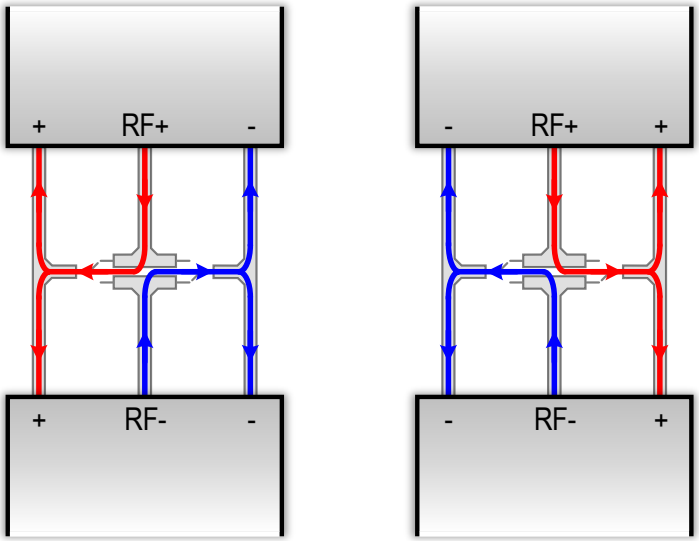


(a) (b)

Figure 3-18: The schematic of (a) control circuit and (b) back-scattering module with two patch antennas and a mixer.

process and has dimensions of 255μm along the y-direction and 263μm along the x-direction. The ground plane of the antenna is made out of the M1-to-M6 layers and there is no dummy metal filling between the radiator and the ground. The antenna is also enclosed by a ground wall (M1-to-M8 metal stack), which is 20-μm away from the patch on all sides. The peak directivity and radiation efficiency of the antenna in the HFSS simulation are 4.4 dBi and 35%, respectively. The transmission lines connecting the antennas' feeds and the mixer are grounded co-planar waveguides (GCPW) implemented using M8 with 2μm width and 10.5μm spacing from the ground. The chip is fabricated in a 22-nm FinFET process and has an area of 1600$\times$980 μm^2 as shown in Fig. 3-20.

Further circuit details and the chip measurement results will be presented in the future publications.



(a) (b)

Figure 3-19: The feeding polarity of the back-scattered signal when (a) when LO=0 and $\overline{LO}$=1 and (b) when LO=1 and $\overline{LO}$=0.

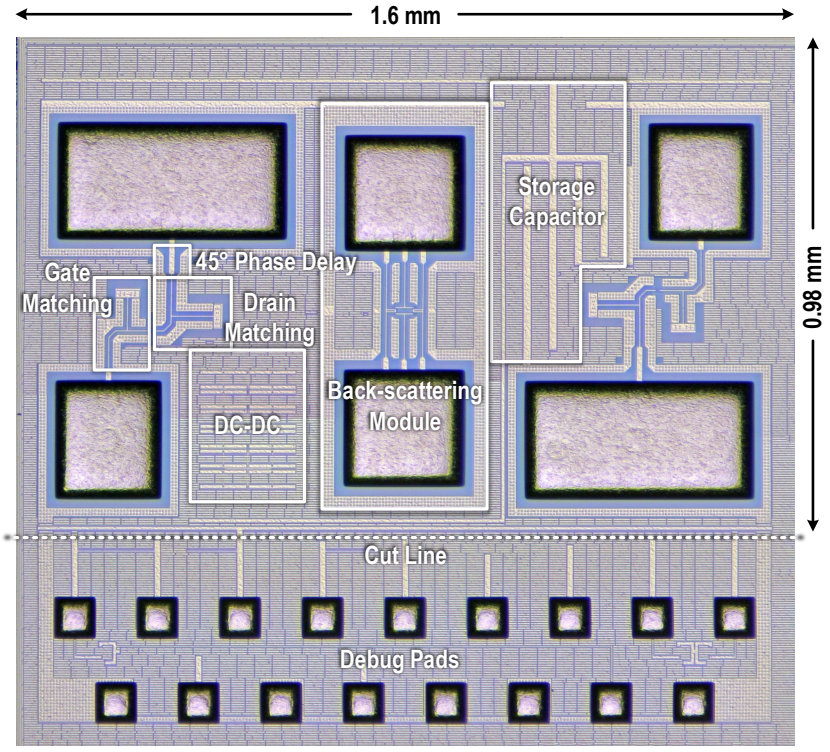


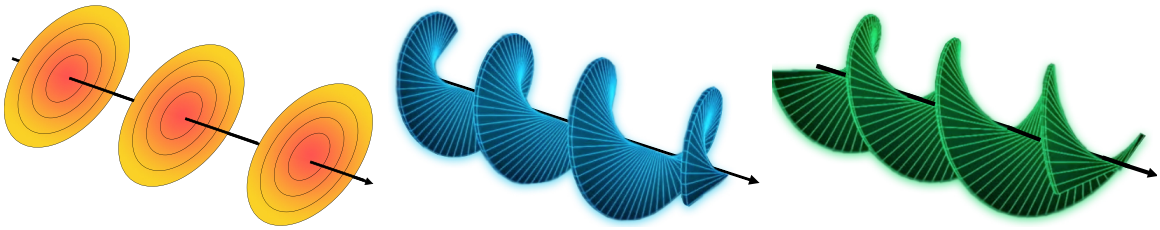
Figure 3-20: Chip micrograph of THz-ID with energy harvester and back-scattering.

Chapter 4

A 0.31-THz Orbital-Angular-Momentum (OAM) Wave Transceiver in CMOS with Bits-to-OAM Mode Mapping

4.1 Orbital-Angular-Momentum (OAM)

In 1909, the idea that electromagnetic (EM) waves carry angular momentum was discussed in a work of Poynting [59], who anticipated that circularly polarized light should have angular momentum. In 1935, it was, for the first time, experimentally verified by Beth [60, 61], who demonstrated the transfer of angular momentum between polarized light and the rotational motion of a birefringent wave plate. Within the frame of paraxial approximations, this angular momentum is divided into spin-angular momentum (SAM) that is linked to circular polarization of the EM wave and OAM that characterizes the rotation of the Poynting vector along the direction of propagation. The optical OAM regime gained a great renew of interest in the 1990s when the quantum characteristics of OAM states were discovered [62], [63]. However, OAM in the radio-frequency band was first simulated in 2007 [64] and experimentally



(a) (b) (c)

Figure 4-1: Wavefront of OAM beams for (a) m=0 (plane wave), (b) m=-1 and (c) m=-2 modes.

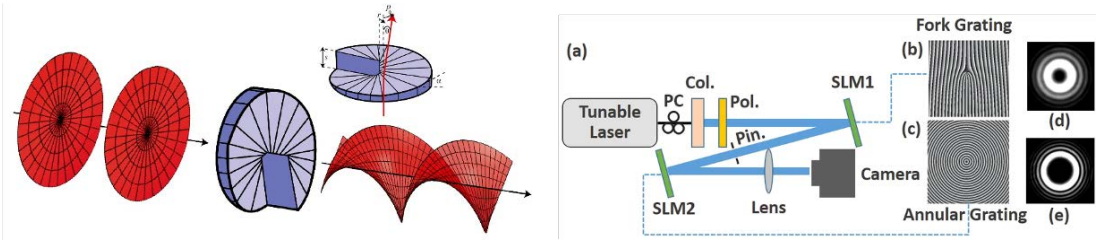
verified in 2011 [65].

An OAM-based wave possesses a wavefront with a helical phase distribution around the central axis of the beam with a phase singularity running along the axis. There are two classes of Gaussian beams which are known to carry OAM modes: Bessel-Gaussian (BG) beams and Laguerre-Gaussian (LG) beams. Both are solutions of Helmholtz equation solved in cylindrical coordinates under paraxial approximation. Mathematically, LG_{pm} modes are given by [66]:

$$LG_{pm} = \frac{C}{\sqrt{(1+z^2/z_R^2)}} \cdot \left[\frac{r\sqrt{2}}{w(z)}\right]^{|m|} \cdot L_p^{|m|}\left(\frac{2r^2}{w^2(z)}\right) \cdot e^{\frac{-r^2}{w^2(z)}} \cdot e^{jm\phi}, \tag{4.1}$$

where r, ϕ, z are coordinate variables for cylindrical coordinate system, C is a constant, $w(z)$=$w(0)\sqrt{(z^2+z_R^2)/z_R^2}$ is the $1/e$ radius of the Gaussian term with $w(0)$ being the beam waist at z=0, z_R is the Rayleigh range, $L_p^{|m|}(x)$ is an associated Laguerre polynomial and p is the number of radial modes in the intensity distribution. The term $e^{jm\phi}$ represents the azimuthal variation of phase with m representing its index i.e. OAM mode. Note that the z-variation, i.e., variation in the direction of propagation, is omitted for the sake of simplicity. Different OAM modes are determined by the handedness and the total phase change (ϕ=$2m\pi$, m=0, $\pm$1, $\pm$2...) of the wavefront twist as visualized in Fig. 4-1. Left-handed modes (i.e. clockwise rotation) are represented by positive integers and right-handed modes (i.e. anticlockwise rotation) are represented by negative integers.

Conventional OAM generation approaches involve dielectric spiral-phase plate



(a) (b)

(c) (d)

Figure 4-2: Discrete-components-based prototypes for the generation of OAM beams: (a) spiral-phase plate [6], (b) holographic gratings [7], (c) circular antenna array by NTT [8], and (d) circular antenna array by NEC [9].

(SPP) at optical [6] and millimeter-wave [67] frequencies, planar SPP [68], flat plate with holes [69], passive uniform circular antenna array [70–72], or metasurface in conjunction with separate signal drivers [73]. Some of these dicrete-component-based RF, mm-Wave, and optical prototypes are shown in Fig. 4-2. These discrete solutions, however, lead to very bulky, expensive, and power-hungry systems. Most of these systems also cannot dynamically switch between OAM modes. Up until now, no chip-based OAM component at any frequency is reported.

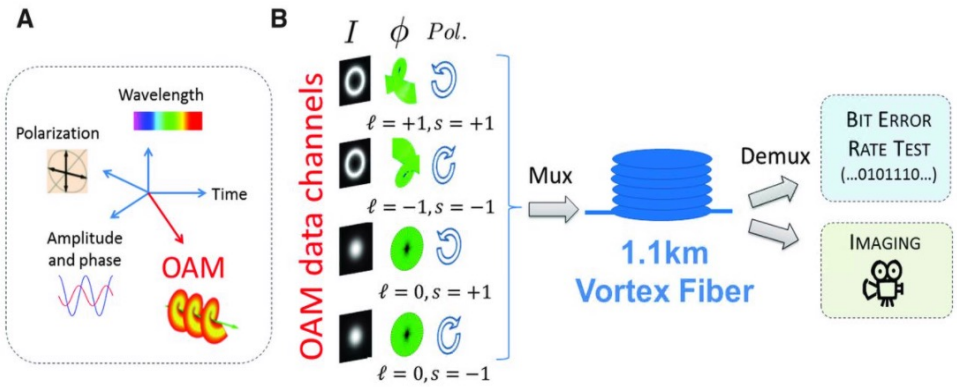
4.1.1 Application in High Data Rate Communication

Different OAM modes are orthogonal to each other i.e. they can be spatially multiplexed and de-multiplexed with theoretically no cross-talk. Previously, using this property multi-OAM-mode transmission has been studied for the enhancement of spectral efficiency [10, 67, 71, 72, 74]. At optical frequencies, 400 Gbps data transmission is achieved using four OAM modes at a single wavelength, and 1.6 Tbps using two OAM modes over 10 wavelengths [10] (Fig. 4-3a). In [67], four indepen-

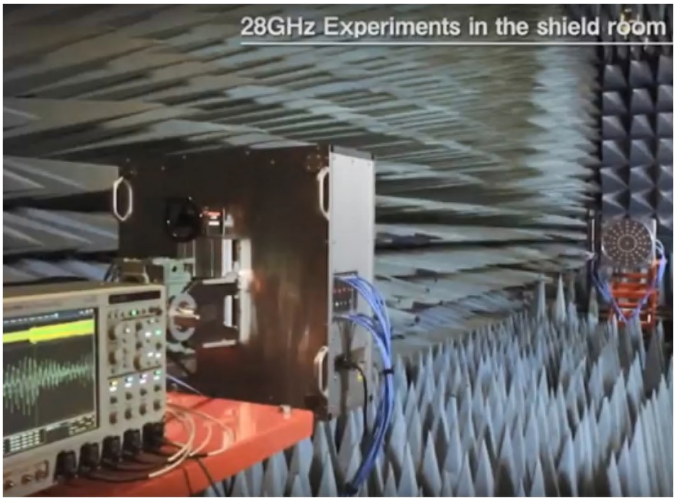
dent OAM beams on each of two orthogonal polarizations, modulated with 16QAM 28 GHz signal, were multiplexed to achieve a data rate of 32 Gbps. Recently, Nippon Telegraph and Telephone Corporation (NTT) has demonstrated wireless transmission at a distance of 10 m using an OAM system operating at 28 GHz as shown in Fig. 4-3b. Eleven data signals, each at a bit rate of 7.2 to 10.8 Gbps, were generated and simultaneously carried by multiple OAM-multiplexed EM waves, achieving a data rate of 100 Gbps [8]. At 40 GHz, the work in [72] has demonstrated over 100 Gbps using mode division multiplexing with seven OAM modes (m=0, $\pm$1, $\pm$2, $\pm$3) and dual linear polarization. However, it should be noted that spatial-multiplexing of OAM modes does not increase the channel capacity beyond what is achievable in multiple-input-multiple-output (MIMO) communication systems [75].

4.1.2 Application in Physical-Layer Security

THz band is enabling beyond-5G and 6G communications [76–80]. Large antenna arrays are the basic building blocks for such networks similar to 5G MIMO systems. An emerging challenge is the security of these wireless links, which are susceptible to eavesdropping at unintended positions, due to beam divergence and antenna side-lobes. Traditionally, wireless communication is secured at network and application layers using digital encryption techniques which rely on the trustworthy secret key distribution. Such security architectures are becoming computationally intensive and are not scalable with ubiquitous THz-links operating at multi-Gbps with strict energy constraints and latency requirements [81]. Physical-layer security (PLS) significantly relaxes the requirements for security at other layers [82]. OAM is a potential candidate that can physically secure the one-way transmission of secret keys in such networks and is easily generated from planar antenna arrays. The instantaneous mode of an OAM beam, when driven by the bits of the secret key, encodes the information within the phase twist around the beam axis (Fig. 4-4). It can only be effectively detected by a receiver with multiple phase-comparing antennas located around that axis. Such positioning requirement boosts the robustness against eavesdropping at off-axis locations [83, 84], where the SNR of the inter-antenna phase gradient rapidly drops below



(a)



(b)

Figure 4-3: (a) Conceptual diagram for 400 Gbps data transmission using four OAM at a single wavelength [10]. (b) Experimental setup in a shielded room demonstrated by NTT achieving 100 Gbps using five OAM modes at 28 GHz [8].

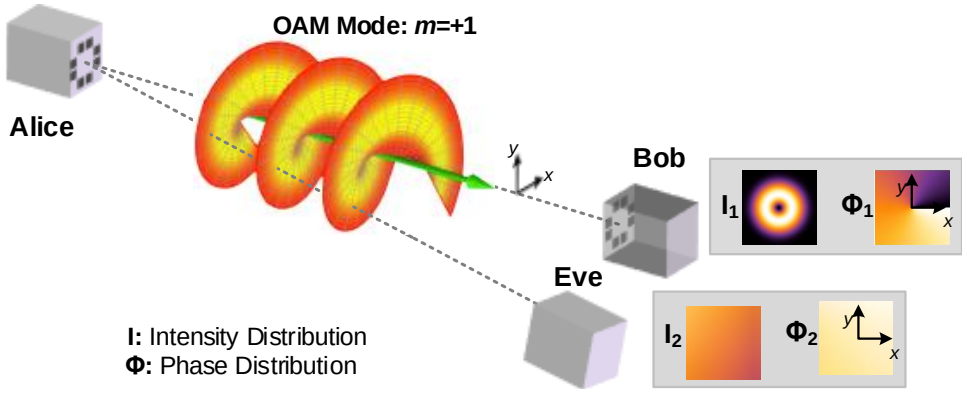


Figure 4-4: Potential application of THz-OAM transceiver in physically-secure wireless link against off-beam-axis eavesdropping.

the detectable threshold. This makes OAM-based security unique as compared to the other PLS techniques that rely on the distortion of the signal constellation in unintended directions using directional or space-time modulation [85–88].

4.2 THz-OAM Transceiver Architecture

This thesis, for the first time, presents a CMOS active antenna array that not only can generate and receive OAM waves at 310 GHz, but also perform electrical OAM mode switching among the m=+1 (left-handed), -1 (right-handed), (+1)+(-1) (superposition), and 0 (plane wave) states [17,18]. The above multiplexing and security applications are, therefore, made possible at the chip scale. The chip architecture is shown in Fig. 4-5. It consists of eight THz modulator/detector units (referred to as *pixel* henceforth) driven by a 310 GHz signal generator through a power divider. The pixels, with their integrated patch antenna, are placed in a uniform circular pattern. Each pixel generates radiation with a phase difference of $\Delta\phi$ with respect to its neighboring pixels. $\Delta\phi$ is adjusted by the LO signals from the controller, and its values of 0, +45°, and -45° correspond to the OAM modes of m=0, +1, and -1, respectively. An on-chip controller configures the chip in either transmission or reception mode. In the transmission mode, a Keccak block generates data of a random key, which can be mapped to the instantaneous OAM modes. In the reception mode, each pixel mixes its received wave with the local 310 GHz signal and generates an IF output. Analog

phase comparison of these IF signals enables the determination of the incident OAM mode. The THz-OAM chip has an area of only 2.1×2.6 mm^2, which is the smallest among all prior OAM prototypes.

4.2.1 Circular Antenna Array

The array factor for a circular antenna array is given as

$$AF = \sum_{n=0}^{N-1} I_n e^{jn\phi_n} e^{jkr_n[\cos\alpha_n \sin\theta\cos\phi + \sin\alpha_n \sin\theta \sin\phi]}, \tag{4.2}$$

where N is the number of elements, I_n and ϕ_n are the excitation amplitude and phase for the nth element, k is wavenumber, r_n and α_n are the radius and angle of the nth element and θ and ϕ are polar coordinates. In a uniform circular antenna array: $\alpha_n = 2n\pi/N$, and in order to generate OAM modes: $\phi_n = n\Delta\phi = 2n\pi/N$. The radiation pattern of the antenna array is determined by multiplying AF with the simulated radiation pattern of the patch antenna. This method is adopted to optimize the array diameter with sidelobe suppression with a fixed number of antennas.

To generate a pure OAM state, in theory, the largest OAM mode can be $|m|<N/2$. In this design N=8 and seven OAM modes (ϕ=2$m\pi$, m=0, ±1, ±2, ±3) can be generated. However, in this chip work, we demonstrate only the m=0, +1, -1 and ±1 modes. The intensity and phase profiles generated by the circular patch antenna array are simulated in the full-wave EM simulator, HFSS [38], for the four OAM modes. The far-field distributions of intensity and phase over a non-model plane are recorded in Fig. 4-6. In Fig. 4-6a, it can be seen that for m=0 the radiated power is centered at the beam axis, while for m=+1 and -1 the same radiated power is now uniformly distributed around the central null running along the beam axis. For the superposed mode m=(+1)+(-1), there are two counter rotating beams with a null separating them along the diagonal. Fig. 4-6b shows that the left and right-handed phase twisted for m=+1 and -1, respectively, along with the phase singularity at the center. The plane wave has no phase variation and the superposed mode shows two out of phase rotations. Note that the phase distribution is not discontinued for

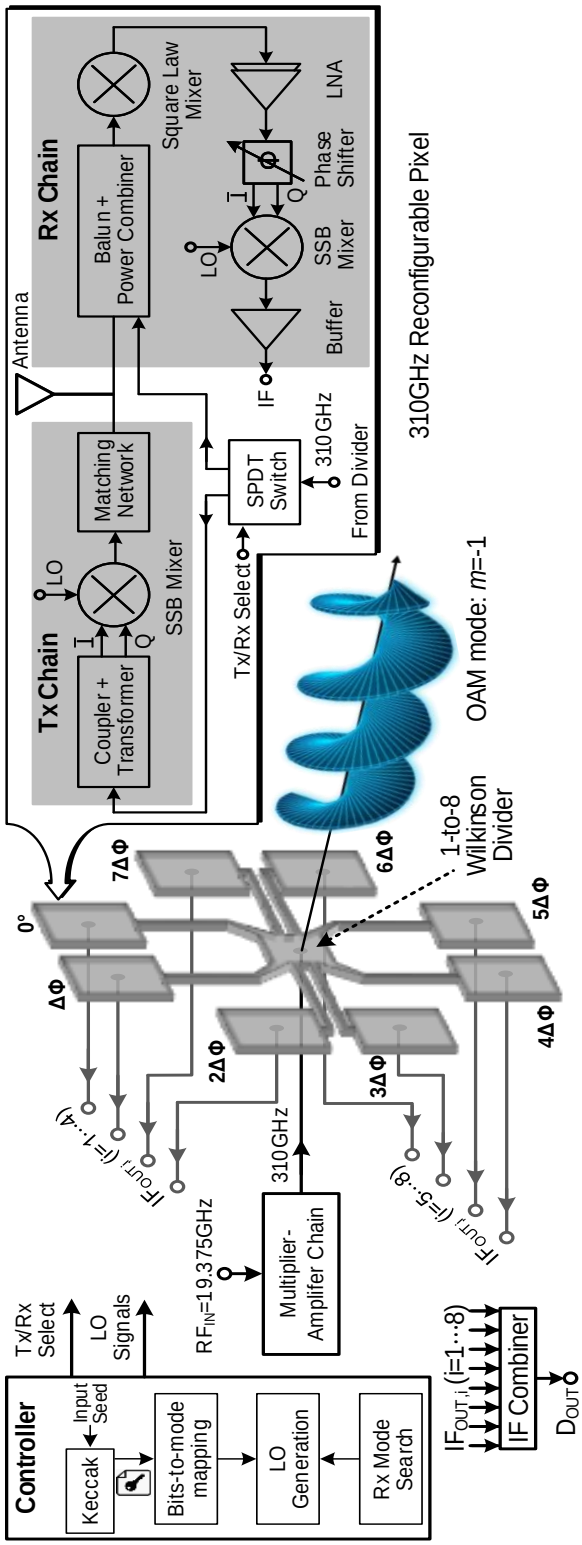
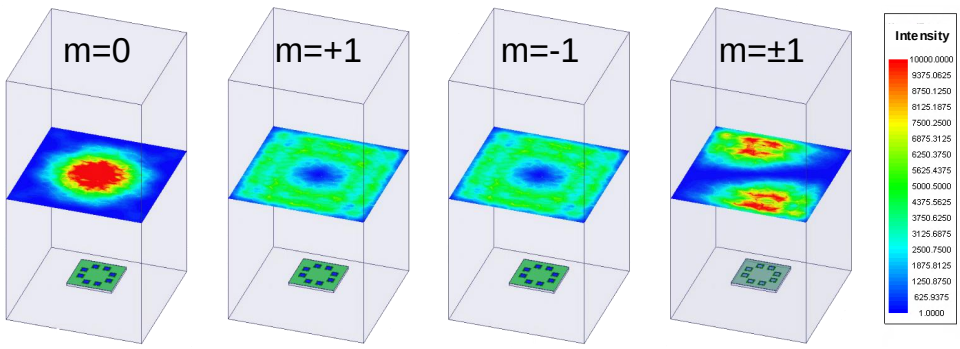
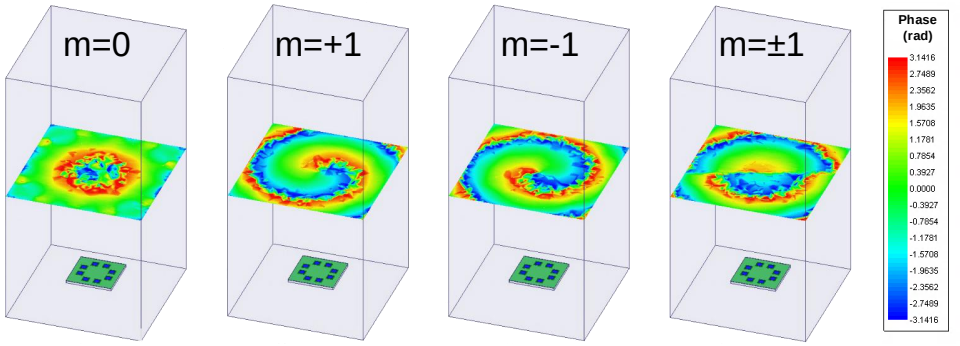


Figure 4-5: Architecture of the 0.31 THz-OAM transceiver in CMOS.



(a)



(b)

Figure 4-6: Simulated (a) intensity and (b) phase distributions for four OAM modes from a 310 GHz circular patch antenna array.

superposed mode; rather, it represents an intensity null along the diagonal.

The simulated radiation pattern of the antenna array is shown in Fig. 4-7. For the m=+1 mode, a sharp fall in the array directivity at the center is observed due to phase singularity. Note that it has a single donut-shaped lobe with a null in the center rather than two separate sidelobes. The sidelobes are ∼20 dB lower than the main beam for the array with a diameter of one wavelength λ in air. The radiation patterns for the antenna array with the diameters of 1.25λ and 1.5λ are also shown in the inset of Fig. 4-7 and their sidelobes are only ∼10 dB lower than the main beam. This is undesired because it makes the transmission more prone to eavesdropping. Therefore, a diameter of λ for the circular array is adopted in this design.

One major challenge of this antenna array is the distribution of 310 GHz signal to all the Tx and Rx chains with the exact same amplitude and phase which is required to maintain the fidelity of OAM modes. To this end, a modular design is adopted

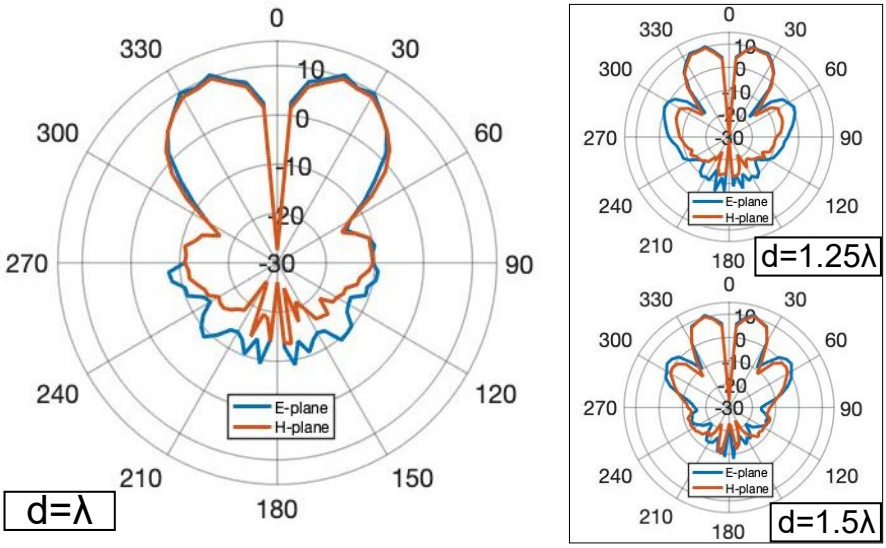


Figure 4-7: Simulated directivity for the circular antenna array with a diameter of λ for m=+1. The inset shows the radiation patterns for the diameters of 1.25λ and 1.5λ.

for the antenna array, where it is divided into four quadrants with two pixels in each as shown in Fig. 4-8. The 310 GHz signal is divided to eights pixel through a symmetric 1-to-8 Wilkinson power divider. The limited space requires the floorplan of two pixels in one quadrant to be different (see Pixel_a and Pixel_b in Fig. 4-8). The matching networks between different circuits are designed to have identical phase shifts. This is done by folding some transmission lines to match in both the pixels. In simulations, the amplitude and phase mismatches are negligible between the pixels. The distribution of 8 MHz LOs (from the controller to each pixel) also follows the same path though the phase coherence requirement, in this case, is much more relaxed. The power divider has a simulated insertion loss of 0.8 dB and is implemented using 2-μm-wide M9 metal traces.

4.2.2 Dual-feed Patch Antenna

To enable front-side radiation, each pixel integrates a patch antenna that is shared between the Tx and Rx chains. To realize such sharing, a square shape patch with two feeds is adopted, so that both feeds excite the same mode (TM_{100} in this case)

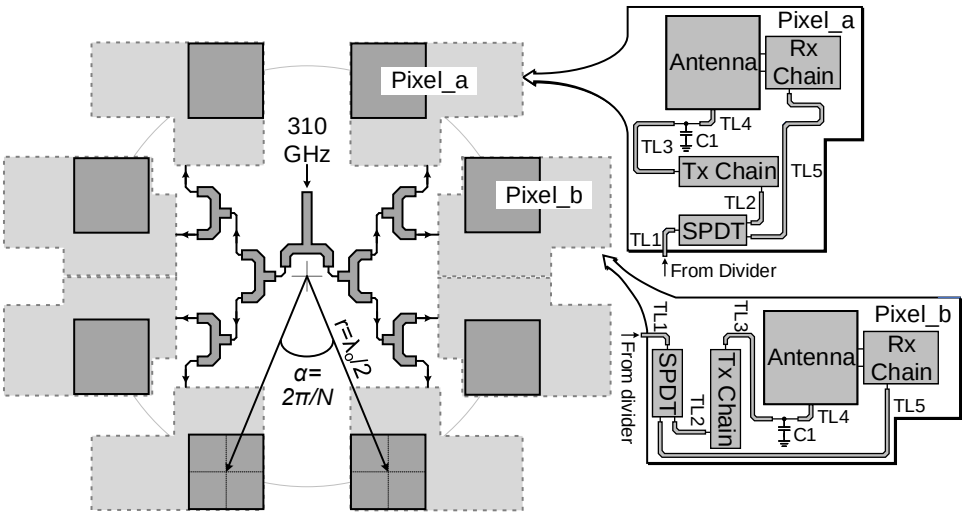
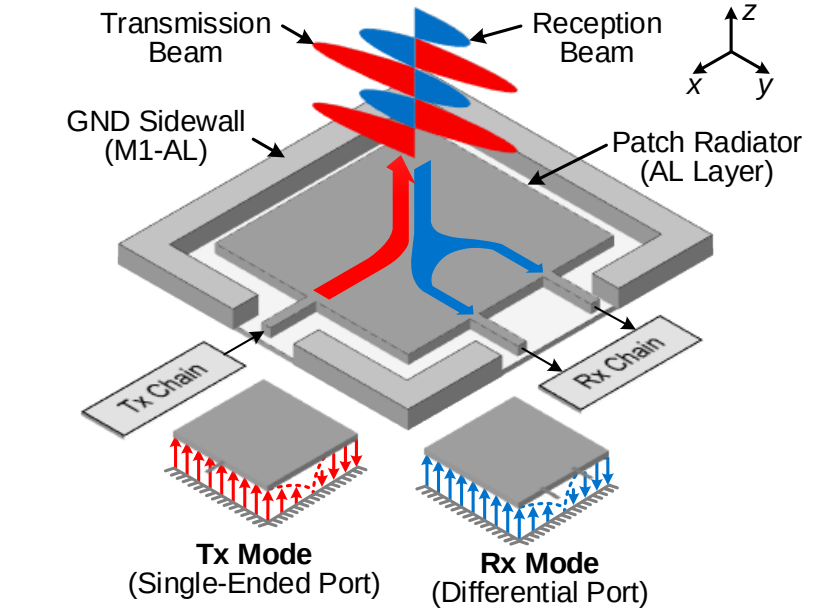


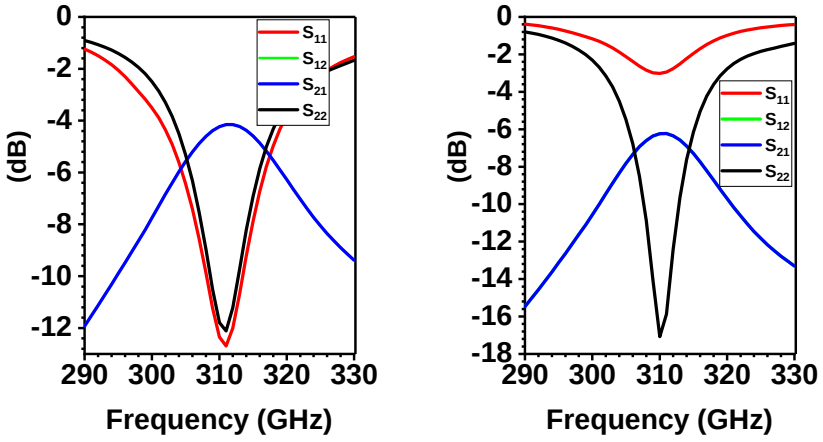
Figure 4-8: Floor plan of circular antenna array showing the phase-coherent distribution of 310 GHz signal to all the pixels. The arrangement of circuit blocks in the two pixels with matching networks is also shown, which avoids phase mismatch at the Tx antenna and the Rx mixer.

and have the same resonance frequency (∼310 GHz) [15]. As Fig. 4-9a indicates, to excite the TM_{100} mode, we can either use a differential feed symmetrically connected to the patch edge along the x-direction, or a single-ended feed connected to the center of the patch edge along the y-direction. Accordingly, the Tx chain has a single-ended output and the Rx chain has a differential input. This scheme ensures that both Tx and Rx have the same linear polarization and helps in avoiding phase ambiguity from the wavefront twist. When the chip is working in the Tx mode, both Tx and Rx ports are matched and this leads to Tx-Rx coupling as shown in Fig. 4-9b, causing a ∼2 dB loss in the radiated power. In the Rx mode, the Tx chain presents a high impedance to the antenna as its mixer is turned off and the Rx-Tx coupling is less as shown in Fig. 4-9c with a ∼1.3 dB loss in the received power. In future iterations, a patch antenna with two orthogonal single-ended feeds can be adopted that excites TM_{100} and TM_{010} modes in Tx and Rx modes respectively to mitigate Tx-Rx coupling.

Regarding the implementation of the patch antenna, its radiator uses the top aluminum (Al-pad) layer of the CMOS process and has a dimension of 218×218-μm^2. The ground plane of the antenna is made out of the M1-to-M2 layers (∼8-μm below the radiator) and there is no dummy metal filling between the radiator and the ground.



(a)



(b) (c)

Figure 4-9: (a) Schematic of multi-port patch antenna with the same excited mode (TM_{100}) for both Tx and Rx. Simulated s-parameters when (b) both Tx and Rx ports are matched, and (c) Tx presents high impedance and Rx port is matched.

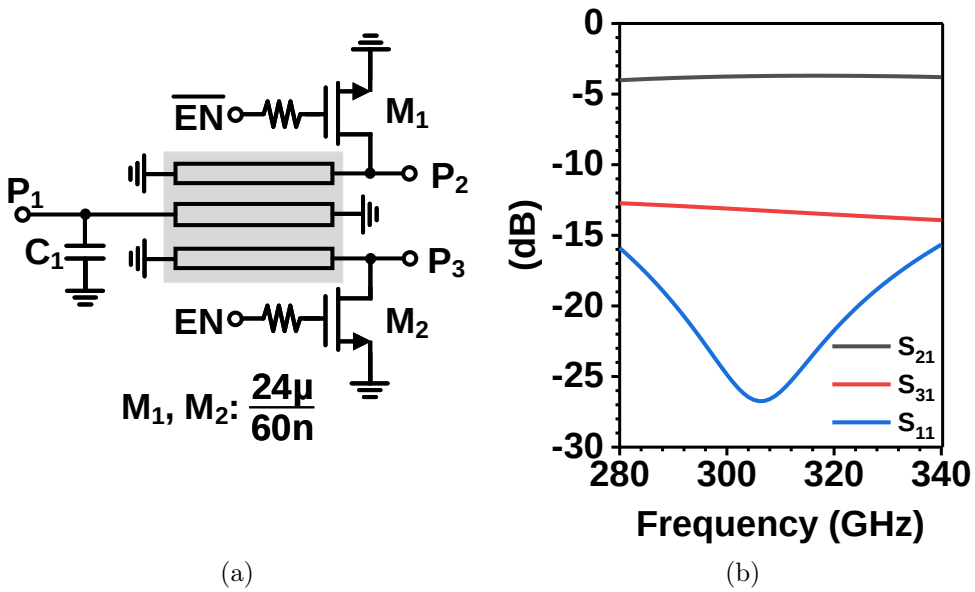
The antenna is also enclosed by a ground wall (M1-to-Al pad stack), which is 20-μm away from the patch on all sides. It reduces the coupling with neighboring electronics and antennas while having a negligible impact on the antenna performance. The square shape of the antenna also has a negligible impact on its performance. The peak directivity and radiation efficiency of the antenna in the HFSS simulation are 5 dBi and 37%, respectively. The antenna array has a peak directivity of 11 dBi for plane wave mode with the same radiation efficiency.

4.3 Design of the 310-GHz Reconfigurable Pixel

The block diagram of the THz-OAM pixel is shown in the inset of Fig. 2-4. The Tx/Rx mode selection is realized by a coupled-line-based SPDT switch [see Fig. 4-10a] [89], which directs the 310-GHz input to either Tx or Rx chain. As shown in Fig. 4-10b, the simulated insertion loss (S_{21}) and isolation (S_{31}) of the switch, when EN=1, are 3.8 dB and 15 dB, respectively. The coupled transmission lines are 40-μm long and are implemented on M9 with 5-μm width and 2-μm spacing. A capacitor C_1 $\approx$19 fF is required for input matching whereas the parasitic capacitance from the 24μm/60nm NMOS devices (M_1 and M_2) are included in the output matching. MOSFETs in the 65-nm bulk CMOS process have poor switching performance at THz frequencies; although a wider channel provides smaller ON-resistance, there is also a stronger coupling of THz signal from the channel to the LO wire through the gate-channel capacitance. To block such coupling, a set of 8-kΩ resistors are added in series with the transistor gates, which improves the switch insertion loss.

4.3.1 Design of the THz-OAM Transmitter Chain

The Tx chain consists of a coupler and a transformer for generating quadrature 310 GHz signals, followed by a single-sideband (SSB) mixer and an antenna matching network as shown in Fig. 4-11a. Compared to conventional high-frequency phase shifters, our mixer-based scheme offers precise phase control and phase-independent amplitude response, which are critical to the fidelity of the OAM wavefront. Although



(a) (b)

Figure 4-10: (a) Schematic of coupled-line-based SPDT switch. (b) Simulated insertion loss (S_{21}), isolation (S_{31}), and return loss (S_{11}) for the SPDT switch with EN=1.

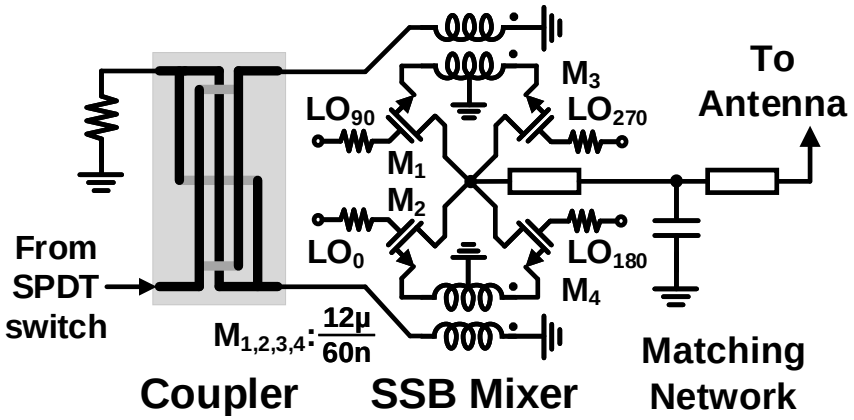
a double-sideband (DSB) mixer involves simpler hardware implementation, we note that the generated upper and lower sidebands are applied with opposite phases from the LO; in our OAM transceiver, therefore, their associated beams would have opposite OAM modes which is undesired. In our design, a SSB mixer based on passive quad switches is adopted to not only suppress the upper-sideband of the output but also to minimize the power consumption. The 8 MHz quadrature LO signals of the mixer are from a divide-by-4 static frequency divider dividing controller clock frequency. Although a divide-by-2 operation can also provide the 8 MHz quadrature LO signal, the additional availability of the LO phases (e.g., 45°, 135°, 225°, and 315°) provided in our divide-by-4 scheme are essential to generate the OAM modes. The phases of the RF and LO signals of the MOSFETs are arranged in the way that at the central current-summing node, the lower sidebands of all branches add up constructively, while the upper sidebands cancel. Through the selection of LO phases, the controller changes the THz output phase. Different OAM modes can then be generated from the array. Mode switching is realized by the data-driven selection of the LO phases. The mode switching speed, although limited by the LO frequency, is

sufficient for the transmission of a secret key (typically 256 bits).

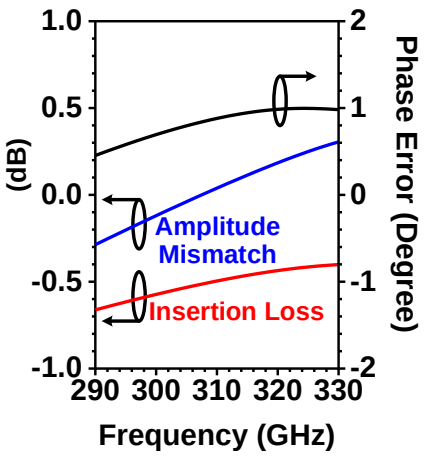
The coupler is implemented on the M8 layer with 2.5-μm width and 2-μm spacing. The simulated insertion loss, and amplitude and phase mismatches of the coupler are 0.5 dB, 0.1 dB and 0.8°, respectively, as shown in Fig. 4-11b. The single-loop center-tap transformer is implemented on the M9 layer with 3-μm width and 3-μm spacing. The simulated insertion loss, and amplitude and phase mismatches of the transformer are 1.3 dB, 0.1 dB and 0.3°, respectively, as shown in Fig. 4-11c. In Fig. 4-11d, we show the EM-circuit co-simulation results of the entire Tx chain. An overall conversion loss of 14 dB is achieved at f_{RF}=310 GHz, at the expense of zero static DC power. The module also effectively suppresses the components at $f_{RF}+f_{LO}$ and $f_{RF}\pm 2f_{LO}$. The component at $f_{RF}+3f_{LO}$, due to its constructive summation at the mixer output node, appears at the output spectrum, with a 10 dB rejection ratio. This component is $4f_{LO}$ away from the required f_{RF}-f_{LO} component and is filtered at the IF output of the Rx. In future iteration, this may be improved by adopting a polyphase N-path mixer structure.

4.3.2 Design of the THz-OAM Receiver Chain

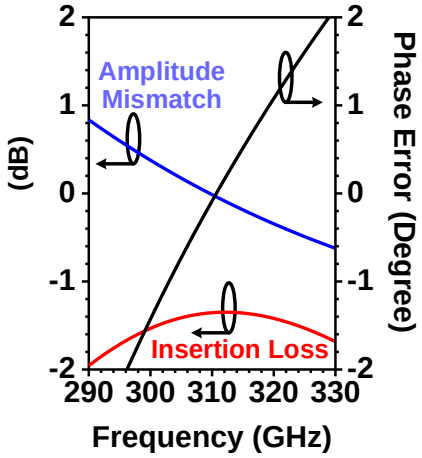
The schematic for the Rx chain is shown in Fig. 4-12a. For chip compactness, the receiver mode uses the same antenna, where the input wave is extracted through differential feeds along the antenna H-plane [see Fig. 4-9a]. Since the operation frequency of our transceiver has exceeded the transistor speed limit of the 65-nm CMOS process used here (f_{max} ≈280 GHz), a pre-amplifier in the RX front-end would not be possible. Hence, an active-mixer-first architecture is adopted. A balun converts the differential received signal to a single-ended signal, which combines with the SPDT-directed 310 GHz signal in a Wilkinson combiner. The 310 GHz signal now behaves as a THz LO that down-converts the received signal inside a MOSFET-based square-law mixer. The generated IF signal, carrying the same phase as the local input wave, is then amplified and undergoes a phase-shifting process inside a SSB mixer (for the same reason as that in the transmission mode). When such a phase shift compensates the OAM phase gradient $\Delta\phi$ among the THz pixels, all IF outputs become



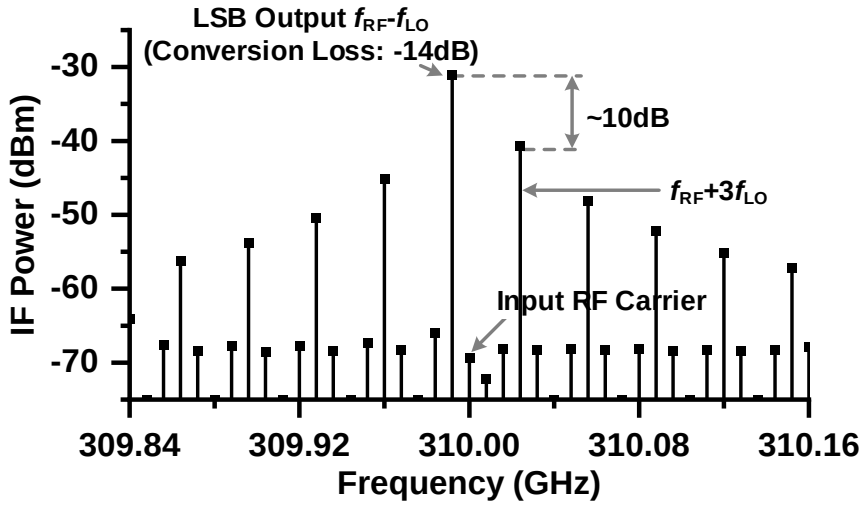
(a)



(b)



(c)



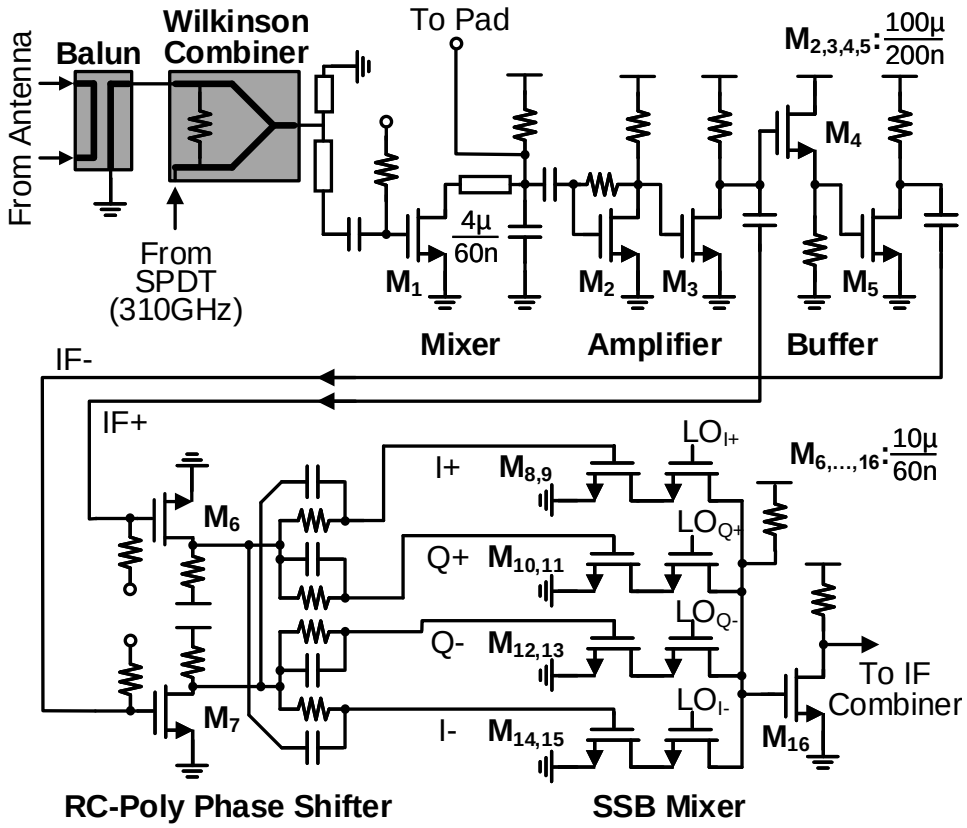
(d)

Figure 4-11: (a) Schematic for Tx chain including coupler, transformers, SSB mixer and matching network. (b) Simulated insertion loss and output mismatch of the coupler. (c) Simulated insertion loss and output mismatch of the transformer. (d) Simulated output spectrum of the Tx chain with a -16 dBm RF input (f_{RF}=310 GHz) and quadrature LO signals at f_{LO}=8 MHz.

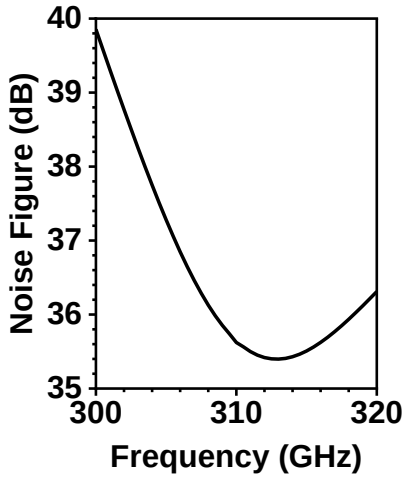
in-phase. The IF combiner in Fig. 2-4 then adds them constructively and provides D_{OUT} as an indicator of whether the incident wave matches the currently selected OAM mode. For simultaneous detection of multiple OAM modes, the pixel IF signals can be directly extracted through pads, amplified and digitized using ADC. Then, relative phase shifts can be determined by digital processing.

A return-path-gap (RPG) based balun similar to the one presented in [90] is used. It consists of two microstrip lines coupled via a slot in the ground plane (i.e. RPG). The RPG slot, closed by four quarter-wavelength slot resonators in the ground plane, only allows transmission (hence input-output coupling) of a quasi-TE-mode wave, which is excited by a differential signal in the input microstrip lines. The simulated insertion loss for the differential mode is ∼1 dB. The balun is implemented using 2-μm-wide M9 microstrip lines and slots in a shunted M1-to-M3 ground. The mixer is based on a NMOS device (4μm/60nm) with drain bias and sub-threshold gate bias (V_G=0.3V < V_{th}). This topology yields lower conversion loss as compared to a passive mixer (without drain bias) but degrades the noise figure due to flicker noise [41]. Therefore, a R-C high pass filter is added between the mixer and baseband amplifier to suppress the low-frequency noise. In the simulation, the mixer has input P_{1dB} of -5.2 dBm, which is much higher than the LO power (∼-16 dBm). The non-linear down-conversion process is highly dependent on LO power and low LO power (due to the distribution of LO from one active path) gives higher conversion loss. As a result, in the simulation, the SSB NF of the receiver is 36 dB at 310 GHz [see Fig. 4-12b].

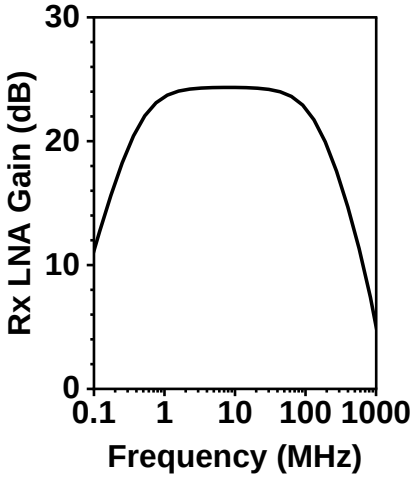
Following the mixer is a two-stage, self-biasing baseband amplifier, which has 3.2-nV/Hz$^{1/2}$ simulated input-referred noise (lower than the mixer output noise), enables an overall conversion gain of 24 dB for the receiver chain [see Fig. 4-12c]. To generate the IF I-Q signals for the SSB mixer, a set of broadband and compact R-C polyphase filters (PPF) are adopted. The SSB mixer uses the same LO signals that are employed in the Tx chain. In simulation, the SSB, including the R-C PPF, has a conversion loss of 12 dB.



(a)



(b)



(c)

Figure 4-12: (a) Schematic for the Rx chain. (b) Simulated receiver NF. (c) Simulated gain of the baseband amplifier.

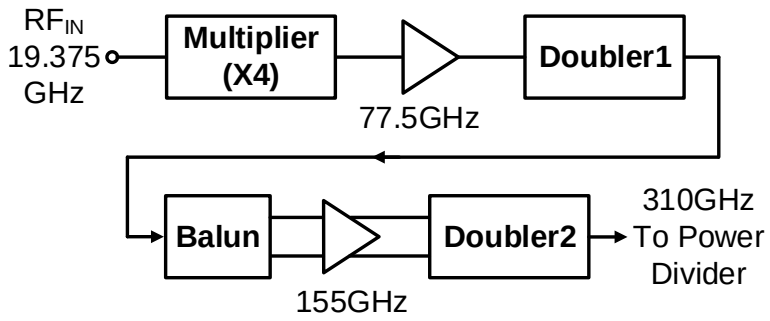
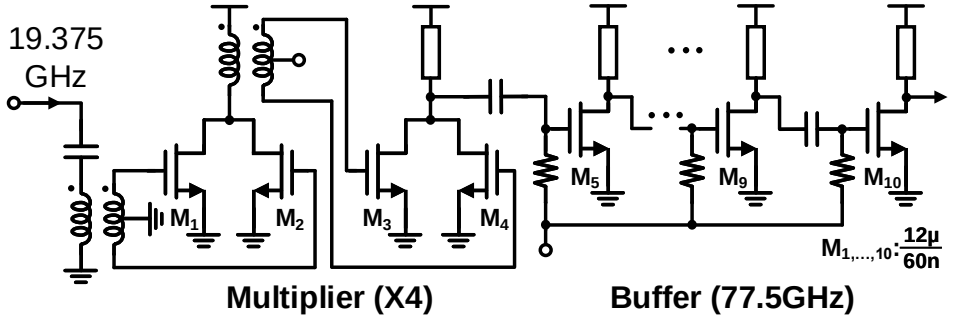


Figure 4-13: Block diagram of the 310-GHz multiplier-amplifier signal source.

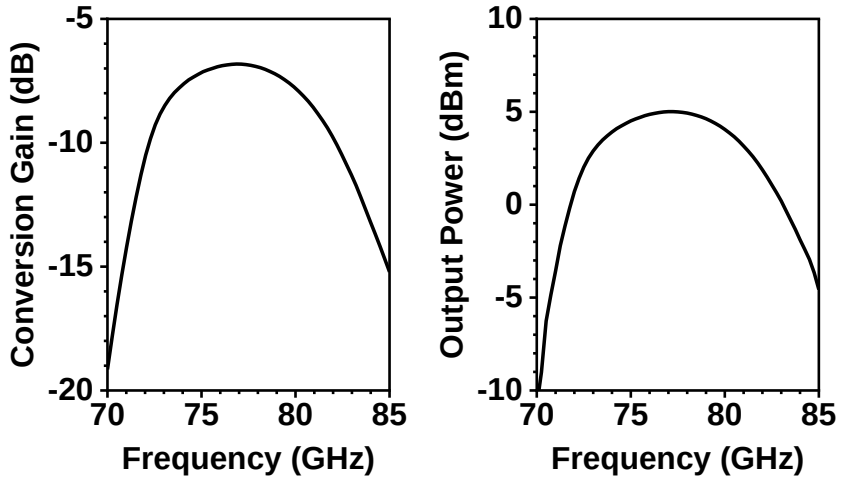
4.4 Design of the 310 GHz Multiplier-Amplifier Chain

The 310 GHz multiplier-amplifier signal source is shown in Fig. 4-13 (a similar design is reported earlier in [91]). At the input of the frequency conversion daisy chain, two push-push frequency doublers that are cascaded through a transformer are used to convert the input signal at 19.375 GHz to 77.5 GHz as shown in Fig. 4-14a. In simulation, the conversion gain of two doublers is -6.8 dB [see Fig. 4-14b], and the output power after the buffer is $\sim$5 dBm [see Fig. 4-14c]. The schematic of Doubler 1 is shown in Fig. 4-15. The millimeter-wave signal from the frequency conversion chain drives a common-source buffer (M_1) and is then turned into differential mode through a single-loop transformer (TF_1). A push-push structure is then used to generate the second-harmonic component while suppressing the tone at the input frequency. As shown in Fig. 4-15b and Fig. 4-15c, the peak conversion gain and output power of Doubler 1 are -3.4 dB and 1.5 dBm, respectively. The simulated DC power of the entire circuit in Fig. 4-15 is 21 mW.

As shown in Fig. 4-13, before the second frequency-doubling, the signal from Doubler 1 is converted to differential mode using a balun and is boosted by a chain of amplifiers [see Fig. 4-17a]. Since the amplifiers are based on a pseudo-differential topology with a neutralization technique (details to be given next), they are sensitive to any amplitude and phase imbalance of the input signal. To minimize such imbalance, a sub-THz balun structure based on a pair of folded slot resonators. As shown in Fig. 4-16, the balun input and output consist of a single-ended microstrip line and a pair of differential microstrip lines, respectively. A gap in the ground plane

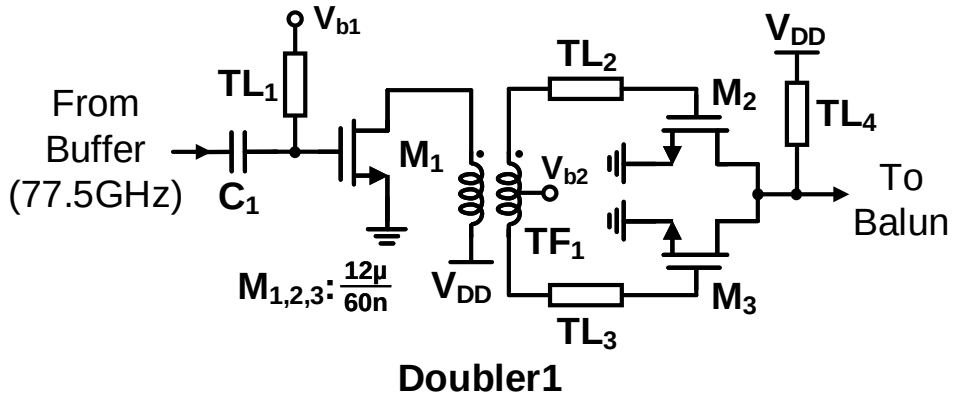


(a)

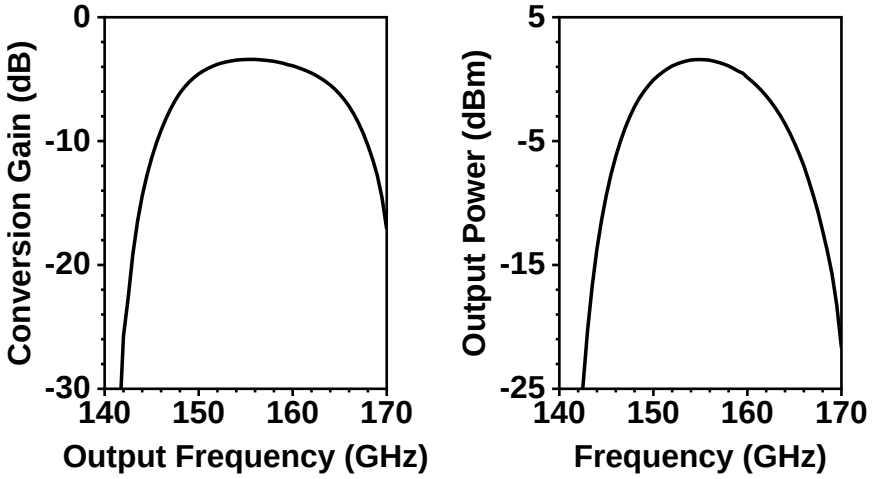


(b) (c)

Figure 4-14: (a) Schematic of the input multiplier (×4) and buffer. (b) Simulated conversion loss of the input multiplier with P_{in}=6 dBm. (c) Simulated output power of the buffer.



(a)

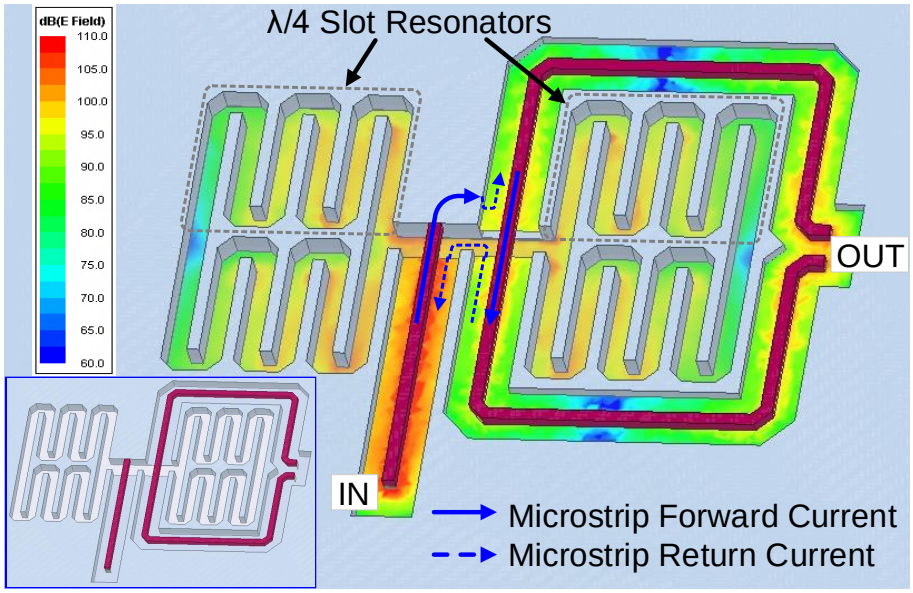


(b) (c)

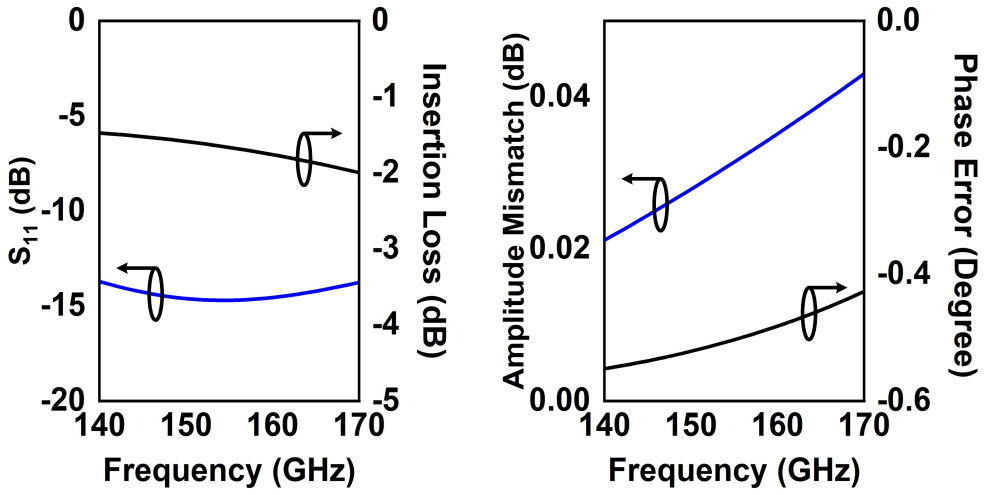
Figure 4-15: (a) Schematic of Doubler 1. (b) Simulated doubler conversion gain at varying output frequency (the input power variation from the preceding circuitry is also included). (c) Simulated doubler output power.

couples the input and output; it is also enclosed by two pairs of quarter-wavelength slot resonators which present high impedance on the two ends of the ground gap. The resonators are folded for compact size and minimum radiative loss. With the excitation by the single-ended signal in the input microstrip, only a fully-differential quasi-TE mode wave is allowed in the ground gap. Meanwhile, since the microstrip pair and the slot resonators at the output side are completely symmetric, when the above quasi-TE wave is coupled back to microstrip mode, the generated output signals are expected to keep perfect out-of-phase balance across a wide range of frequencies. Full-wave EM simulation shows that the insertion loss of the balun is 1.3 dB and the amplitude/phase imbalance is negligible.

The signal generated by the slot balun is then amplified by three identical, pseudo-differential amplifier stages, shown in Fig. 4-17a. The stages are coupled through central-tapped transformers. In each stage, a cross-coupled capacitor pair is used to create negative capacitance that cancels the C_{gd} of the transistors. Although this neutralization scheme does not provide the highest possible gain, the device unilaterization that this scheme enables allows for higher stability and broader bandwidth. The simulated gain of the amplifier chain is shown in Fig. 4-17b, with an average value of $\sim$7 dB in the 150$\sim$160 GHz band. Finally, the signal is frequency doubled again by a pair of push-push transistors (M_3 and M_4). The common node of TL_1 is a virtual ground for the differential 155-GHz signals, whereas it is matched to the output for the in-phase 310-GHz signals. The inductive reactances provided by transmission lines TL_1 (slightly shorter than $\lambda/4$) resonate with the parasitic capacitances of the NMOS devices at 155 GHz. This boosts the swing of the device drain voltages (hence higher device non-linearity). TL_2 is used as part of the output matching network and helps in extracting the 310 GHz signal through a DC isolation capacitor. In simulation, the amplifier chain and Doubler 2 consume DC power of 57 and 24.8 mW, respectively, and the final TX output power (as shown in Fig. 4-17c), is $\sim$-1.6 dBm at 310 GHz.

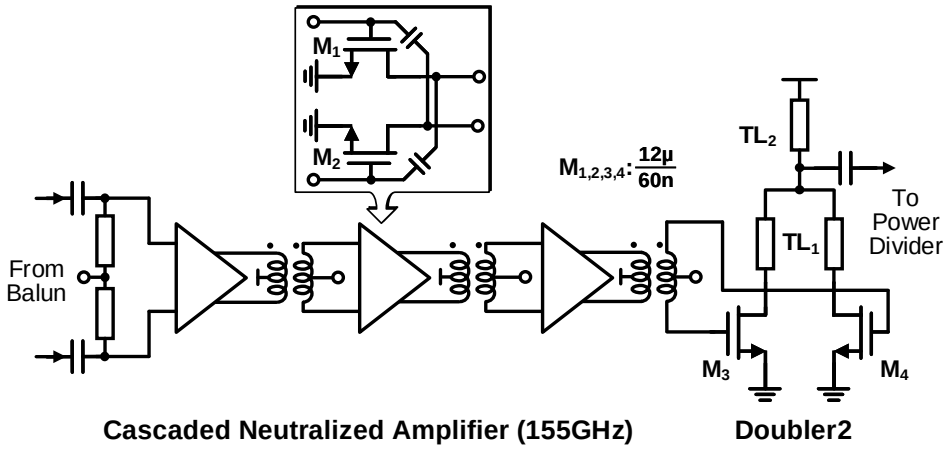


(a)

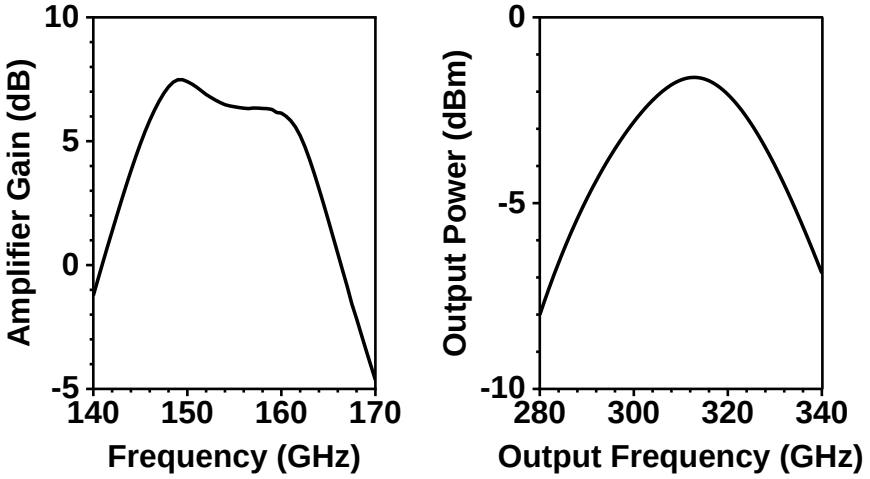


(b) (c)

Figure 4-16: (a) Simulated electric-field distribution of the 155 GHz slot-based balun with the 3D structure shown in the inset. (b) Simulated insertion loss and return loss (S_{11}). (c) Simulated amplitude and phase imbalance at the differential outputs.



(a)



(b) (c)

Figure 4-17: (a) Schematic of Doubler 2 and its input amplifier. (b) Simulated gain of the cascaded neutralized amplifier chain (the input power variation from the preceding circuitry is also included). (c) Simulated output power of Doubler 2 with an input power of +5 dBm.

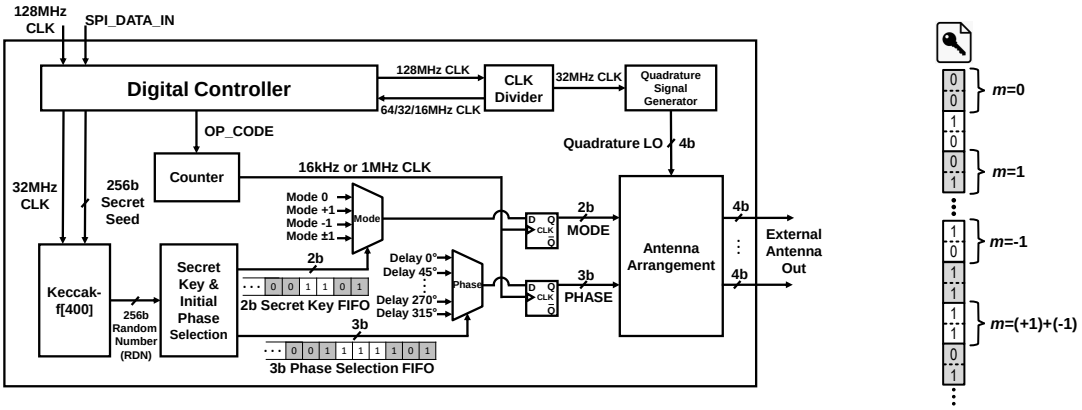
4.5 Controller and OAM Mode Mapping

The system-level architecture of the pseudorandom key generation and the OAM modulation controller is shown in Fig. 4-18a. The high-level protocol flow is as follows.

- A secret seed for key generation and an opcode are transferred into the chip through SPI. The controller operates with a global clock of 128-MHz frequency and divides it into different local clocks of 16, 32, and 64 MHz.
- Keccak-f[400] takes a 256-bits secret seed and generates a 256-bits pseudorandom number which is converted into a secret key and phase selection bits. Each 2 bit of the secret key corresponds to one OAM mode, while each 3 bit of phase selection corresponds to one initial phase distribution. The frequency of OAM modulation achieves up to 1 MHz, while the Keccak operates with the 32-MHz clock.
- A quadrature LO is generated from the local clock, and the antenna arrangement block changes the THz output phase, generating different OAM modes from the antenna array based on the current mode and the phase distribution selection. The LO frequency is programmable between 16 kHz and 32 MHz with a nominal value of 8 MHz.

4.5.1 OAM Mode and Phase Selection Algorithm

Fig. 4-18b shows how the key is mapped to OAM modes. Every 2 bit (00, 01, 10, and 11) represents different OAM modes (m=0, +1, -1, $\pm$1). In order to increase the security of the modulation scheme, 8 different phase patterns (with 45° difference) are randomly assigned to each mode. In the superposed mode (m=$\pm$1), there exists a low-power area (null) due to the out of phase beams. By randomly switching between initial phases and hence different phase patterns, ambiguity increases manifold for eavesdroppers. However, random initial phases won't affect the reception by a legitimate receiver aligned to the beam axis.



(a) (b)

Figure 4-18: (a) Controller architecture for pseudorandom key generation and OAM modulation. (b) Mapping between the bits of secret key and the OAM modes.

4.5.2 Pseudorandom Number Generation

Keccak-f[400] is a SHA3 cryptographic core and is used for pseudorandom number generation [92]. The Keccak algorithm, commonly referred to as a sponge construction, supports two operations: absorb and squeeze. Keccak state can be divided into rate and capacity components with the former determining throughput while the latter determining the security level. Keccak-f[400] implementation is used from [93] which uses a 400-bit internal state. The rate and capacity sizes are set to 128 and 272 bits, respectively.

In order to represent a 128-bit secret key, it requires a 64-long (128-bit/2-bit) OAM mode sequence. Each mode has eight different phase patterns ($45\times m$ of phase change, m=0, $\cdots$, 7) so that another 192-bits (64 $\times$ 3-bits) random sequence is mandatory. The Keccak-f[400] block is exploited as a source of raw entropy to generate random bits at a clock frequency of 32 MHz. However, Keccak could only produce 256-bits while we require 320 (128-bits for secret key and 192-bits for random phase pattern) random bits. Thus, we assigned the first 128-bits secret key. Then, the first 196-bits (most significant (MSB) 196-bits) is XOR-ed with the next 196-bits (least significant (LSB) 196-bits) to generate phase pattern selection bits.

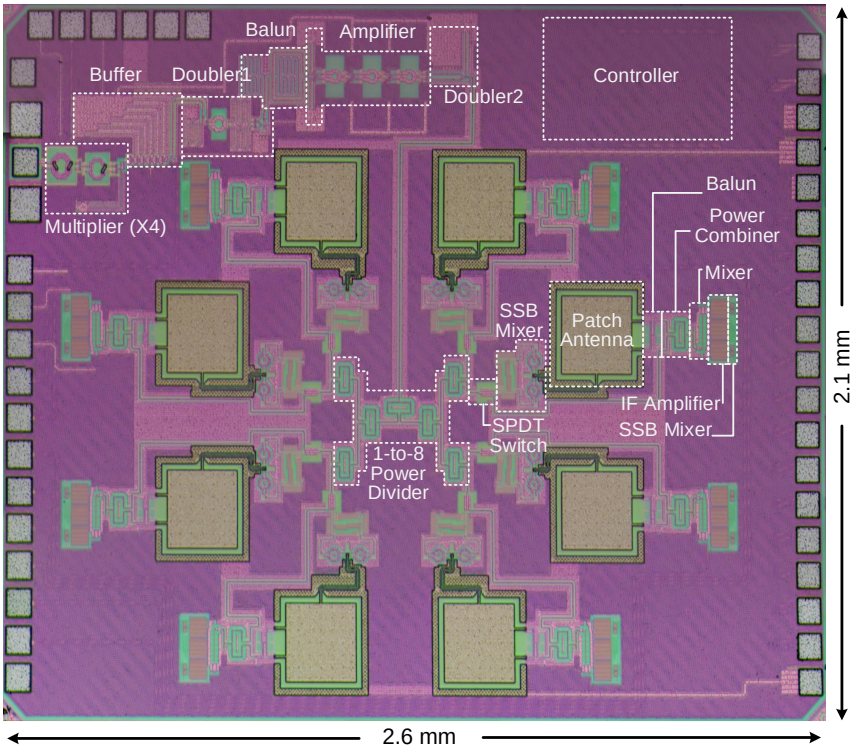


Figure 4-19: Die photograph of the 0.31 THz OAM CMOS chip.

4.6 Experimental Results

The THz-OAM transceiver is fabricated in a TSMC 65-nm bulk CMOS process and its die photograph is shown in Fig. 4-19. The chip occupies an area of 2.1×2.6 mm^2. The measured total DC power consumption by the chip is 154 and 166 mW in the Tx and Rx modes, respectively. The breakdown of power consumption of different components is shown in Fig. 4-20.

4.6.1 Characterization of the Transmitter Mode

The measurement setup for the characterization of Tx mode of the chip is shown in Fig. 4-21a. Given the relatively large divergence of the OAM beam (due to the central null), a detachable low-cost TPX polymethylpentene lens (diameter=25.4 mm, focal length=10 mm) is placed at the front side of the chip to collimate the beam [see Fig. 4-21b]. The lens has a measured gain of ∼20dB. A SPP is used to convert a plane wave to OAM modes and vice versa, by introducing a linear phase variation along

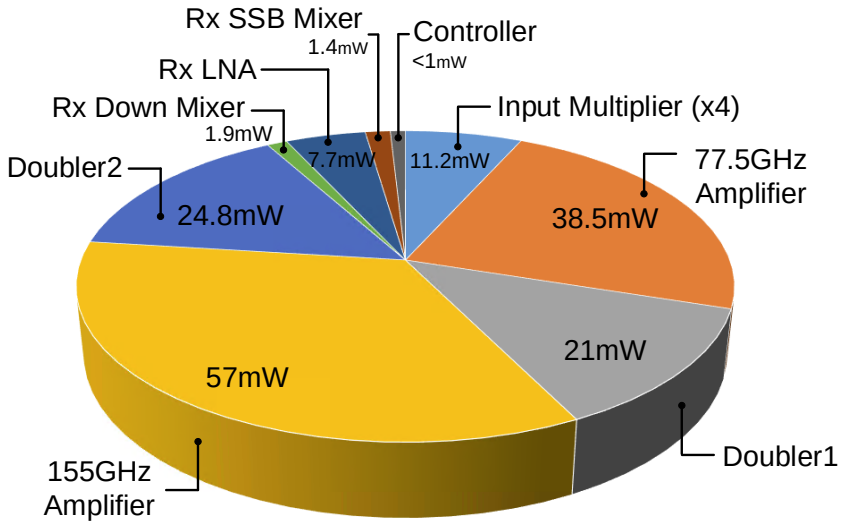


Figure 4-20: Breakdown of the measured power consumption of the chip.

the azimuth direction. A custom-designed THz SPP is 3-D printed using polylactic acid (PLA) material, as shown in the inset in Fig. 4-21b. The total height of SPP is given by the following equation:

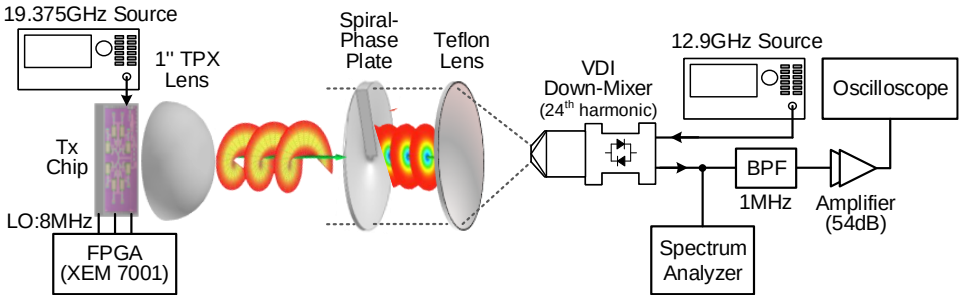
$$h = h_o + h(\phi) = h_o + \frac{m\lambda_o\phi}{2\pi(n - n_o)} \tag{4.3}$$

where m is the OAM mode, λ_o is the wavelength in air, $\phi \in [0, 2\pi)$, and n is the refractive index. The relative dielectric constant of PLA obtained from the vendor's datasheet is 2.5, and hence, n=1.58. This gives ramp height $h(2\pi)$ of 1.68 mm for m=+1 and -1 modes. The base height h_o is chosen to be 4.45 mm, which gives a measured loss of 12 dB.

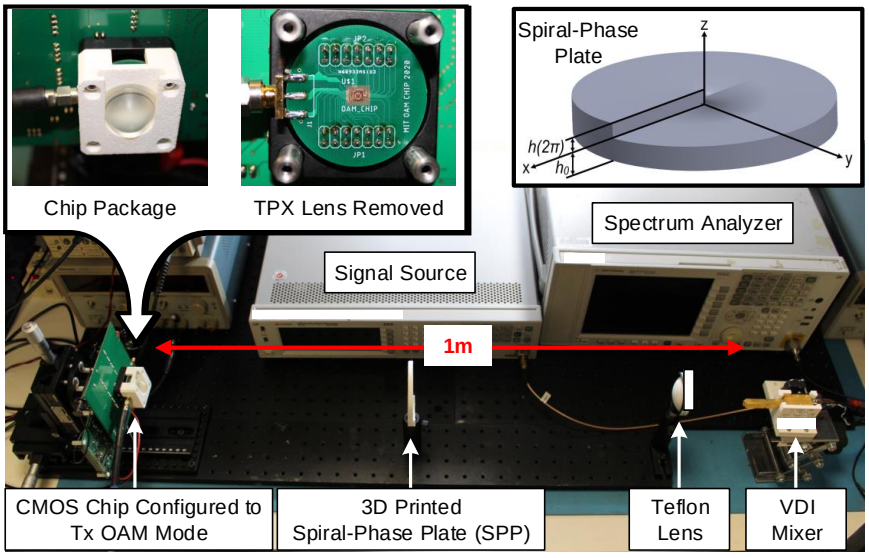
First, the radiated power of the OAM array is measured by configuring the chip to generate a plane wave (m=0 mode), and by placing a VDI WR-3.4 sub-harmonic mixer with an internal amplifier (combined conversion loss ~0 dB) and a feed horn 25 cm away. The corresponding EIRP is determined by Friis equation [47] as

$$EIRP = P_{IF} + CL_M - G_R + 20\log\left(\frac{4\pi R^2}{\lambda}\right), \tag{4.4}$$

where P_{IF} is the measured IF signal power, CL_M is the conversion loss of the mixer,



(a)



(b)

Figure 4-21: (a) Diagram of the experimental setup for transmission mode characterization. (b) Photograph of the test setup. Rx is at a distance of 1 m from the transmitting chip, and a SPP is placed in between. The insets show the chip package with and without the lens and the structure of SPP.

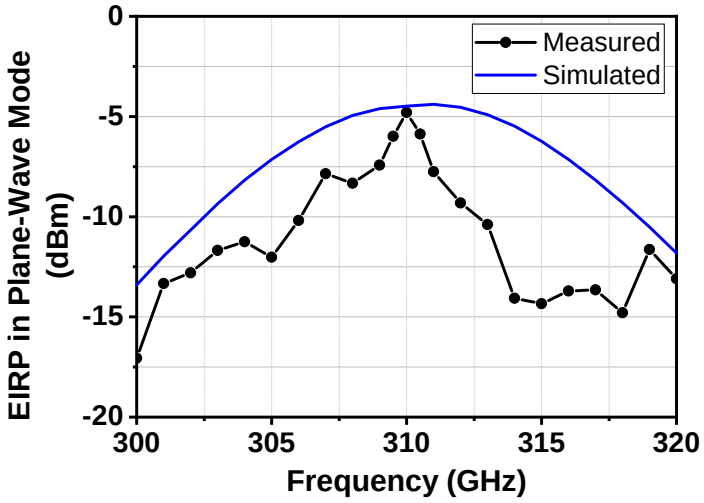


Figure 4-22: Measured EIRP for plane wave mode (m=0). Since the non-zero OAM modes have null in the center, EIRP is not well defined for such modes.

G_R is the feed horn gain (26 dBi), R is the distance between the Tx and Rx and λ is the wavelength. The peak measured EIRP of the chip is -4.8 dBm as shown in Fig. 4-22. Next, the VDI receiver is mechanically scanned across a 2D plane facing the chip in order to measure the wavefront intensity distribution of the chip output. The results in Fig. 4-23 show the expected null at the center of the m=+1 OAM mode. Our chip also enables and utilizes the superposition of the m=+1 and -1 modes, and the measured intensity plot in Fig. 4-23 presents the expected standing peaks and nulls as the result of the summation of the two counter-rotating wavefronts.

Direct measurement of phase spatial distribution is challenging due to the required μm-level Rx position precision at THz frequency; instead, the setup shown in Fig. 4-21 is adopted, where a SPP is placed in front of the VDI receiver and serves as a "mode filter" by converting the input with matched OAM mode into a plane wave. For different combinations between OAM modes of the transmitting array and the configuration of Rx SPP (m=+1 or -1), the VDI receiver output power is recorded in TABLE 4.1. The measured spectra for the highlighted rows in TABLE 4.1 are shown in Fig. 4-24, showing 17 dB difference between the matched and unmatched cases, indicating the purity of OAM modes generated by the chip. Note that, when the Rx has no SPP and when the Tx mode is non-zero, ideally, the Rx output power should

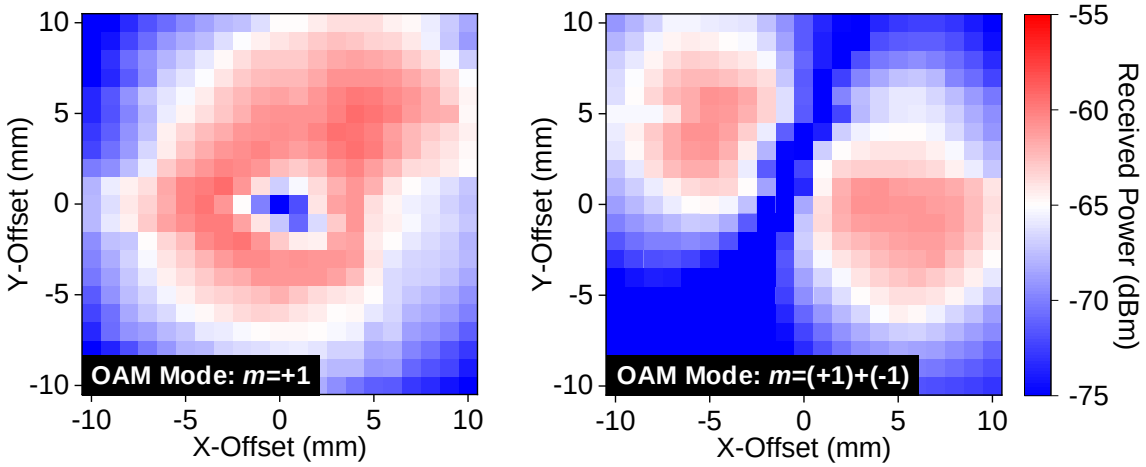


Figure 4-23: Measured intensity distribution for OAM modes m=+1 and m=(+1)+(-1) (superposition).

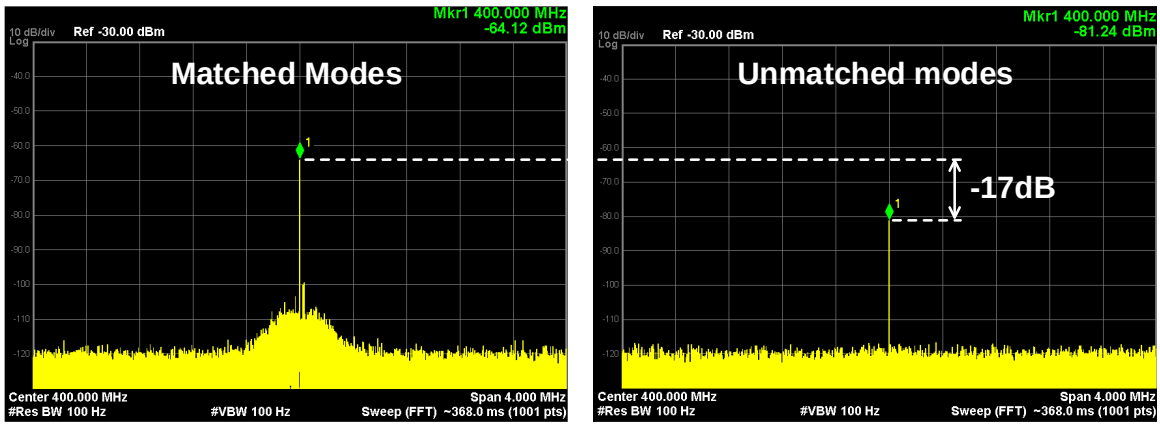


Figure 4-24: Tx OAM mode-checking: a 17-dB difference in IF power is measured when the Tx mode is +1 and the Rx SPP is +1 (matched) and -1 (unmatched).

be low, but any off-axis misalignment of the OAM array will get the Rx antenna to point at a non-zero portion of the OAM wavefront, resulting in non-negligible received power. It should also be noted that the P_{RX} values in the table include the SPP loss except for the “No SPP" case.

In order to demonstrate the dynamic switching among OAM modes, the chip output mapped from a repeated 1-Mb/s Keccak-generated data sequence is verified, and the time-domain outputs of the Rx with different SPP configurations are shown in Fig. 4-25. It shows good correlation with matched modes, partial correlation of the m=+1 or m=-1 modes with the m=(+1)+(-1) superposition mode, as well as the rejection of unmatched modes. Note that in Round 2 and 3, the amplitude is lower

Table 4.1: Tx Mode Checking

Tx Mode	Rx SPP	P_{RX} (dBm)
0	No SPP	-50
0	+1	-69
0	-1	-70
+1	No SPP	-58
+1	+1	-64
+1	-1	-81
-1	No SPP	-58
-1	+1	-80
-1	-1	-64
±1	No SPP	-76
±1	+1	-68
±1	-1	-67

than that in Round 1. This is due to the additional loss from the SPP. The presence of superposed mode with random initial phases increases the difficulty of eavesdropping by randomly posing intensity nulls to the eavesdropper; though at the expense of higher error probability for the legitimate receiver as can be seen in Fig. 4-25. Note that demonstrated 1-Mb/s data rate is for the intended application of transmission of the secret key and not the maximum achievable data rate of the proposed RF front-end architecture.

4.6.2 Characterization of the Receiver Mode

To test the reception mode of the chip, a VDI WR3.4 source (P_{out}=-5 dBm) is used. With a SPP inserted (see Fig. 4-26), the setup becomes an OAM mode generator. For different combinations between the configuration of Tx SPP (m=+1 or -1) and OAM modes of the receiving array, the combined IF power is recorded in Table 4.2. The chip shows >10 dB rejection when the OAM modes on the two sides are unmatched for all combinations of the modes. One example is shown in Fig. 4-27, when the VDI Tx is always in m=+1 mode, whereas the chip detection mode is configured to m=+1

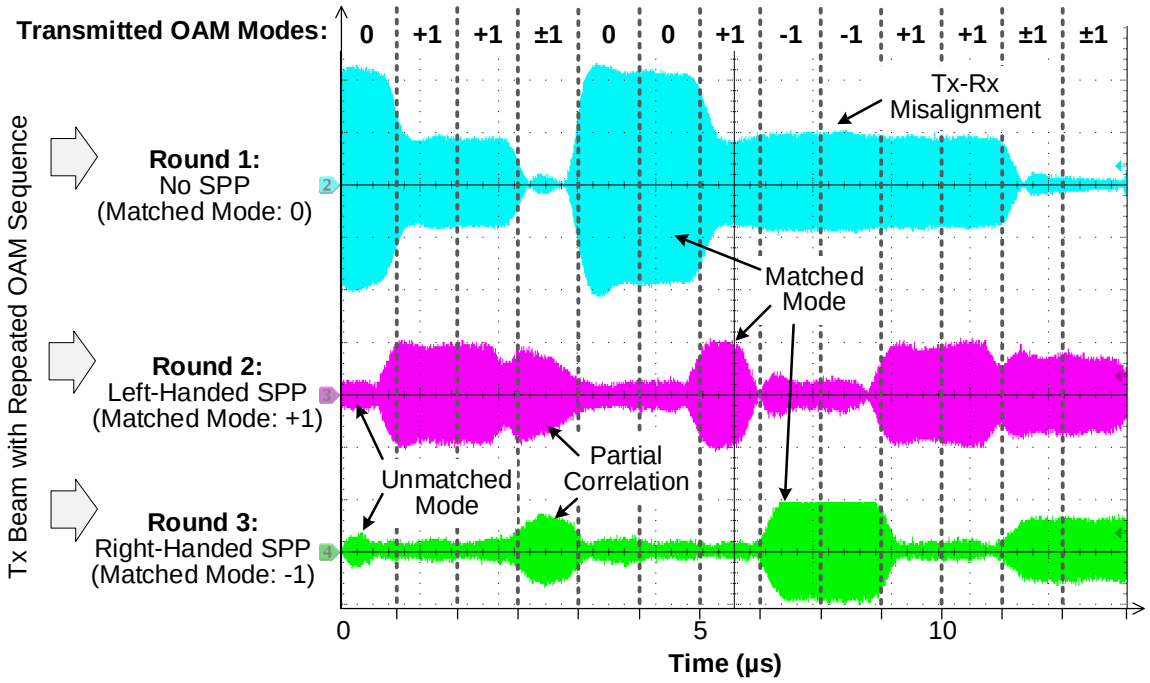


Figure 4-25: Time-domain output of the receiver configured to respond to different OAM modes when it is illuminated by the same OAM sequence generated by on-chip Keccak.

and m=-1, respectively, and rejection is 12 dB. The measured conversion loss of the chip for plane wave (m=0) is ∼30 dB as shown in Fig. 4-28. The LO distribution network for the Rx chain seems shifted upwards resulting in lower LO power input to the down-conversion mixer at the lower frequency end. This explains the discrepancy between the simulation and measurement results.

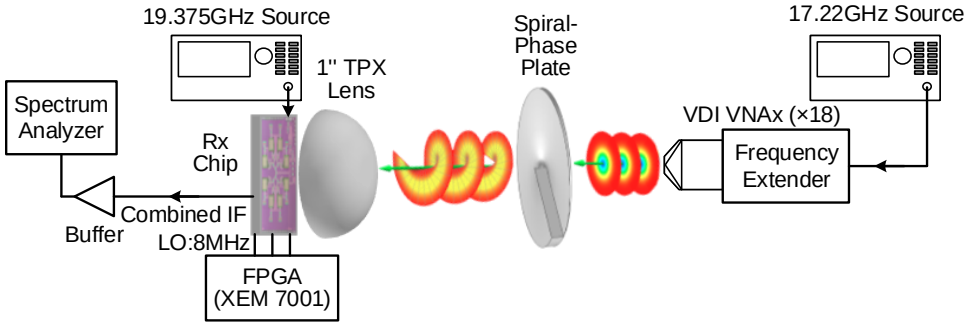


Figure 4-26: Diagram of the experimental setup for receiver mode characterization.

Table 4.2: Rx Mode Checking

Tx SPP	Rx Mode	P_{IF} (dBm)
No SPP	0	-64
No SPP	+1	-74
No SPP	-1	-75
No SPP	±1	-74
+1	0	-89
+1	+1	-78
+1	-1	-90
+1	±1	-84
-1	0	-91
-1	+1	-89
-1	-1	-78
-1	±1	-85

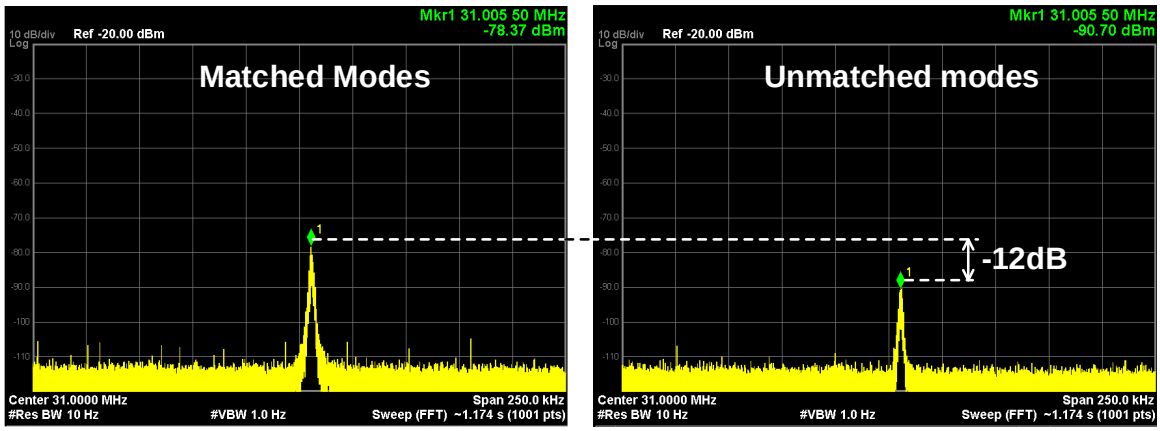


Figure 4-27: Measured spectrum of combined IF in Rx mode when Tx SPP is +1, and Rx mode is +1 (matched) and -1 (unmatched).

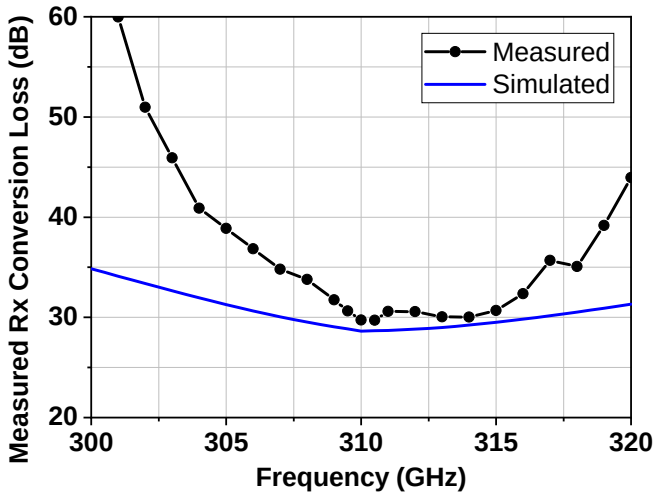
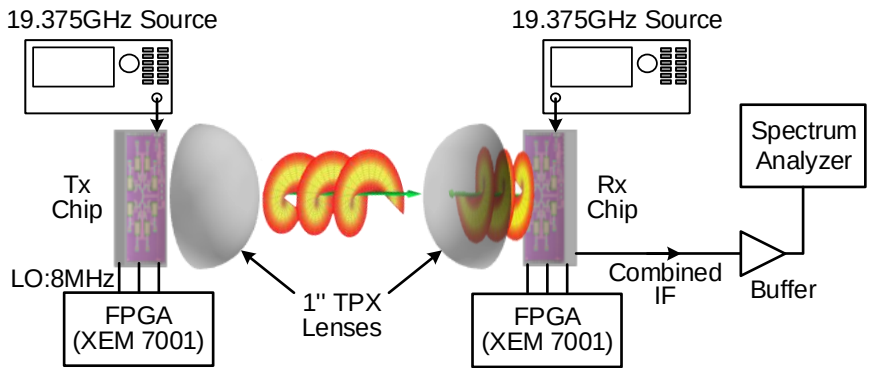


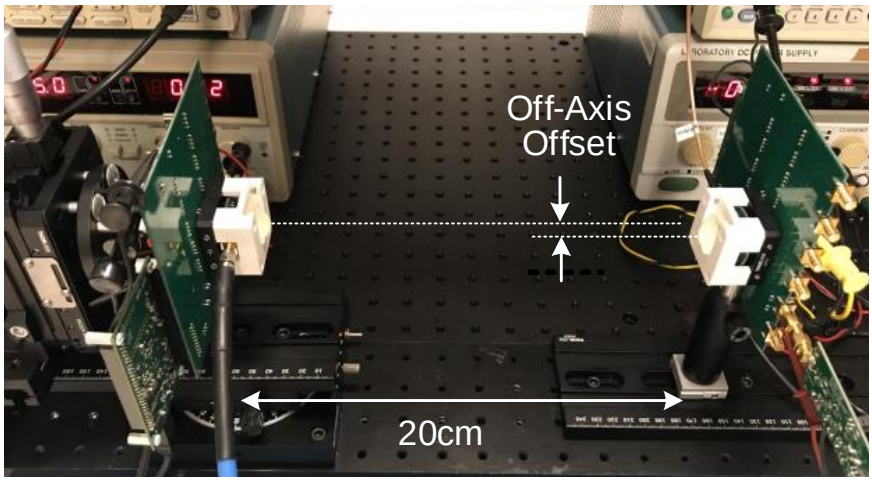
Figure 4-28: Measured conversion loss of a single pixel for plane wave mode (m=0). The calculation assumes that the power incident to the chip is divided equally among the eight antennas.

4.6.3 Characterization of CMOS OAM link

Finally, a full-silicon OAM link is tested using the measurement setup shown in Fig. 4-29. Two chips configured in Tx and Rx mode, respectively, are placed 20 cm apart. Both the chips are configured to be in the m=+1 mode, and the combined IF output from the Rx chip is measured with controlled axial misalignment, as shown in Fig. 4-30a. It is evident that the reception is highly sensitive to the Rx offset from the array axis demonstrating the aforementioned PLS. Note that the experiment is performed with the matched modes. Without prior knowledge of the mode (as for eavesdroppers), the mode detection will be even harder with offset misalignment. The measured beam profiles (using the setup shown in Fig. 4-21), when both the Tx chip and Rx SPP are in mode m=0 and +1, are shown in Fig. 4-30b. The result clearly shows that an OAM Tx-Rx link, compared to its plane-wave counterpart, has a much higher sensitivity to angular misalignment.

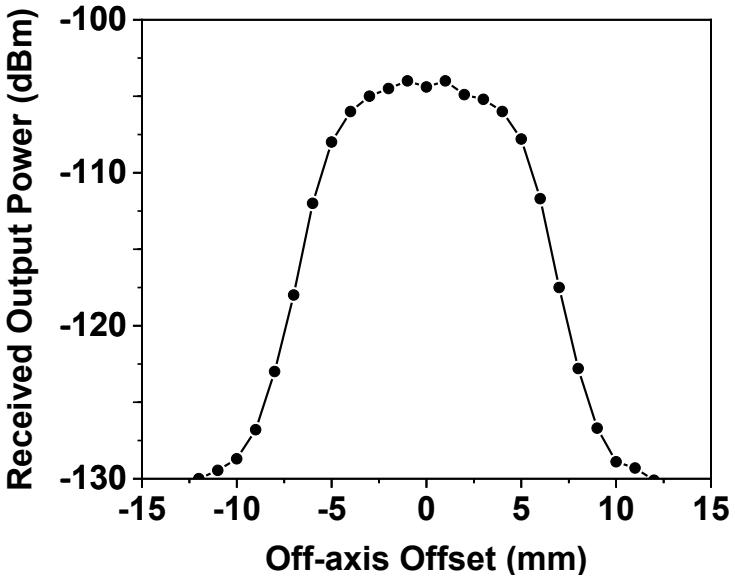


(a)

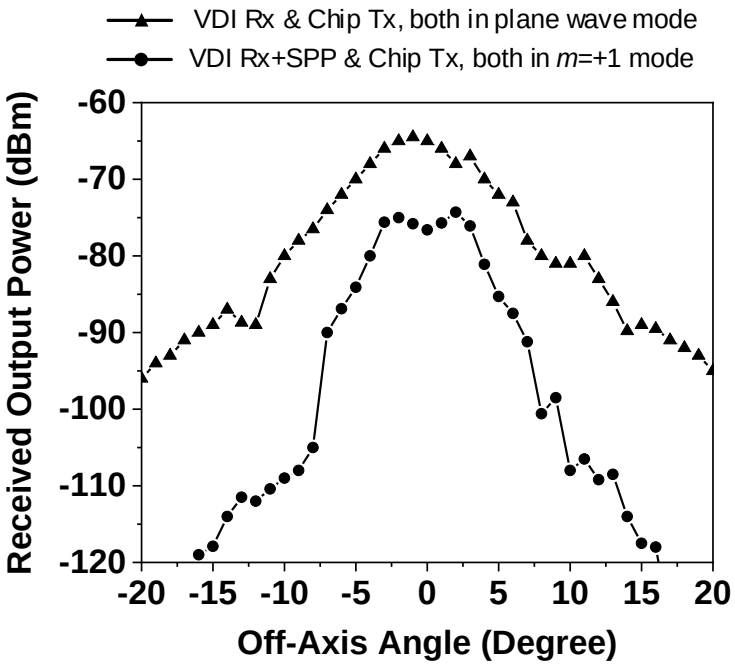


(b)

Figure 4-29: (a) Diagram of the experimental setup for the characterization of full-silicon OAM link and sensitivity to co-axial alignment. (b) Photograph of the test setup.



(a)



(b)

Figure 4-30: (a) Measured sensitivity of OAM Tx-Rx to co-axial alignment. (b) Measured alignment angle sensitivity for the plane wave (m=0) and OAM (m=+1) modes.

4.7 Analysis of OAM-PLS

This section evaluates the security vulnerabilities of the OAM modulation of our THz system under various physical-layer threat models. The effectiveness of these threat models is analyzed for varying attacker complexity levels under different conditions.

Consider Alice as a THz transmitter with a uniform circular antenna array enabling the OAM wave generation with bits-to-OAM mode mapping and randomized phase switching for secret key sharing. Bob is a legitimate receiver with a similar uniform circular antenna array for OAM wave reception. The transmitter and receiver antenna arrays should be well aligned to the beam axis. Eve is an unauthorized eavesdropper that is located anywhere between Alice and Bob with one or multiple receivers. In the proposed physical-layer security scheme, the confidential messages, e.g., secret keys, are mapped to different OAM modes. The secret key is transmitted by hopping between these OAM modes and the initial phase distribution of each mode is controlled by a cryptographically-secure pseudorandom number generator.

The OAM mode can only be decoded with the phase gradient information, and a single receiver is not enough to compute the phase difference. Thus, Eve with one receiver is unable to distinguish between modes transmitted.

Fig. 4-31 indicates a threat model in which Eve has two receivers. In this threat model, we define an unsecured area, where Eve can evaluate the phase gradient between two antennas. The assumptions for this threat model analysis are as follows:

1. Eve is located where the beam power is at its maximum for OAM modes.

2. Alice is the only source of noise, and Eve's receiver has a 0dB noise figure.

3. The distances from Alice to the two antennas are equal (i.e. $L_1 = L_2$). Similarly, the two antennas are at an equal distance from the beam axis (i.e $r_1 = r_2$) and the angle between them is precisely known.

4. Eve with two antennas has LO phase mismatch, which is a function of the distance between the two antennas.

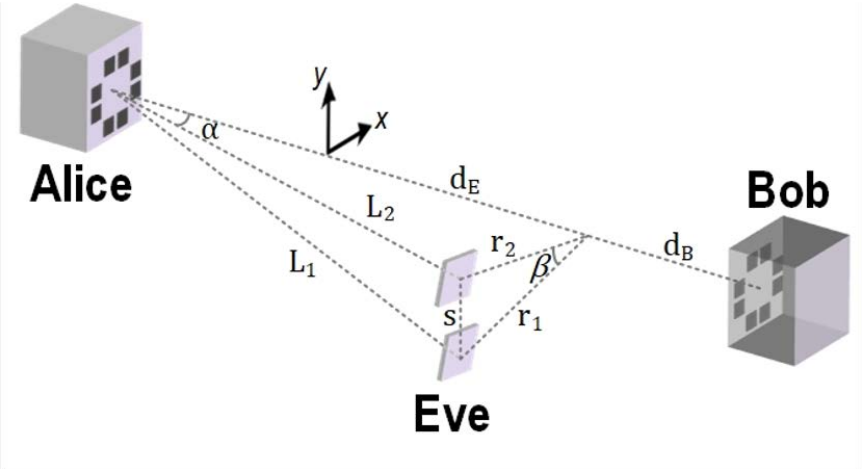


Figure 4-31: Threat model where Eve has two receivers or two colluding eavesdroppers are present.

First, given the phase noise from Alice, which generates the 310 GHz signal, the phase noise is integrated to find the minimum detectable phase difference (β_{min}). The minimum phase precision (β_{min}) between the two receivers is given by

$$\beta_{min} = \frac{360^\circ \times f_{IF}}{Jitter_{RMS}} = 6.9^\circ \tag{4.5}$$

where $Jitter_{RMS}$ is given as

$$Jitter_{RMS} = \frac{\sqrt{2 \times 10^{IntegratedPN/10}}}{2\pi f_{IF}} \tag{4.6}$$

where *IntegratedPN* is the total phase noise integrated for a commercial frequency synthesizer (E8257D PSG Analog Signal Generator) and f_{IF} is the intermediate frequency of the down-converted signal at Eve's receiver, assumed as 10MHz.

Based on Eq. (4.5), the two antennas should be apart from each other at least 6.9° in order to evaluate the phase difference without ambiguity. The distance between the two antennas (s) is given by

$$s = 2d_{AE} \sin\left(\frac{\beta}{2}\right) \tan(\alpha) \tag{4.7}$$

where d_{AE} is the distance of Eve from Alice along the beam-axis and α is the angle between the Eve and beam-axis at Alice as shown in Fig. 4-31. The maximum value of

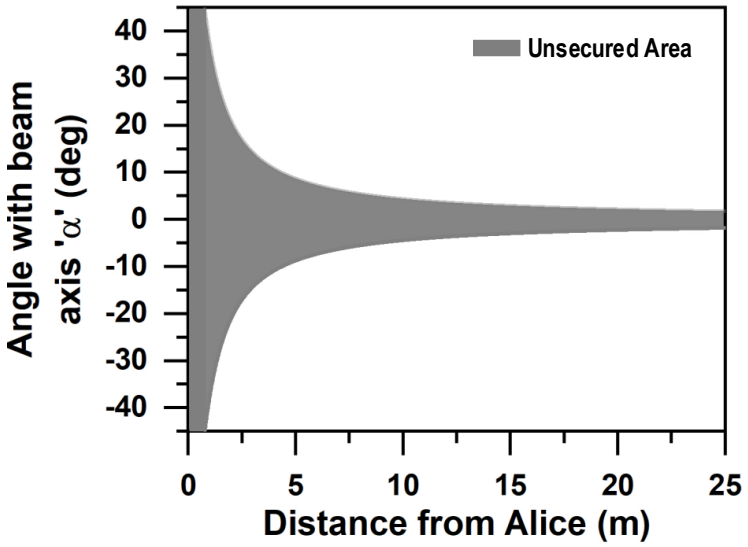


Figure 4-32: Calculated unsecured region (for β=15°and s_{limit}=20cm) where Eve with two receivers can detect phase gradient and hence OAM modes.

s is limited as the two antennas are required to be synchronized at the THz frequency level which is difficult due to the relatively short wavelength and requires μm precision. The maximum distance between two antennas after which THz LO phase mismatch is more than β is denoted as s_{limit}.

Fig. 4-32 visualizes the unsecured area of the system when β and s_{limit} are set to 15° and 20cm, respectively. Theoretically, Eve located in the unsecured area is able to decode the different OAM modes by evaluating the phase difference between the received signals from different antennas. However, even if Eve has multiple antennas perfectly placed, the boundary of the unsecured area still depends on the resources for eavesdropping. For example, the typical Coefficient of Thermal Expansion (CTE) of FR4 PCB is 17ppm/°C, thus 10cm PCB with 6° temperature variation may change the dimension by 10μm, which leads to about 4° of phase error. Therefore, larger antenna spacing with the presence of the phase noise will eventually fail to provide enough phase accuracy to detect the OAM mode. For m=(+1)+(-1) mode, the expected standing peaks and nulls are measured for the sum of the two counter-rotating wavefronts. Since those peaks and nulls are randomly shifted in each transmission

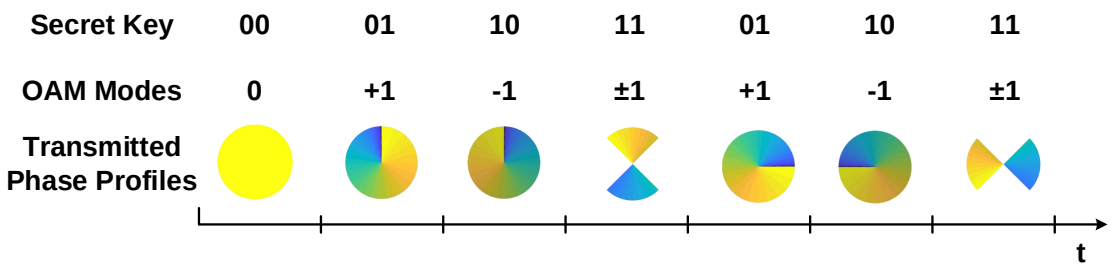


Figure 4-33: Keccak-f[400] based random twisting of transmitted phase profiles in each transmission ensures that Eve experiences nulls for superposed mode.

by Keccak-f[400] based pseudorandom number generator, Eve cannot fully record the signals at certain locations. The random twisting of the transmitted phase profile in each transmission is shown in Fig. 4-33. Therefore, in a practical scenario, the unsecured area for two-antenna Eve is even more restricted than shown in Fig. 4-32. It is possible for Eve to have more than two antennas or more than two eavesdroppers can collude together. They can jointly infer the superposition mode even if there exists an arbitrary delay between transmissions. However, it is difficult to synchronize all of the eavesdroppers at the THz frequency and, hence, distinguish the communication delay. The robustness of OAM-PLS can be further improved by employing higher order OAM especially higher order superposed modes with random twists.

4.8 Comparison with the State-of-Art

The THz-OAM chip is capable of dynamically generating data-driven OAM modes: m=0, +1, -1 and (+1)+(-1), as well as detecting these modes with >10 dB rejection of mismatched modes. TABLE 4.3 provides a comparison with other discrete-component-based RF and mm-Wave OAM prototypes. Note that, in the compared works, each OAM mode is transmitting its own independent data stream and multiple OAM modes are spatially multiplexed to enhance spectral efficiency. However, in our work, a single data stream is encoded in multiple OAM modes to transmit it securely. Our work is also the first demonstration of a full-silicon OAM link at any frequency and is the first hardware delivering dynamic OAM mode switching in the THz regime.

Table 4.3: Comparison with Prior RF and mm-Wave OAM Prototypes

	Nature Comm. '14 [67]	**Wireless Comm. '17 [71]**	**ICCW '20 [72]**	**This work**
Implementation	Discrete Transceivers + SPP + Quasi-Optical Beam Combiner	Active-Driven Antenna Arrays + Parabolic Reflectors	Active-Driven Antenna Arrays	Active-Driven Antenna Array on a 65-nm CMOS Chip + Teflon Lens
Frequency (GHz)	28	10	40	310
OAM Modes	±1, ±3	±2, ±3	0, ±1, ±2, ±3	0, +1, -1, ±1
Data Modulation	16 QAM/Mode Dual Polarization	32 QAM on each mode, Full Duplex	256 QAM/Mode Dual Polarization	Bits-to-Mode OAM Hopping
Radiated Power (dBm)	8	0	11.5	-24.8 (-4.8 EIRP)
Antenna Aperture Diameter (cm)	30	60	120	1.35
Application	Enhanced Spectral Efficiency	Enhanced Spectral Efficiency	Enhanced Spectral Efficiency	Physical-Layer Security
DC Power (mW)	N/A	N/A	N/A	154 (Tx), 166 (Rx)

Chapter 5

Bluetooth Low Energy (BLE) Compatible Wake-up Receiver for Ingestible Capsule

5.1 Motivation and Challenges

Ingestible electronics have revolutionized the standard of care for a variety of health conditions. It is now possible to perform video capture [94], electronically controlled drug release [95], pH, temperature, and pressure recording [96], and heart rate and respiration monitoring [97] from within electronic pill-like capsules placed in the gastrointestinal (GI) tract. Extending the capacity and safety of these devices, and reducing the power consumption, could enable broad deployment of prolonged-monitoring systems for patients. In this thesis, a BLE-compatible wake-up receiver is designed for potential application in an ingestible capsule (Fig. 5-1). The capsule contains a certain drug and will release it upon request of an external transmitter. The capsule is expected to stay inside a human body for at least 60 days and operate with a small coin cell battery with limited capacity. The purpose of the wake-up receiver is to provide an ultra-low power authentication of trigger messages during the entire lifetime of the capsule.

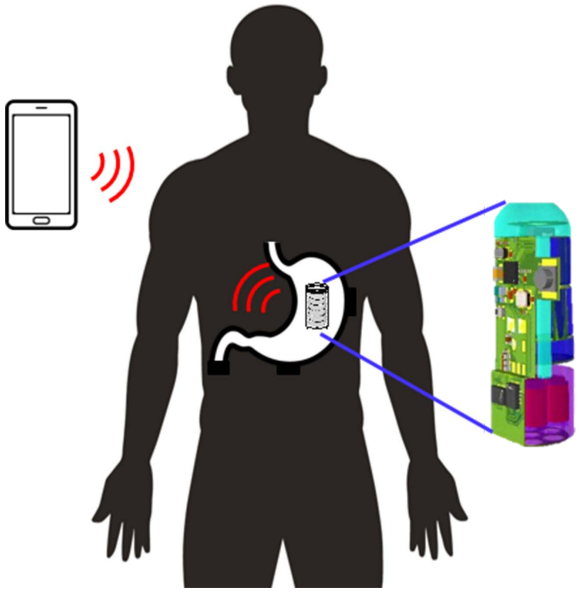


Figure 5-1: Potential application of high sensitivity and ultra-low-power wake-up receiver in an ingestible capsule.

Due to limited volume inside the capsule, a custom-designed antenna is required that is much smaller than the wavelength of operation frequency ($\leq$4 mm on the longer side) and works efficiently in the presence of closely placed electronics and batteries. The GI track environment around the capsule (especially dielectric constant) can change significantly several times during the day. This results in a variation of the antenna performance especially the resonance frequency of the antenna shifts drastically. In order to mitigate this problem, an air-gap ($\sim$1 mm) is established between the antenna and capsule body. This ensures that the near-field of the antenna remains relatively constant and hence the performance. The challenges of the receiver chip are presented in the next section.

5.2 Wake-up Receiver Specifications

There are many specifications that the receiver should meet.

- **Standard:** In order to be able to wake the receiver up using a commercially available cell phone, the receiver needs to comply with existing standards. The most convenient and energy efficient one is BLE. The 2.48 GHz BLE channel

also leads to a relatively small antenna size that can fit within the capsule form factor as compared to lower frequencies (e.g., 900 MHz) or ultrasound.

- **Power consumption:** An average power consumption below 1μW is targeted so that the receiver can last for at least 60 days with limited capacity batteries. This is achieved by duty-cycling i.e. the receiver is in sleep mode when it is not listening. The duty-cycled ratio is

$$D = \frac{T_{ON}}{T_R} \tag{5.1}$$

where T_{ON} is the time interval when the receiver is ON and actively listening and T_R is the repetition interval of switching ON the receiver. A duty cycle ratio of D=0.1% is selected to allow a power budget of 1 mW for the receiver. A high duty cycle ratio however also leads to longer latency but in our application, it is not a critical issue.

- **Data Rate:** The standard BLE packets are transmitted at 1 Mbps with a GFSK modulation of a 500 kHz frequency deviation. In order to reduce the power consumption and improve sensitivity (through reduction of required receiver bandwidth), the data rate is reduced to 125 kbps. This is achieved through bit repetition by sending 8 bits for one actual bit of the wake-up pattern.

- **Sensitivity:** It is observed in animal testing that the BLE signal attenuates by 60-70 dB depending on the location and orientation of the capsule inside the animal body. Hence, in order to ensure reliable communication with +4 dBm of transmitted power from a commercial BLE transmitter, the targeted sensitivity of the receiver is -90 dBm. The sensitivity is calculated as

$$P_{sens} = -174dBm/Hz + NF + 10log_{10}(BW) + SNR_{min} \tag{5.2}$$

where NF is the effective noise figure and BW is the effective bandwidth of the receiver, and SNR_{min} is the minimum required SNR for BER$<10^{-3}$. As shown in the next section, our receiver has NF=9 dB and BW=0.5 MHz, and GFSK modulation requires SNR_{min}=12 dB. This gives the estimated sensitivity of -96 dBm.

The figure-of-merit (FoM) for the wake-up receivers is defined as

$$FoM = -Sensitivity(dBm) + 10log_{10}\left(\frac{1}{Latency}\right) - 10log_{10}\left(\frac{P_{DC}}{1mW}\right) \quad (5.3)$$

FoM of the proposed receiver is very competitive 111.3 under stringent operating conditions.

5.3 Circuits Design for the Wake-up Receiver

The schematic of the wake-up receiver is shown in Fig. 5-2. The on-chip RF front-end comprises a tunable matching network (TMN), low-noise amplifier (LNA), mixer, and impedance sensor. It is followed by IF amplifiers chain with programmable gain, FSK demodulator, base-band amplifier and Schmitt trigger. The authentication processor validates the wake-up pattern and triggers the wake-up signal. An off-chip resonator (FBAR) is used with the Pierce oscillator to generate a 2.489 GHz LO frequency. The same signal is used for the impedance sensor and the clock signals for the FSK demodulator (at 9.73 MHz) and processor (at 1.24 MHz) are also derived from it through frequency dividers. An impedance sensor, consisting of phase and envelop detectors, periodically compares the phase and amplitude of the voltages at TMN and at a reference impedance (Z^*_{LNA}). Then, a control circuit tunes the matching network and also feeds the data to a machine learning algorithm. The calibration of the matching network is performed few times everyday and the daily patterns are learned to minimized the energy consumption for future search of optimal network. Next, the details of individual circuits are presented.

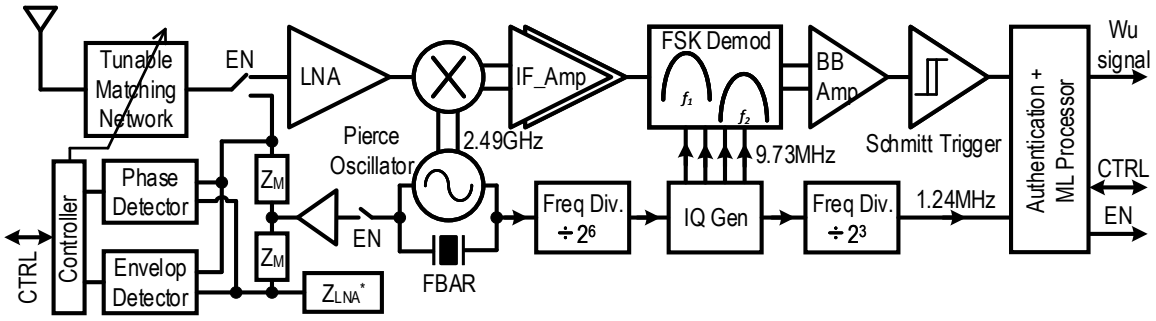
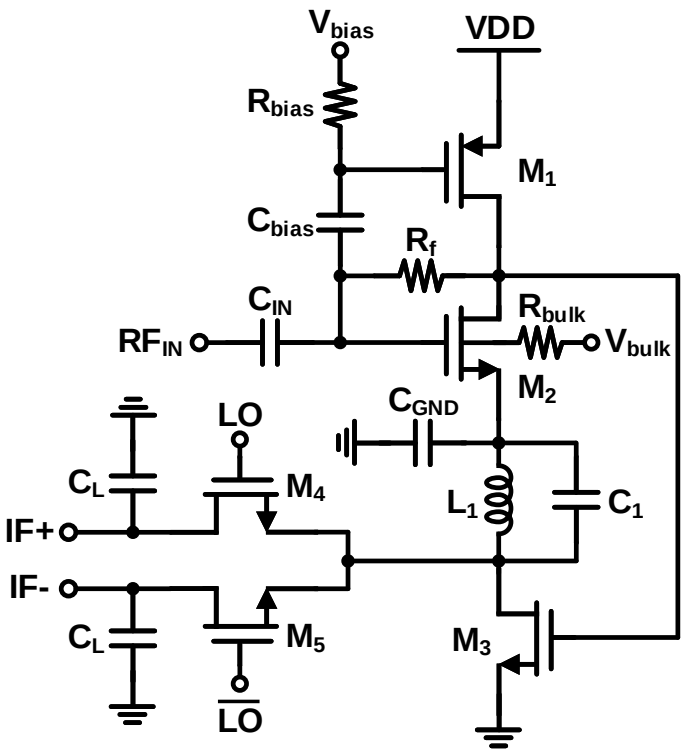


Figure 5-2: The schematic of the wake-up receiver with a control loop for the matching network tunning.

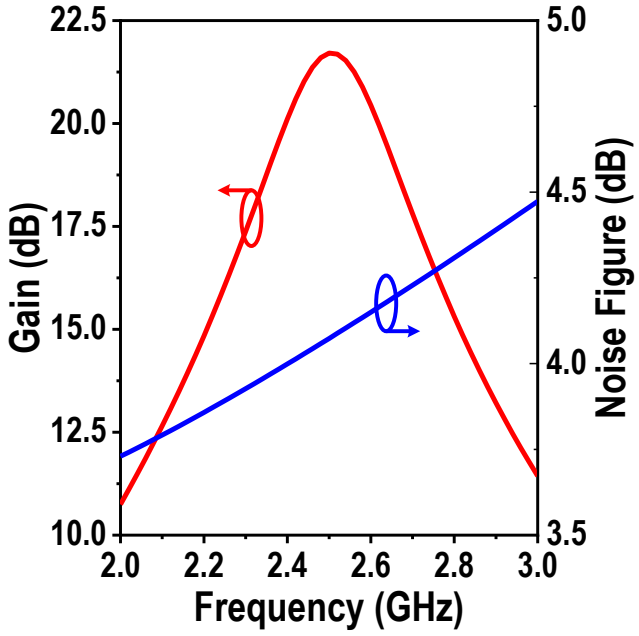
5.3.1 Low-Noise Amplifier and Mixer

Fig. 5-3 shows the schematic of LNA and mixer. M_1, M_2, and R_f form the complementary g_m-boosted input stage. C_{bias} decouples the DC biasing of M_1 and M_2, thus optimum sizing for g_m of each transistor can be independently selected. M_1 is directly biased at the gate with V_{bias}, and M_2 is forward body biased to lower its threshold voltage and enhance low voltage operation. M_3 is stacked below M_2 as a second gain stage. Hence, the current is reused for the second common source stage and leads to low power operation. The LNA consumes 214μA current from a 0.7V supply. The LC resonator tank formed by L_1 and C_1 is used to both cancel the AC leakage between the two gain stages and to resonate the output impedance of the second stage. The simulated gain and noise figure of the LNA are $\sim$ 21 dB and $\sim$ 4 dB, respectively, as shown in Fig. 5-3b.

The LNA is followed by a passive single-sideband mixer with a 0.5 pF load to limit the out-of-band interference. It has a simulated voltage conversion gain of 0.5 dB and down-converts the RF signals to the IF signal with GFSK modulation between 9.48MHz and 9.98MHz. Due to the lack of a channel selection filter after the LNA, the mixer folds the noise onto the IF signals giving a noise figure of 3 dB. The differential IF signals are then amplified by a chain of four IF amplifiers with programmable gains. The gain control prevents saturation at higher input signals. A differential amplifier with switchable source degeneration resistance is used for this purpose. As the signal undergoes down-conversion to IF and gets amplified by the IF



(a)



(b)

Figure 5-3: (a) The schematic of the LNA and mixer. (b) Simulated gain and noise figure of the LNA.

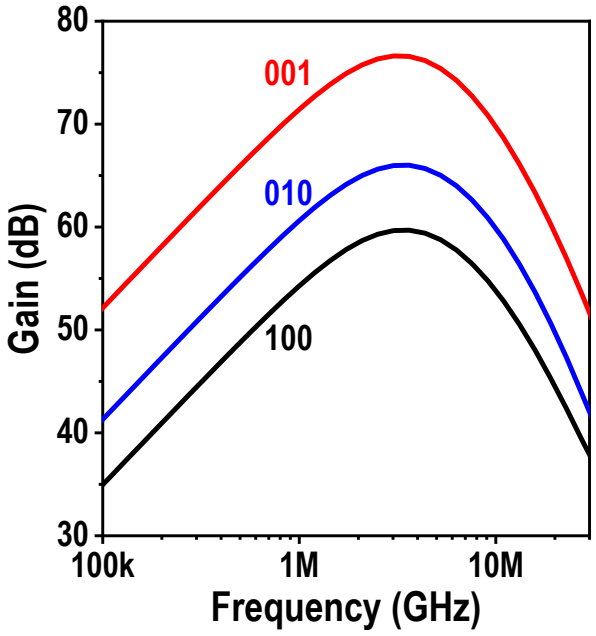


Figure 5-4: Simulated programmable gain of IF amplifier chain with N-path filter.

amplifiers, it needs to be filtered to reject any out-of-band interferers and to reduce the overall noise bandwidth in order to achieve the required sensitivity. Hence, the block directly following the first amplifier stage is a bandpass filter (BPF) implemented using a N-path filter. It is a switched capacitor filter whose center frequency is the same as the switching clock frequency (9.73MHz in our case). The gain of the IF amplifier chain with a 4-path filter is programmable by ∼15 dB as shown in Fig. 5-4. The amplifier chain consumes 24μW power from a 0.7 V supply.

A tunable matching network based on two L-sections (with series inductors and shunt capacitors) is used both to match the antenna with the input impedance of the LNA and also to provide a passive gain to improve the overall sensitivity. In particular, a matching network that transforms an antenna impedance of $Z_{ANT} = 50\Omega$ into an input impedance of $Z_{LNA} = 350\Omega$, provides a passive gain of:

$$A_{passive} = \sqrt{\frac{Z_{LNA}}{Z_{ANT}}} \tag{5.4}$$

Hence, a large input impedance of LNA is preferable for a higher passive gain.

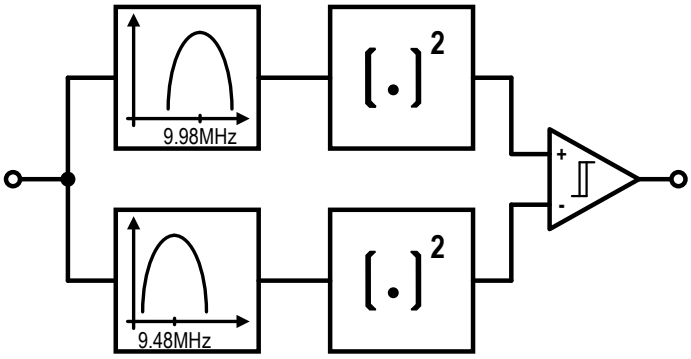


Figure 5-5: FSK demodulator circuit.

5.3.2 FSK Demodulator

The GFSK modulated BLE packets are demodulated in order to extract the actual transmitted bits from the base station to be able to detect the wake-up pattern. As the frequency deviation for FSK modulated signal is fixed to 500 kHz and the data rate is adjusted to be 125 kbps by using bit repetition, the FSK demodulation can utilize two narrow band BPFs with a 500 kHz difference between their center frequencies. Filters are followed by energy detection and comparison circuit, as shown in Fig. 5-6a. The higher frequency f_1 corresponds to bit '1' and lower f_2 translates to bit '0' as stated by the BLE standard [98].

The filters are implemented as a N-path filter with a clock frequency of f_{CLK}= 9.73MHz and the high frequency filter is centered around f_1=9.98MHz while the other is centered around f_2=9.48MHz. As the bandwidth of the filters is less than 500 kHz, it is important to have some programmable control of the center frequencies to compensate for the process and clock frequency variations. The filter circuit is shown in Fig. 5-6a where two differential Gm-cells are used to control the center frequency shift away from the clock frequency. By adding the Gm-cells, the input impedance of the switched capacitor load changes from capacitive to a complex impedance resulting in a center frequency shift. For instance, a conventional switched capacitor filter with a load capacitor of C_F forms a low pass filter with the switch resistance and then the mixing effect upconverts this filter response around the clock frequency f_{CLK}. By

adding the Gm-cells, then the impedance becomes

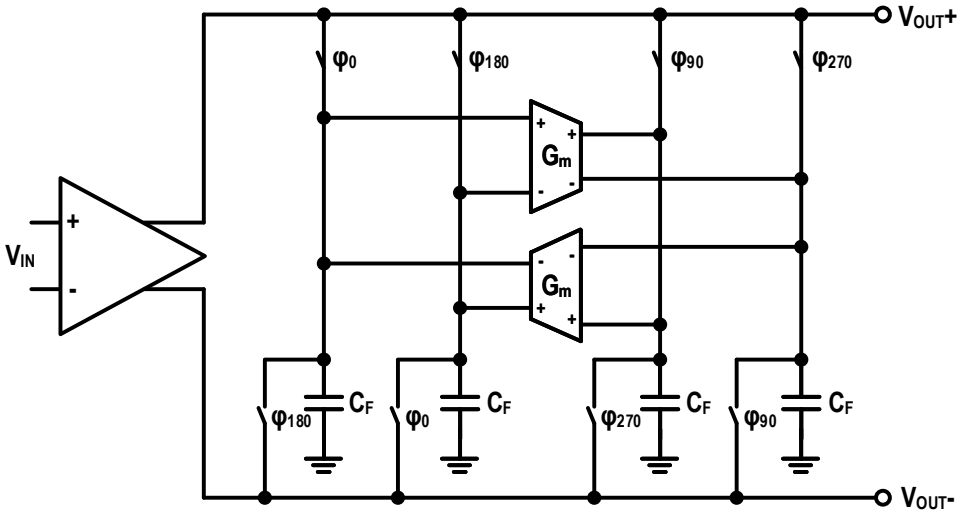
$$Y_{Gm}(s) = sC_F - jG_m = jC_F(\omega - \omega_F) \tag{5.5}$$

where ω_F=G_m/C_F. It shows that a positive frequency shift of ω_F can be achieved by having a negative Gm value while a negative frequency shift is attainable by reversing the polarity of the differential Gm structure. Therefore, two narrow band BPFs with the required frequency deviation can be designed to detect the transmitted bits. The center frequency programmability is shown in Fig. 5-6b and Fig. 5-6c for negative and positive transconductance values, respectively.

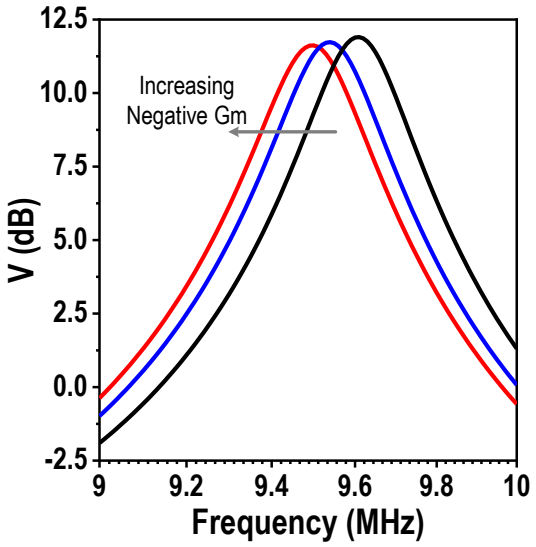
5.3.3 Film Bulk Acoustic Resonators (FBAR)

Film Bulk Acoustic Resonators (FBARs) are used in low-power oscillators to create a stable frequency with low phase noise due to their high-Q (Quality Factor) [99, 100]. FBAR is employed as the resonator with the Pierce oscillator for LO frequency generation as well as for the clock signals of the filters. The resonators are typically modeled with the modified Butterworth Van Dyke (m-BVD) model shown in Fig. 5-7a [101]. This model captures all the characteristics of the resonator i.e. both the series and parallel resonance characteristics. The measured m-BVD model parameters of the FBAR used in this project are given in TABLE 5.1. Fig. 5-7b shows the simulated characteristics of FBAR with these parameters. It has the following features:

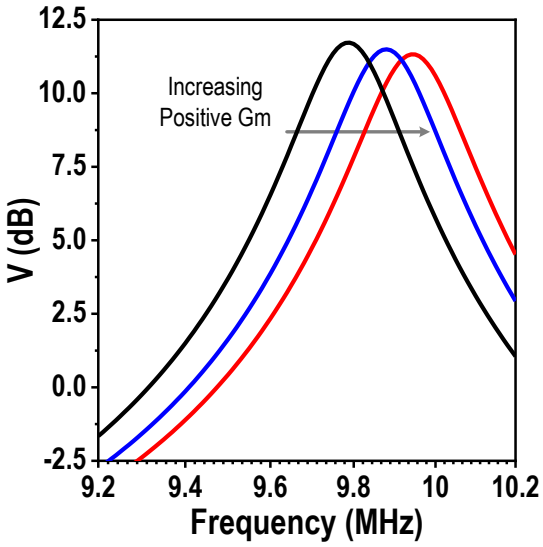
1. The impedance is low and resistive at the series resonance frequency f_s.
2. The impedance is very high and resistive at a slightly higher parallel resonance frequency f_p.
3. The coupling coefficient is defined as $\mathrm{k}^2 = (f_p/f_s)^2 - 1$ and indicates the amount of tuning available from the resonator.
4. At frequencies far away from resonance, the impedance is capacitive.
5. Between the two resonant frequencies, the impedance is inductive.



(a)



(b)

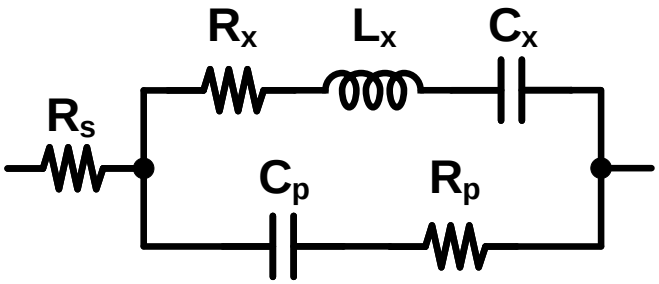


(c)

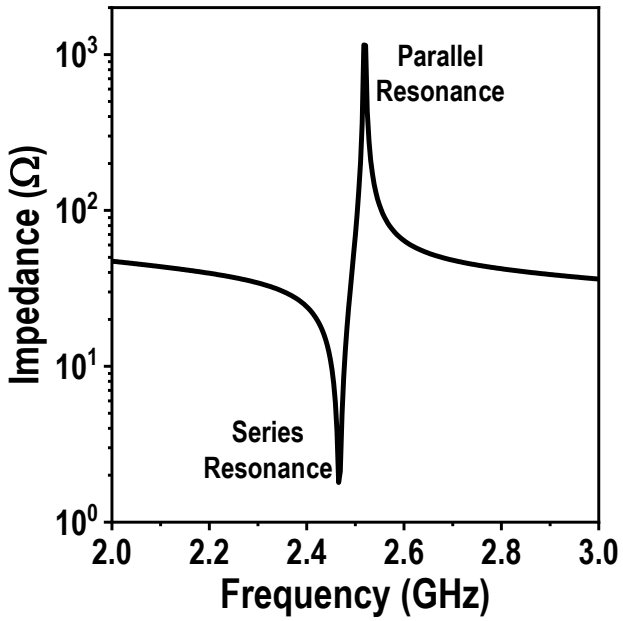
Figure 5-6: (a) The schematic of Gm-shifted bandpass filters for FSK demodulator. (b) Simulated frequency response of the filters at different Gm values.

Table 5.1: BVD MODEL PARAMETERS OF THE FBAR

$\mathbf{R_x}$	$\mathbf{L_x}$	$\mathbf{C_x}$	$\mathbf{C_p}$	$\mathbf{R_p}$	$\mathbf{R_s}$
0.23mΩ	75.9nH	54.59fF	1.23pF	0.68Ω	1.26Ω



(a)



(b)

Figure 5-7: (a) Modified Butterworth Van Dyke model and (b) simulated impedance characteristics of the FBAR resonator.

5.3.4 Pierce Oscillator

Due to the advantages of current-reuse, high amplitudes of oscillation, low power, low voltage operation, self-biasing, and tunability, the inverter-based Pierce oscillator is chosen in this design [102]. The schematic of the oscillator is shown in Fig. 5-8. The g_m of both the transistors (M_1 and M_2) adds up and this current-reuse reduces power consumption for the same loop-gain as compared to a single transistor. The resistor R_f provides DC biasing by setting the gate voltage and hence, the circuit is self-biased. This circuit also provides rail-to-rail oscillation. Since there are only two transistors stacked, this topology is amenable to low-supply voltage designs. The FBAR behaves like an inductor at frequencies between its series and parallel resonance. This inductance resonates with the gate, drain and other parasitic capacitors at the effective parallel resonance frequency. The active transistors M_1 and M_2 sees a high impedance at this frequency. Under some approximations, the DC loop-gain of this circuit at the resonant frequency is

$$Gain \propto (g_{mP} + g_{mN}) \cdot R_p \tag{5.6}$$

where R_p is the FBAR impedance at parallel resonance. Thus, the circuit oscillates when designed with sufficient g_m. The oscillator consumes 300μA to provide sufficient $g_{m,total}$=9.7mS. The oscillation frequency can be tuned to a certain extent ($\sim$10 MHz) by adding explicit capacitor banks C_1 and C_2 at the gate and drain of the oscillator, respectively.

5.4 Conclusion and Future Work

In this chapter, a system-level analysis for the duty-cycled BLE wake-up receiver is presented to determine the sensitivity, data rate and duty-cycling period. A new architecture is then developed with high programmability and periodic calibration of the antenna matching network. A prototype of the wake-up receiver is built in 65-nm CMOS technology. The receiver is designed for at least -90 dBm of sensitivity to

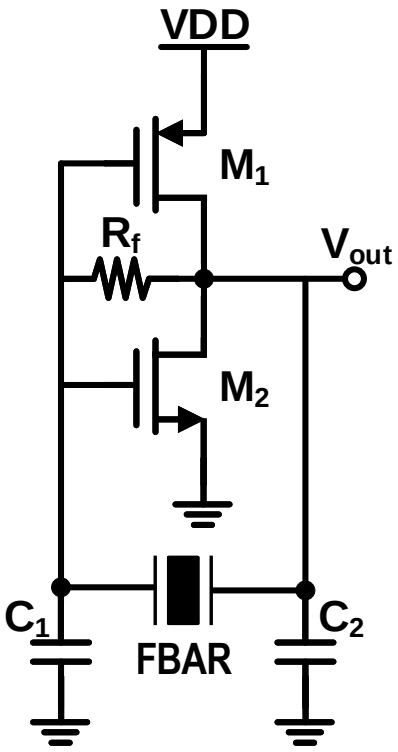


Figure 5-8: The schematic of the inverter-based Pierce oscillator.

account for the 60-70 dB power loss of the wave traveling through the human body. The receiver operates from a 0.7 V supply and consumes an average power of 1μW at a latency of 0.25 sec with a custom transmission interval. Further details on the challenges, analysis and innovations in the custom-antenna design, impedance sensor, and machine learning based energy-efficient search algorithms will be presented in future publications.

Chapter 6

Conclusion and Future Works

6.1 THz-ID and THz Energy Harvesting

This thesis demonstrates a new application of THz CMOS electronics, which utilizes its advantages in compact size and package-less chip integration. We also show that silicon THz transceivers, which are long considered to be power-hungry, can be applied in ultra-low-power systems if a back-scattering communication scheme is adopted. Meanwhile, our work demonstrates the feasibility of integrating asymmetric cryptography, such as elliptic-curve encryption, on a passive tag. Our presented tag is built entirely on a low-cost CMOS chip, and is around 3× smaller than the smallest package-less, far-field chip reported previously [31]. It also offers multi-antenna beam-steering functionality for the first time in RFIDs. The uplink and downlink data rates are 2kbps and 100kbps, respectively and have been demonstrated at a distance of 5-cm. The tag employs a security processor with a peak power consumption of 21μW.

The presented work demonstrates the feasibility of security ID tags with ultra-small size and cost, which is expected to empower a wide range of new applications in manufacturing, logistics, anti-counterfeiting, and so on. To fully make these applications practical, a few more technologies should be developed. The size and cost requirements for the THz-ID reader, compared to the tags, are much more relaxed, it is still highly preferred that the reader front-end is implemented using silicon integrated

circuits. Rapid advances are being made in this area. For example, in [103], the 200-to-255-GHz power amplifier using 130-nm SiGe BiCMOS process (f_{max} ≈500 GHz) is already capable of generating 20 mW of power, which is only 7 dB away from the VDI AMC used in our tag reader. In the light of the recent developments of high-speed and high-power SiGe and CMOS processes [58, 104–106] with up to 720-GHz f_{max} and up to 7.1-V breakdown voltage, achieving a radiation power of 100 mW in the sub-THz regime is no longer unimaginable.

Although, the energy harvesting circuit presented in this thesis has enabled the embedding of THz-ID in opaque packaging, there is a need for further miniaturization of the harvester for applications in micro-robots, micro-sensors etc. Further, new topologies can be explored where harvesters can be stacked for higher output voltage thus avoiding the need for lossy DC-DC converter. All of these advances can promise longer distance communication that can enable applications such as controlling micro-drones, where size, cost, beam-steering, and low power are important. Other IoT applications can follow especially with the advances in 6G communication and beyond.

6.2 THz-OAM Transceiver

A 0.31-THz uniform circular patch antenna array is demonstrated in the 65-nm CMOS process that can transmit and receive waves carrying OAM. The chip is capable of dynamically generating data-driven OAM modes: m=0, +1, -1, and (+1)+(-1), as well as detecting these modes with >10 dB rejection of mismatched modes. Our work is also the first demonstration of a full-silicon OAM link at any frequency and is the first hardware delivering dynamic OAM mode switching in the THz regime.

The presented work opens up opportunities in mode-multiplexing wireless communications and PLS for one-way key transmission using low-cost microelectronic chips. The chip can use OAM modes for transmitting security keys (usually 256 bits) at a relatively low data rate (limited by the SNR due to the central null) and then switch to the plane wave mode for exchanging symmetrically encrypted data at higher data rates. In future iterations, the 155 GHz power amplifier (PA) and the frequency dou-

bler can be integrated inside the pixel. This will not only improve the link budget for high-speed wireless communication but also make the architecture more scalable for higher OAM modes. PA-integrated pixels placed in concentric circles and all driven by the same reference signals will make the generation and multiplexing of higher order OAM modes feasible which are essential for improving the OAM security. Moreover, the presented chip will empower a wide range of new applications of OAM in the THz regime [107–109]. In [108], it has been shown that OAM beams penetrate deeper into the biological tissues as compared to Gaussian beams. This property of OAM can be combined with the THz absorption signature of tumor cells for early skin cancer detection. Further, it is shown in [109] that it is possible to detect rotational Doppler shifts using OAM waves. Therefore, it becomes possible to design THz-OAM radars with the capability of detecting both the linear and rotational Doppler shifts which will be extremely powerful.

Appendix A

Noise Voltage of an Open-Circuit Photodiode Under Illumination

In the downlink THz MOSFET detector (Fig. 2-17), an open-circuit photodiode under illumination is used to provide the gate bias of the transistor. The net output current of the photodiode, although is zero, should be treated as the sum of two opposite current flows [110]. One is the photocurrent I_p generated by the illumination, and the other is the diffusion current I_d due to the forward bias of the diode:

$$I_d = -I_p = I_0(e^{\frac{V_0}{V_t}} - 1), \tag{A.1}$$

where I_0 is the reverse saturation current of the p-n junction, V_t is the thermal voltage (V_t=kT/q ≈26 mV at 300 K), and V_0 is the open-circuit photodiode voltage. The respective noise fluctuations associated with the above currents are uncorrelated, so the total equivalent noise current power spectral density of the device is [110, 111]:

$$\tilde{i_n^2}/\Delta f = 4q(|I_p| + I_0) \approx 4q|I_p|. \tag{A.2}$$

The open-circuit noise voltage of the photodiode is then considered to be the

product of (A.2) and the diode differential resistance at the bias (R_d=$V_t/|I_p|$):

$$\tilde{v_n^2} = \tilde{i_n^2} \cdot R_d^2 = 4q|I_p| \cdot \left(\frac{V_t}{|I_p|}\right)^2 \Delta f = 4q\frac{V_t^2}{|I_p|}\Delta f = 4kTR_d\Delta f \tag{A.3}$$

Interestingly, the generated noise is the same as the thermal noise of a resistor equal to R_d of the photodiode, and decreases with larger illumination. Hence, its noise contribution to the output noise voltage of the MOSFET detector in Fig. 2-17 is:

$$\tilde{v}_{n,det}^2 = g_m^2 \cdot \tilde{v_n^2} \cdot r_{ds}^2 = g_m^2 r_{ds}^2 \cdot 4kTR_d\Delta f, \tag{A.4}$$

where g_m and r_{ds} are the transconductance and output resistance of the MOSFET. Note that (A.4) is much smaller than the MOSFET's own channel thermal noise ($\tilde{v}_{n,ch}^2 = 4kTr_{ds}\Delta f$): for the MOSFET biased in the triode mode (Fig. 2-17), the simulated g_m and r_{ds} are 1.4 μS and 7.7 kΩ, respectively, and I_p in normal tag operation is $\sim$0.1 μA (hence $R_d\approx$260 kΩ). Therefore, $\tilde{v}_{n,ch}$ is $\sim$11 nV/Hz$^{1/2}$, while $\tilde{v}_{n,det}$ in (A.4) is $\sim$0.7 nV/Hz$^{1/2}$.

Bibliography

[1] Mohamed I. Ibrahim, Muhammad Ibrahim Wasiq Khan, Chiraag S. Juvekar, Wanyeong Jung, Rabia Tugce Yazicigil, Anantha P. Chandrakasan, and Ruonan Han. THzID: A 1.6mm^2 Package-Less Cryptographic Identification Tag with Backscattering and Beam-Steering at 260GHz. In *IEEE International Solid-State Circuits Conference (ISSCC)*, pages 24–26, 2020.

[2] Li Xu, Maya Lassiter, Xiao Wu, Yejoong Kim, Jungho Lee, Makoto Yasuda, Masaru Kawaminami, Marc Miskin, David Blaauw, and Dennis Sylvester. A 210×340×50μm Integrated CMOS System for Micro-Robots with Energy Harvesting, Sensing, Processing, Communication and Actuation. In *2022 IEEE International Solid- State Circuits Conference (ISSCC)*, volume 65, pages 1–3, 2022.

[3] Alejandro J. Cortese, Conrad L. Smart, Tianyu Wang, Michael F. Reynolds, Samantha L. Norris, Yanxin Ji, Sunwoo Lee, Aaron Mok, Chunyan Wu, Fei Xia, Nathan I. Ellis, Alyosha C. Molnar, Chris Xu, and Paul L. McEuen. Microscopic sensors using optical wireless integrated circuits. *Proceedings of the National Academy of Sciences*, 117(17):9173–9179, 2020.

[4] Marcus J. Weber, Yoshiaki Yoshihara, Ahmed Sawaby, Jayant Charthad, Ting Chia Chang, and Amin Arbabian. A Miniaturized Single-Transducer Implantable Pressure Sensor With Time-Multiplexed Ultrasonic Data and Power Links. *IEEE Journal of Solid-State Circuits*, 53(4):1089–1101, 2018.

[5] F. Ellinger, M. Claus, M. Schröter, and C. Carta. Review of advanced and Beyond CMOS FET technologies for radio frequency circuit design. In *2011 IEEE MTT-S International Microwave and Optoelectronics Conference (IMOC 2011)*, pages 347–351, 2011.

[6] Alison M. Yao and Miles J. Padgett. Orbital angular momentum: origins, behavior and applications. *Advances in Optics and Photonics*, 3(2):161–204, June 2011.

[7] Shuang Zheng and Jian Wang. Measuring Orbital Angular Momentum (OAM) States of Vortex Beams with Annular Gratings. *Scientific Reports*, 7(1):40781, Jan 2017.

[8] Microwave Journal. "NTT Successfully Demonstrates 100 Gbps Wireless Transmission Using OAM Multiplexing for the First Time". https://www.microwavejournal.com/articles/30341-ntt-successfully-demonstrates-100-gbps-wireless-transmission-using-oam-multiplexing-for-the-first-time.

[9] NEC Corp. Press. "NEC successfully demonstrates real-time digital OAM mode multiplexing transmission over 100m in the 150GHz-band for the first time". https://www.nec.com/en/press/202003/global_20200310_01.html.

[10] Bozinovic Nenad, Yue Yang, Ren Yongxiong, Tur Moshe, Kristensen Poul, Huang Hao, E. Willner Alan, and Ramachandran Siddharth. Terabit-Scale Orbital Angular Momentum Mode Division Multiplexing in Fibers. *Science*, 340(6140):1545–1548, 2013.

[11] Cheng Wang and Ruonan Han. Rapid and energy-efficient molecular sensing using dual mm-Wave combs in 65nm CMOS: A 220-to-320GHz spectrometer with 5.2mW radiated power and 14.6-to-19.5dB noise figure. In *2017 IEEE International Solid-State Circuits Conference (ISSCC)*, pages 302–303, 2017.

[12] Cheng Wang, Xiang Yi, Mina Kim, Qingyu Ben Yang, and Ruonan Han. A Terahertz Molecular Clock on CMOS Using High-Harmonic-Order Interrogation of Rotational Transition for Medium-/Long-Term Stability Enhancement. *IEEE Journal of Solid-State Circuits*, 56(2):566–580, 2021.

[13] Xibi Chen, Muhammad Ibrahim Wasiq Khan, Xiang Yi, Xingcun Li, Wenhua Chen, Jianfeng Zhu, Yang Yang, Kenneth E. Kolodziej, Nathan M. Monroe, and Ruonan Han. A 140GHz Transceiver with Integrated Antenna, Inherent-Low-Loss Duplexing and Adaptive Self-Interference Cancellation for FMCW Monostatic Radar. In *2022 IEEE International Solid- State Circuits Conference (ISSCC)*, volume 65, pages 80–82, 2022.

[14] Xiang Yi, Cheng Wang, Zhi Hu, Jack W. Holloway, Muhammad Ibrahim Wasiq Khan, Mohamed I. Ibrahim, Mina Kim, Georgios C. Dogiamis, Bradford Perkins, Mehmet Kaynak, Rabia Tugce Yazicigil, Anantha P. Chandrakasan, and Ruonan Han. Emerging terahertz integrated systems in silicon. *IEEE Transactions on Circuits and Systems I: Regular Papers*, pages 1–14, 2021.

[15] Mohamed I. Ibrahim, Muhammad Ibrahim Wasiq Khan, Chiraag S. Juvekar, Wanyeong Jung, Rabia Tugce Yazicigil, Anantha P. Chandrakasan, and Ruonan Han. THzID: A 1.6mm^2 Package-Less Cryptographic Identification Tag with Backscattering and Beam-Steering at 260GHz. In *IEEE International Solid-State Circuits Conference (ISSCC)*, pages 24–26, 2020.

[16] Muhammad Ibrahim Wasiq Khan, Mohamed I. Ibrahim, Chiraag S. Juvekar, Wanyeong Jung, Rabia Tugce Yazicigil, Anantha P. Chandrakasan, and Ruonan Han. CMOS THz-ID: A 1.6-mm^2 Package-Less Identification Tag Using

Asymmetric Cryptography and 260-GHz Far-Field Backscatter Communication. *IEEE Journal of Solid-State Circuits*, 56(2):340–354, 2021.

[17] Muhammad Ibrahim Wasiq Khan, Jongchan Woo, Xiang Yi, Mohamed I. Ibrahim, Rabia Tugce Yazicigil, Anantha Chandrakasan, and Ruonan Han. A 0.31THz CMOS Uniform Circular Antenna Array Enabling Generation/Detection of Waves with Orbital-Angular Momentum. In *2021 IEEE Radio Frequency Integrated Circuits Symposium (RFIC)*, pages 203–206, 2021.

[18] Muhammad Ibrahim Wasiq Khan, Jongchan Woo, Xiang Yi, Mohamed I. Ibrahim, Rabia Tugce Yazicigil, Anantha P. Chandrakasan, and Ruonan Han. A 0.31-THz Orbital-Angular-Momentum (OAM) Wave Transceiver in CMOS With Bits-to-OAM Mode Mapping. *IEEE Journal of Solid-State Circuits*, 57(5):1344–1357, 2022.

[19] Roy Want. An Introduction to RFID Technology. *IEEE Pervasive Computing*, (January-March):25–33, 2006.

[20] Halma plc. "Centrack". https://centrak.com/.

[21] CYBRA Corporation. "Smart seals". https://cybra.com/rfid-smart-seals/.

[22] McKinsey Retail. Future of Retail Operations Winning in a Digital Era. https://www.mckinsey.com/industries/retail/our-insights/future-of-retail-operations-winning-in-a-digital-era.

[23] Retail Shrink. Inventory Shrink Cost The US Retail Industry $46.8 Billion. https: //www.forbes.com/sites/tjmccue/2019/01/31/inventory-shrink-cost-the-us-retail-industry-46-8-billion/4ebcfeed6b70.

[24] Parama Kartika Dewa, I. Nyoman Pujawan, and Iwan Vanany. Human errors in warehouse operations: an improvement model. *International Journal of Logistics Systems and Management*, 27(3):298–317, 2017.

[25] McKinsey Warehousing Costs. Getting a Handle on Warehousing Costs. https://www.mckinsey.com/business-functions/operations/our-insights/getting-a-handle-on-warehousing-costs.

[26] Semiconductor Industry Association Anti-Counterfeiting Task Force. Winning the Battle Against Counterfeit Semiconductor Products. https://www.semiconductors.org/wp-content/uploads/2018/06/SIA-Anti-Counterfeiting-Whitepaper-1.pdf.

[27] Gitanjali Swamy and Sanjay Sarma. *White Paper: Manufacturing Cost Simulations for Low Cost RFID Systems*. MIT Auto-ID Center, 2003.

[28] Hugo Pristauz. RFID Chip Assembly for 0.1 Cents? *OnBoard Technology*, (September):46–49, 2006.

[29] Li-Xuan Chuo, Yao Shi, Zhihong Luo, Nikolaos Chiotellis, Zhiyoong Foo, Gyouho Kim, Yejoong Kim, Anthony Grbic, David Wentzloff, Hun-Seok Kim, and David Blaauw. A 915MHz Asymmetric Radio Using Q-Enhanced Amplifier for a Fully Integrated 3x3x3 mm^3 Wireless Sensor Node with 20m Non-Line-of-Sight Communication. In *IEEE International Solid-State Circuits Conference (ISSCC)*, pages 132–134, 2017.

[30] Bo Zhao, Nai Chung Kuo, Benyuanyi Liu, Yi An Li, Lorenzo Lotti, and Ali M. Niknejad. A 5.8GHz Power-Harvesting 116μmx116μm "Dielet" Near-Field Radio with On-Chip Coil Antenna. In *IEEE International Solid-State Circuits Conference (ISSCC)*, pages 456–458, 2018.

[31] Maryam Tabesh, Mustafa Rangwala, Ali Niknejad, and Amin Arbabian. A Power-Harvesting Pad-Less mm-Sized 24/60GHz Passive Radio with On-Chip Antennas. In *IEEE Symposium of Very-Large-Scale Integrated Circuits (VLSI)*, 2014.

[32] Chiraag Juvekar, Hyung-Min Lee, Joyce Kwong, and Anantha Chandrakasan. A Keccak-Based Wireless Authentication Tag with per-Query Key Update and Power-Glitch Attack Countermeasures. In *IEEE International Solid-State Circuits Conference (ISSCC)*, pages 290–292, 2016.

[33] Stefano Pellerano, Javier Alvarado, and Yorgos Palaskas. A mm-Wave Power-Harvesting RFID Tag in 90 nm CMOS. *IEEE Journal of Solid-State Circuits*, 45(8):1627–1637, 2010.

[34] Taiyun Chi, Hechen Wang, Min-Yu Huang, Fa Foster Dai, and Hua Wang. A Bidirectional Lens-Free Digital-Bit-In/-Out 0.57mm^2 Terahertz Nano-Radio in CMOS with 49.3mW Peak Power Consumption Supporting 50cm Internet-of-Things Communication. In *IEEE Custom Integrated Circuits Conference (CICC)*, 2017.

[35] Maryam Tabesh, Nemat Dolatsha, Amin Arbabian, and Ali M. Niknejad. A Power-Harvesting Pad-Less Millimeter-Sized Radio. *IEEE Journal of Solid-State Circuits (JSSC)*, 50(4):962–977, 2015.

[36] Jens Hermans, Roel Peeters, and Cristina Onete. Efficient, Secure, Private Distance Bounding without Key Updates. In *Proceedings of the 6th ACM Conference Security Privacy Wireless Mobile Network*, pages 207–218, 2013.

[37] Constantine Balanis. *Antenna Theory, Third Edition*. Wiley-Interscience, 2005.

[38] High Frequency Structure Simulator (HFSS) User Guide. http://www.ansys.com/.

[39] Cheng Wang and Ruonan Han. Dual-Terahertz-Comb Spectrometer on CMOS for Rapid, Wide-Range Gas Detection with Absolute Specificity. *IEEE Journal of Solid-State Circuits*, 52(12):3361–3372, 2017.

[40] Erik Öjefors, Ullrich R Pfeiffer, Alvydas Lisauskas, and Hartmut G Roskos. A 0.65 THz Focal-Plane Array in a Quarter-Micron CMOS Process Technology. *IEEE Journal of Solid State Circuits*, 44(7):1968–1976, 2009.

[41] Muhammad Ibrahim Wasiq Khan, Suna Kim, Dae Woong Park, Hyoung Jun Kim, Seok Kyun Han, and Sang Gug Lee. Nonlinear Analysis of Nonresonant THz Response of MOSFET and Implementation of a High-Responsivity Cross-Coupled THz Detector. *IEEE Transactions on Terahertz Science and Technology*, 8(1):108–120, 2018.

[42] Roel Peeters and Jens Hermans. Wide Strong Private RFID Identification based on Zero-Knowledge. *IACR Cryptology ePrint Archive*, 2012:389, 2012.

[43] Peter L Montgomery. Speeding the pollard and elliptic curve methods of factorization. *Mathematics of computation*, 48(177):243–264, 1987.

[44] Marc Joye and Sung-Ming Yen. The montgomery powering ladder. In *International workshop on cryptographic hardware and embedded systems*, pages 291–302. Springer, 2002.

[45] Michael Hutter, Jurgen Schilling, Peter Schwabe, and Wolfgang Wieser. NaCl's Crypto_box in Hardware. In *International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, pages 81–101, Saint-Malo, France, 2015.

[46] Lumerical. FDTD Product Reference Manual. http://www.lumerical.com/.

[47] Harald T. Friis. A Note on a Simple Transmission Formula. *Proceedings of the IRE and Waves and Electrons*, 34(5):254–256, 1946.

[48] Johannes Wolkerstorfer. Scaling ECC Hardware to a Minimum. In *Cryptographic Advances in Secure Hardware (CRASH)*, pages 207–214, Leuven, Belgium, 2005.

[49] Utsav Banerjee, Chiraag Juvekar, Andrew Wright, A. Arvind, and Anantha P. Chandrakasan. An Energy-Efficient Reconfigurable DTLS Cryptographic Engine for End-to-End Security in IoT Applications. In *IEEE International Solid-State Circuits Conference*, San Francisco, CA, 2018. IEEE.

[50] Marc Z. Miskin, Alejandro J. Cortese, Kyle Dorsey, Edward P. Esposito, Michael F. Reynolds, Qingkun Liu, Michael Cao, David A. Muller, Paul L. McEuen, and Itai Cohen. Electronically integrated, mass-manufactured, microscopic robots. *Nature*, 584(7822):557–561, Aug. 2020.

[51] Pingyang He, Dixian Zhao, Liang Liu, Jie Xu, Qianglin Zheng, Chuan Yu, and Xiaohu You. A W-Band 2×2 Rectenna Array With On-Chip CMOS Switching Rectifier and On-PCB Tapered Slot Antenna for Wireless Power Transfer. *IEEE Transactions on Microwave Theory and Techniques*, 69(1):969–979, 2021.

[52] Pingyang He and Dixian Zhao. High-Efficiency Millimeter-Wave CMOS Switching Rectifiers: Theory and Implementation. *IEEE Transactions on Microwave Theory and Techniques*, 67(12):5171–5180, 2019.

[53] Med Nariman, Farid Shirinfar, Anna Papió Toda, Sudhakar Pamarti, Ahmadreza Rofougaran, and Franco De Flaviis. A Compact 60-GHz Wireless Power Transfer System. *IEEE Transactions on Microwave Theory and Techniques*, 64(8):2664–2677, 2016.

[54] Pascal Burasa, Nicolas G. Constantin, and Ke Wu. High-Efficiency Wideband Rectifier for Single-Chip Batteryless Active Millimeter-Wave Identification (MMID) Tag in 65-nm Bulk CMOS Technology. *IEEE Transactions on Microwave Theory and Techniques*, 62(4):1005–1011, 2014.

[55] Edoh Shaulov, Samuel Jameson, and Eran Socher. W-band energy harvesting rectenna array in 65-nm CMOS. In *2017 IEEE MTT-S International Microwave Symposium (IMS)*, pages 307–310, 2017.

[56] Nir Weissman, Samuel Jameson, and Eran Socher. W-Band CMOS on-chip energy harvester and rectenna. In *2014 IEEE MTT-S International Microwave Symposium (IMS2014)*, pages 1–3, 2014.

[57] Hao Gao, Marion K. Matters-Kammerer, Pieter Harpe, Dusan Milosevic, Ulf Johannsen, Arthur van Roermund, and Peter Baltus. A 71GHz RF energy harvesting tag with 8% efficiency for wireless temperature sensors in 65nm CMOS. In *2013 IEEE Radio Frequency Integrated Circuits Symposium (RFIC)*, pages 403–406, 2013.

[58] H Lee, S Rami, S Ravikumar, V Neeli, K Phoa, B Sell, and Y Zhang. Intel 22nm FinFET (22FFL) Process Technology for RF and mmWave Applications and Circuit Design Optimization for FinFET Technology. In *2018 IEEE International Electron Devices Meeting (IEDM)*, pages 316–319, San Francisco, CA, 2018. IEEE.

[59] John Henry Poynting. The wave motion of a revolving shaft, and a suggestion as to the angular momentum in a beam of circularly polarised light. *Proceedings of the Royal Society London*, 82:560–567, July 1909.

[60] Richard A. Beth. Direct Detection of the Angular Momentum of Light. *Phys. Review*, 48:471–471, Sep 1935.

[61] Richard A. Beth. Mechanical Detection and Measurement of the Angular Momentum of Light. *Phys. Review*, 50:115–125, Jul 1936.

[62] V.Y. Bazhenov, M.V. Vasnetsov, and M.S. Soskin. Laser beams with screw dislocations in their wavefronts. *Journal of Experimental and Theoretical Physics*, 52:429–431, Oct 1990.

[63] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, and J. P. Woerdman. Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes. *Phys. Review A*, 45:8185–8189, Jun 1992.

[64] B. Thidé, H. Then, J. Sjöholm, K. Palmer, J. Bergman, T. D. Carozzi, Ya. N. Istomin, N. H. Ibragimov, and R. Khamitova. Utilization of Photon Orbital Angular Momentum in the Low-Frequency Radio Domain. *Physical Review Letters*, 99:087701, Aug 2007.

[65] Fabrizio Tamburini, Elettra Mari, Bo Thidé, Cesare Barbieri, and Filippo Romanato. Experimental verification of photon angular momentum and vorticity with radio techniques. *Applied Physics Letters*, 99(20):204102, 2011.

[66] The orbital angular momentum of light. volume 39 of *Progress in Optics*, pages 291 – 372. Elsevier, 1999.

[67] Y. Yan, X. Guodong, L. Martin P. J., H. Hao, A. Nisar, B. Changjing, R. Yongxiong, C. Yinwen, L. Long, Z. Zhe, M. Andreas F. T. Moshe, P. Miles J., and W. Alan E. High-capacity millimetre-wave communications with orbital angular momentum multiplexing. *Nature Communications*, Sep. 2014.

[68] Li Cheng, Wei Hong, and Zhang-Cheng Hao. Generation of Electromagnetic Waves with Arbitrary Orbital Angular Momentum Modes. *Scientific Reports*, 4(1), 2014.

[69] Anass Beniss, Ronan Niemiec, Christian Brousseau, Kouroch Mahdjoubi, and Olivier Emile. Flat plate for OAM generation in the millimeter band. page 1, Gothenburg, Sweden, April 2013.

[70] Kang Liu, Hongyan Liu, Yuliang Qin, Yongqiang Cheng, Shunan Wang, Xiang Li, and Hongqiang Wang. Generation of OAM Beams Using Phased Array in the Microwave Band. *IEEE Transactions on Antennas and Propagation*, 64(9):3850–3857, 2016.

[71] W. Zhang, S. Zheng, X. Hui, R. Dong, X. Jin, H. Chi, and X. Zhang. Mode Division Multiplexing Communication Using Microwave Orbital Angular Momentum: An Experimental Study. *IEEE Transactions on Wireless Communications*, 16(2):1308–1318, 2017.

[72] H. Sasaki, Y. Yagi, T. Yamada, T. Semoto, and D. Lee. An Experimental Demonstration of over 100 Gbit/s OAM Multiplexing Transmission at a Distance of 100 m on 40 GHz Band. In *2020 IEEE International Conference on Communications Workshops*, pages 1–6, 2020.

[73] Shixing Yu, Long Li, Guangming Shi, Cheng Zhu, Xiaoxiao Zhou, and Yan Shi. Design, fabrication, and measurement of reflective metasurface for orbital angular momentum vortex wave in radio frequency domain. *Applied Physics Letters*, 108(12):121903, 2016.

[74] W. Cheng, W. Zhang, H. Jing, S. Gao, and H. Zhang. Orbital Angular Momentum for Wireless Communications. *IEEE Wireless Communications*, 26(1):100–107, Feb. 2019.

[75] O. Edfors and A. J. Johansson. Is Orbital Angular Momentum (OAM) Based Radio Communication an Unexploited Area? *IEEE Transactions on Antennas and Propagation*, 60(2):1126–1131, 2012.

[76] Shuping Dang, Osama Amin, Basem Shihada, and Mohamed Slim Alouini. What should 6G be? *Nature Electronics*, 3(1):20–29, 2020.

[77] Theodore S. Rappaport, Yunchou Xing, Ojas Kanhere, Shihao Ju, Arjuna Madanayake, Soumyajit Mandal, Ahmed Alkhateeb, and Georgios C. Trichopoulos. Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond. *IEEE Access*, 7:78729–78757, 2019.

[78] Michele Polese, Josep Jornet, Tommaso Melodia, and Michele Zorzi. Toward end-to-end, full-stack 6G terahertz networks. *IEEE Communications Magazine*, 58(11):48–54, 2020.

[79] Vitaly Petrov, Thomas Kurner, and Iwao Hosako. IEEE 802.15.3d: first standardization efforts for sub-terahertz band communications toward 6G. *IEEE Communications Magazine*, 58(11):28–33, 2020.

[80] *Federal Communication Commission (FCC) takes steps to Open Spectrum Horizons for New Services and Technologies. https://docs.fcc.gov/public/attachments/DOC-356588A1.pdf.*

[81] H. Vincent Poor and Rafael F. Schaefer. Wireless physical layer security. *Proceedings of the National Academy of Sciences*, 114(1):19–26, 2017.

[82] Jianjun Ma, Rabi Shrestha, Jacob Adelberg, Chia-Yi Yeh, Zahed Hossain, Edward Knightly, Josep Miquel Jornet, and Daniel M. Mittleman. Security and eavesdropping in terahertz wireless links. *Nature*, 563:89–93, Nov 2018.

[83] W. Huang, Y. Li, D. Wei, and Q. Zhang. Research on Physical Layer Security Scheme Based on OAM. volume 11604, page 573–586, Jun. 2019.

[84] I. B. Djordjevic. OAM-Based Hybrid Free-Space Optical-Terahertz Multidimensional Coded Modulation and Physical-Layer Security. *IEEE Photonics Journal*, 9(4):1–12, 2017.

[85] Aydin Babakhani, David B. Rutledge, and Ali Hajimiri. Transmitter Architectures Based on Near-Field Direct Antenna Modulation. *IEEE Journal of Solid-State Circuits*, 43(12):2674–2692, 2008.

[86] Jixin Guo, Lorenzo Poli, Mohammad Abdul Hannan, Paolo Rocca, Shiwen Yang, and Andrea Massa. Time-Modulated Arrays for Physical Layer Secure Communications: Optimization-Based Synthesis and Experimental Assessment. *IEEE Transactions on Antennas and Propagation*, 66(12):6939–6949, 2018.

[87] Quanjiang Zhu, Shiwen Yang, Ruilin Yao, and Zaiping Nie. Directional Modulation Based on 4-D Antenna Arrays. *IEEE Transactions on Antennas and Propagation*, 62(2):621–628, 2014.

[88] X. Lu, S. Venkatesh, B. Tang, and K. Sengupta. Space-Time Modulated 71-to-76GHz mm-Wave Transmitter Array for Physically Secure Directional Wireless Links. In *2020 IEEE International Solid- State Circuits Conference - (ISSCC)*, pages 86–88, Feb 2020.

[89] F. Meng, K. Ma, K. S. Yeo, C. C. Boon, W. M. Lim, and S. Xu. A 220–285 GHz SPDT Switch in 65-nm CMOS Using Switchable Resonator Concept. *IEEE Transactions on Terahertz Science and Technology*, 5(4):649–651, 2015.

[90] Muhammad Ibrahim Wasiq Khan, Mohamed I. Ibrahim, Chiraag S. Juvekar, Wanyeong Jung, Rabia Tugce Yazicigil, Anantha P. Chandrakasan, and Ruonan Han. CMOS THz-ID: A 1.6-mm^2 Package-Less Identification Tag Using Asymmetric Cryptography and 260-GHz Far-Field Backscatter Communication. *IEEE Journal of Solid-State Circuits*, 56(2):340–354, 2021.

[91] Xiang Yi, Cheng Wang, Xibi Chen, Jinchen Wang, Jesús Grajal, and Ruonan Han. A 220-to-320-GHz FMCW Radar in 65-nm CMOS Using a Frequency-Comb Architecture. *IEEE Journal of Solid-State Circuits*, 56(2):327–339, 2021.

[92] Guido Bertoni, Michaël Peeters, Gilles Van Assche, et al. The Keccak reference. https://keccak.team/files/Keccak-reference-3.0.pdf. 2011.

[93] H. Lee, C. S. Juvekar, J. Kwong, and A. P. Chandrakasan. A Nonvolatile Flip-Flop-Enabled Cryptographic Wireless Authentication Tag With Per-Query Key Update and Power-Glitch Attack Countermeasures. *IEEE Journal of Solid-State Circuits*, 52(1):272–283, 2017.

[94] Gavriel Iddan, Gavriel Meron, Arkady Glukhovsky, and Paul Swain. Wireless capsule endoscopy. *Nature*, 405(6785):417–417, May 2000.

[95] Peter J van der Schaar, J Frits Dijksman, Henny Broekhuizen-de Gast, Jeff Shimizu, Niels van Lelyveld, Hans Zou, Ventzeslav Iordanov, Christoph Wanke, and Peter D Siersema. A novel ingestible electronic drug delivery and monitoring device. *Gastrointestinal Endoscopy*, 78(3):520–528, May 2013.

[96] Sabba Maqbool, Henry P Parkman, and Frank K Friedenberg. Wireless capsule motility: comparison of the SmartPill GI monitoring system with scintigraphy for measuring whole gut transit. *Digestive Diseases and Sciences*, 54(10):2167–2174, Aug 2009.

[97] G. Traverso, G. Ciccarelli, S. Schwartz, T. Hughes, T. Boettcher, R. Barman, R. Langer, and A. Swiston. Physiologic Status Monitoring via the Gastrointestinal Tract. *PLOS ONE*, 10(11):1–13, 11 2015.

[98] Bluetooth SIG Standard, 2020. Bluetooth Specification Version 5.2. https://www.bluetooth.com/specifications/specs/.

[99] Arun Paidimarri, Phillip M. Nadeau, Patrick P. Mercier, and Anantha P. Chandrakasan. A 2.4 GHz Multi-Channel FBAR-based Transmitter With an Integrated Pulse-Shaping Power Amplifier. *IEEE Journal of Solid-State Circuits*, 48(4):1042–1054, 2013.

[100] Arun Paidimarri, Nathan Ickes, and Anantha P. Chandrakasan. A +10 dbm ble transmitter with sub-400 pw leakage for ultra-low duty cycles. *IEEE Journal of Solid-State Circuits*, 51(6):1331–1346, 2016.

[101] J.D. Larson, P.D. Bradley, S. Wartenberg, and R.C. Ruby. Modified Butterworth-Van Dyke circuit for FBAR resonators and automated measurement system. In *2000 IEEE Ultrasonics Symposium. Proceedings. An International Symposium (Cat. No.00CH37121)*, volume 1, pages 863–868 vol.1, 2000.

[102] Y.H. Chee, A.M. Niknejad, and J. Rabaey. A sub-100μ W 1.9-GHz CMOS oscillator using FBAR resonator. In *2005 IEEE Radio Frequency integrated Circuits (RFIC) Symposium - Digest of Papers*, pages 123–126, 2005.

[103] Mohamed Hussein Eissa and Dietmar Kissinger. A 13.5dBm Fully Integrated 200-to-255GHz Power Amplifier with a 4-Way Power Combiner in SiGe:C BiCMOS. In *IEEE International Solid-state Circuits Conference (ISSCC)*, pages 82–84, San Francisco, CA, 2019. IEEE.

[104] B Heinemann, H Rücker, R Barth, F Bärwolf, J Drews, G G Fischer, A Fox, O Fursenko, T Grabolla, F Herzel, J Katzer, J Korn, A Krüger, P Kulse, T Lenke, M Lisker, S Marschmeyer, A Scheit, D Schmidt, J Schmidt, M A Schubert, A Trusch, C Wipf, and D Wolansky. SiGe HBT with fT/fmax of 505 GHz/720 GHz. In *IEEE International Electron Device Meeting*, pages 51–54, San Francisco, CA, 2016.

[105] S. N. Ong, S. Lehmann, W. H. Chow, C. Zhang, C. Schippel, L. H.K. Chan, Y. Andee, M. Hauschildt, K. K.S. Tan, J. Watts, C. K. Lim, A. Divay, J. S. Wong, Z. Zhao, M. Govindarajan, C. Schwan, A. Huschka, A. Bcllaouar, W. Loo, J. Mazurier, C. Grass, R. Taylor, K. W.J. Chew, S. Embabi, G. Workman, A. Pakfar, S. Morvan, K. Sundaram, M. T. Lau, B. Rice, and D. Harame. A 22nm FDSOI Technology Optimized for RF/mmWave Applications. In *IEEE Radio Frequency Integrated Circuits Symposium*, 2018.

[106] H. J. Lee, S. Morarka, S. Rami, Q. Yu, M. Weiss, G. Liu, M. Armstrong, C.-Y. Su, D. Ali, B. Sell, and Y. Zhang. Implementation of High Power RF Devices with Hybrid Workfunction and OxideThickness in 22nm Low-Power FinFET

Technology. In *IEEE International Electron Devices Meetings (IEDM)*, pages 610–613, San Francisco, CA, 2019.

[107] N. B. Simpson, K. Dholakia, L. Allen, and M. J. Padgett. Mechanical equivalence of spin and orbital angular momentum of light:an optical spanner. *Optics Letters*, 22(1):52–54, Jan 1997.

[108] Netanel Biton, Judy Kupferman, and Shlomi Arnon. OAM light propagation through tissue. *Scientific Reports*, 11(1):2407, Jan 2021.

[109] Richard Neo, Sergio Leon-Saval, Joss Bland-Hawthorn, and Gabriel Molina-Terriza. OAM interferometry: the detection of the rotational Doppler shift. *Optics Express*, 25(18):21159–21170, Sep 2017.

[110] Aldert Van Der Ziel. Noise in Solid-State Devices and Lasers. *Proceedings of the IEEE*, 58(8):1178–1206, 1970.

[111] U. F. Gianola. Photovoltaic Noise in Silicon Broad Area p-n Junctions. *Journal of Applied Physics*, 27(1):51–54, 1956.