# CMOS THz-ID: A 1.6-mm$^2$ Package-Less Identification Tag Using Asymmetric Cryptography and 260-GHz Far-Field Backscatter Communication

Muhammad Ibrahim Wasiq Khan, *Graduate Student Member, IEEE*, Mohamed I. Ibrahim, *Student Member, IEEE*, Chiraag S. Juvekar, *Member, IEEE*, Wanyeong Jung, *Member, IEEE*, Rabia Tugce Yazicigil, *Member, IEEE*, Anantha P. Chandrakasan, *Fellow, IEEE*, and Ruonan Han, *Senior Member, IEEE*

***Abstract*— This article presents an ultra-small, high-security identification tag that is entirely built in a CMOS chip without external components. The usage of backscatter 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 backscatter 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 beamsteering for enhanced link budget. For authentication and secure wireless data transmission, the tag also integrates a compact elliptic-curve-cryptography (ECC) dedicated processor, which is based on a narrow-strong private identification protocol. The presented tag has a peak power consumption of 21 $\mu$W and can be powered by a chip-wide array of photodiodes and a DC–DC converter. Using a low-cost 65-nm bulk CMOS technology, the terahertz (THz) ID chip has an area of only 1.6 mm$^2$ and demonstrates the measured downlink speed of 100 kb/s and the upload speed of 2 kb/s 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 tag size is the smallest among all prior radio-frequency identifications (RFIDs) using far-field communications.**

***Index Terms*— Backscatter communication, beamsteering, CMOS, elliptic-curve cryptography (ECC), far field, identification tag, package-less, radio-frequency identification (RFID), security, terahertz (THz).**

## I. Introduction

RADIO-FREQUENCY identification (RFID) tags have been widely adopted in tracking, authentication, localization, supply-chain management, and so on [1]. At present, commercial RFID chips rely on external antenna or inductor packaging to facilitate efficient coupling of the RF waves. This, 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 the chip packaging, which takes up to two thirds of the total tag cost [2], [3]. This makes RFID technologies much less competitive than, for example, printed barcodes for low-cost products (e.g., a 50-cent candy bar) [1]. 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.

In order to enable secure and ubiquitous asset tagging, fully passive, particle-sized cryptographic chips without external packaging are highly desired. However, the recently demonstrated prototypes [4]–[8] that took the above path face either size, energy, communication, or security limitations. In [4], a 9-mm$^2$ sensor node (volume = 27 mm$^3$) is implemented out of a stacked packaging of multiple functionality layers for photo-voltaic powering, battery, antenna, and so on, which increases the overall cost. In [5], a $116 \times 116$ $\mu$m$^2$ monolithic radio chip is demonstrated, but it relies on near-field inductive coupling at 5.8 GHz, which severely limits the operation range to $\sim$1 mm. In comparison, far-field tag interrogation using

Manuscript received May 13, 2020; revised July 18, 2020; accepted August 6, 2020. Date of publication August 24, 2020; date of current version January 28, 2021. This article was approved by Associate Editor K. Okada. This work was supported by the National Science Foundation under Grant SpecEES ECCS-1824360. This paper was presented at the IEEE Solid-State Circuit Conference (ISSCC), San Francisco, CA, USA, February 2020. *(Corresponding author: Muhammad Ibrahim Wasiq Khan.)*

Muhammad Ibrahim Wasiq Khan, Mohamed I. Ibrahim, Anantha P. Chandrakasan, and Ruonan Han are with the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology (MIT), Cambridge, MA 02139 USA (e-mail: ibrahimw@mit.edu).

Chiraag S. Juvekar was with the Massachusetts Institute of Technology (MIT), Cambridge, MA 02139 USA. He is now with Analog Devices Inc., Boston, MA 02110 USA.

Wanyeong Jung was with the Massachusetts Institute of Technology (MIT), Cambridge, MA 02139 USA. He is now with the Department of Electrical Engineering and Computer Science, Korea Advanced Institute of Technology, Daejeon 34141, South Korea.

Rabia Tugce Yazicigil is with the Department of Electrical and Computer Engineering, Boston University, Boston, MA 02215 USA.

Color versions of one or more of the figures in this article are available online at https://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSSC.2020.3015717

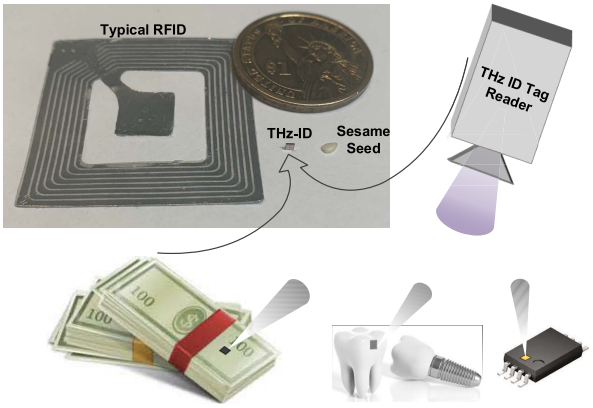



Fig. 1. Cryptographic THz-ID tag: a size comparison and its potential applications.

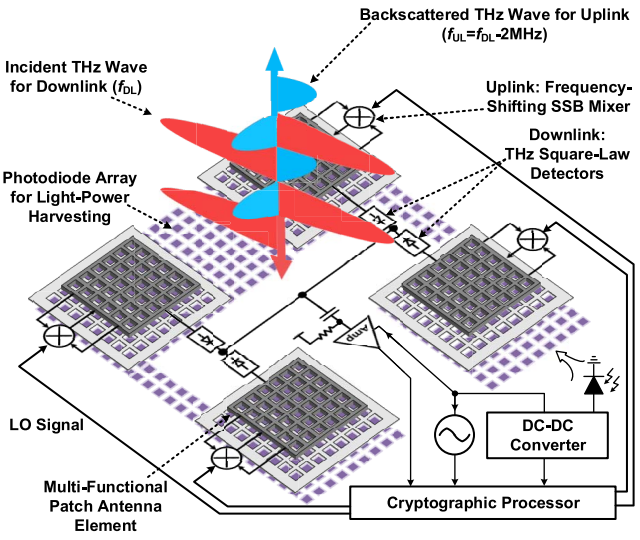



Fig. 2. Overall architecture of the THz-ID tag.

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 [6], but the chip-integrated transmitter (Tx) and receiver (Rx) antennas also increase the chip size to $3.7 \times 1.2$ mm$^2$. While this is already an impressive form factor, to fully enable the applications described previously, further miniaturization is desired. It is also noteworthy that the abovementioned three works [4]–[6] also do not support cryptographically secure identification. To this end, Juvekar *et al.* [7] demonstrated a secure authentication tag, but the chip requires an 8-mm$^2$ external antenna; moreover, only a symmetric-key cryptography is realized due to the limitations of size and energy.

In this article, we present a package-less, monolithic tag chip in CMOS, that has a size of $1.2 \times 1.3$ mm$^2$ (shown in Fig. 1) [9]. To enable far-field operation with such small form factor, the downlink/uplink carrier frequency is pushed into the low terahertz (THz) regime (260 GHz). This, along with a Tx–Rx antenna sharing technique, allows for an on-chip integration of a $2 \times 2$ antenna array and a tag-side, beamsteering capability. An operation range of 5 cm is demonstrated, which makes barcode-reader-like applications possible. 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 $\mu$W, which is provided by an array of chip-integrated photodiodes. This article is organized as follows. In Section II, the overall architecture of the chip is described. Details of the THz downlink and uplink circuits are given in Section III. Then, Section IV presents the design of the ECC security processor. The photo-voltaic powering scheme is discussed in Section V. After showing the experiments and demonstrations in Section VI, we conclude this article in Section VII with comparisons with the prior state of the arts.

## II. Tag Hardware Architecture

The architecture of the tag chip is shown in Fig. 2. The incident 260-GHz wave (red) from the reader is coupled to a $2 \times 2$ 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 $\sim$1:1. Half of this power, used for the downlink, is rectified to baseband via four THz square-law detectors. The other half of the input power is used for the backscatter uplink communication. It is noteworthy that a strong, direct reflection of the incident downlink wave, due to the large surface of the object to be tagged, is inevitable. It is, therefore, critical to eliminate the interference of such reflected waves to the actual data-modulated signal, which is backscattered by the chip. To this end, single-sideband (SSB) frequency mixing is added to the backscattering process, so that the final carrier frequency for the uplink ($f_{\mathrm{UL}}$) is $\sim$2 MHz below that for the downlink ($f_{\mathrm{DL}}$). Meanwhile, the chip is designed so that the polarization of the backscattered wave (blue in Fig. 2) is also rotated by 90° so that the tag reader's Rx antenna with a linear polarization aligned with the backscattered wave can further suppress the directly 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 $\sim 2\times$. More details of the antennas will be given in Section III-A.

Both the downlink and the uplink utilize on/off-shift-keying (OOK) modulation and offer data rates at 100 and 2 kb/s, 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 cryptographic processor. With independent, digital control of the phase in each LO, beamsteering for the THz uplink wave is achieved. This enhances the link budget when the tag is not perpendicularly facing the tag reader. Moreover, without the beamsteering capability, the tag would act like a mirror and make the backscatter 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 [10] under a public-key cryptography scheme (specifically elliptical-curve cryptograhy). It 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.

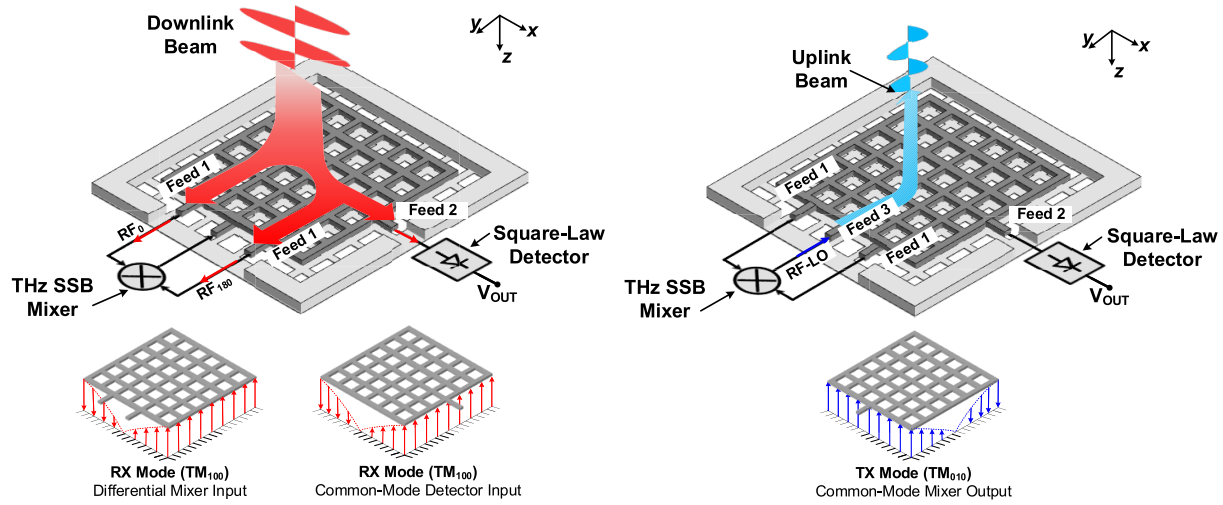



Fig. 3. Schematic of the multi-port patch antenna with excited (a) $TM_{100}$ for downlink and (b) $TM_{010}$ for uplink.

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 fishnet pattern (see Fig. 2). A DC–DC converter is implemented in order to boost the photodiode output voltage to ∼1 V. An 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.

## III. THz Downlink and Uplink

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

### A. Multi-Functional On-Chip Patch Antenna

To enable front-side radiation, the tag integrates $2 \times 2$ patch antennas that are shared between the downlink and the 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 shown in Fig. 3(a), 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 antenna, the received power is split into the two feeds for backscatter (Feed 1) and downlink demodulation (Feed 2). Accordingly, the THz SSB mixer has a differential input, whereas the THz square-law detector for the OOK de-modulation of downlink has a single-ended input [see Fig. 3(a)].

Next, to radiate the uplink signal with orthogonal polarization, the $TM_{010}$ mode of the same antenna is used [see Fig. 3(b)] 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 III-B. 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 [see Fig. 4(a)].[1]

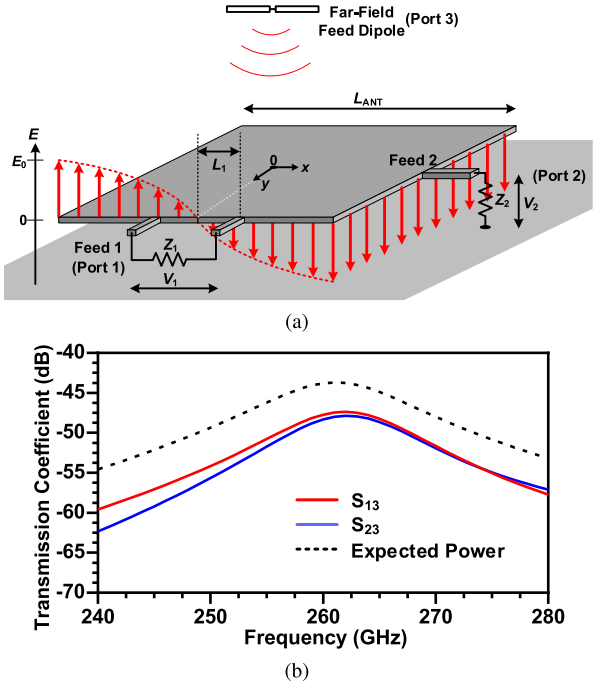



Fig. 4. (a) Electrical-field distribution of the $TM_{100}$ mode in the multi-port antenna. (b) Simulated power transmission coefficients from a far-field feed dipole (2 cm away) to the two ports associated with the downlink, when they are terminated by $Z_1 = 150\ \Omega$ and $Z_2 = 450\ \Omega$, respectively. 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 ports 1 and 2 are equal and maximized.

To ensure the reliability of both the downlink de-modulation and the backscattering, the power splitting ratio in Fig. 3(a)

[1]We, however, 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 III-B.

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. 4(a)]. 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 ground) along the $x$-direction approximately follows an anti-symmetric sinusoidal pattern [see Fig. 4(a)] and can be expressed as [11]:

$$V(x) = V_0 \cdot \sin \frac{\pi x}{2L_{\text{ANT}}} \tag{1}$$

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

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

where $L_1$ is the distance of each Feed 1 wire from the antenna edge center [see Fig. 4(a)]. For equal power splitting (i.e., $P_1 = P_2$), the required ratio $K$ is derived

$$K = \frac{Z_2}{Z_1} = \frac{1}{4\left(\sin \frac{\pi L_1}{2L_{\text{ANT}}}\right)^2}. \tag{3}$$

In our design, the value of $L_1/L_{\text{ANT}}$, 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 [12], with a far-field half-wave dipole antenna [port 3 in Fig. 4(a)]. 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 of $K = 3$). When $Z_1 = 150\ \Omega$ and $Z_2 = 450\ \Omega$, maximum total power transfer from the feed dipole to the two patch antenna ports ($S_{13}$ and $S_{23}$ in Fig. 4) is obtained, meaning that the wave reflection on the antenna is minimum. Fig. 4(b) shows the simulated power transmission co-efficient (including free-space propagation loss) when the abovementioned 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 $\mu$m in the $x$-direction and 235 $\mu$m 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 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 $\mu$m away from the patch at all sides. This reduces the coupling with neighboring electronics and antennas, while its effect on the antenna performance is negligible. 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.

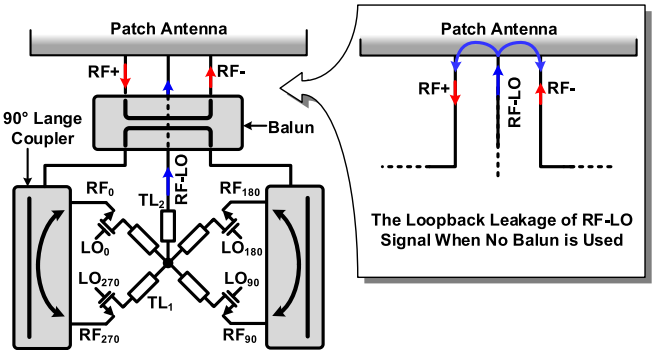



Fig. 5. Schematic of the backscattering module consisting of a passive SSB mixer, a balun, and two 90° Lange couplers. The loopback effect with the absence of the input balun is also shown.

### *B. THz Frequency-Shifting Backscatter Module*

Instead of using a dedicated Tx signal source on a tag [6], which is too power hungry to be practical for THz IDs, our uplink adopts an energy-efficient backscatter scheme for the incident wave. As described in Section II, the backscatter module applies a frequency shifting to the THz signal. As shown in Fig. 5, the backscatter module consists of a passive single-side (SSB) band 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. Next, details of the components in the backscatter module are given.

*1) Input Balun:* In Fig. 3(b), 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 $f_{\text{LO}}$ 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 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 (RPG)-based balun introduced in [13] is used, which consists of two microstrip lines coupled via a slot in the ground plane [i.e., RPG, see Fig. 6(a)]. 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. This is illustrated in the electromagnetic simulation shown in Fig. 6(b), 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 $>$10 dB from 240 to 280 GHz. The balun is implemented using 2-$\mu$m-wide M9 microstrip lines and slots in a shunted M1–M3 ground. Note that a wire placed along the central line of the balun connects the SSB mixer output ($f_{\text{RF}} - f_{\text{LO}}$) and the antenna (see Fig. 5); 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.

*2) Coupler:* The Lange coupler that generates the quadrature phases for the input 260-GHz signal is shown in Fig. 7(a).

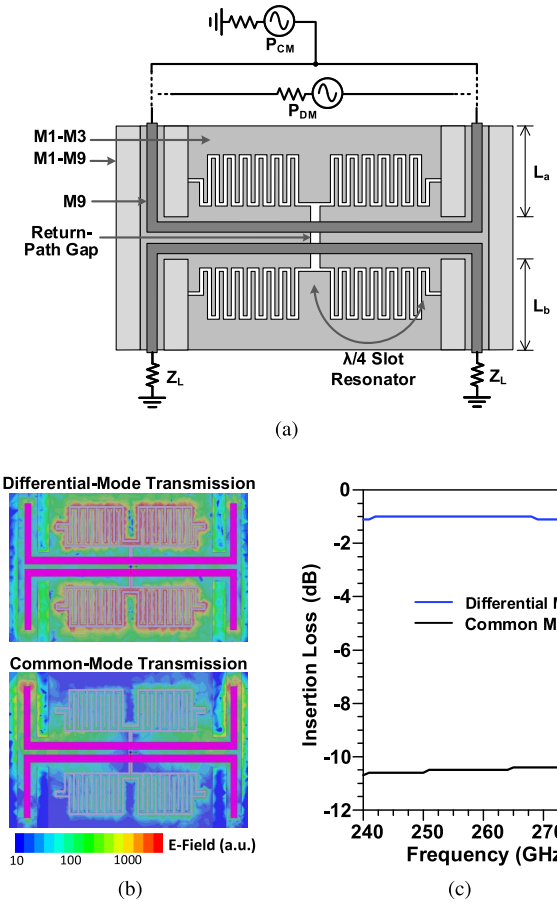



Fig. 6. 260-GHz balun based on an RPG. (a) Structure, (b) simulated electrical-field distribution, and (c) simulated insertion loss from the input to one load $Z_L$.

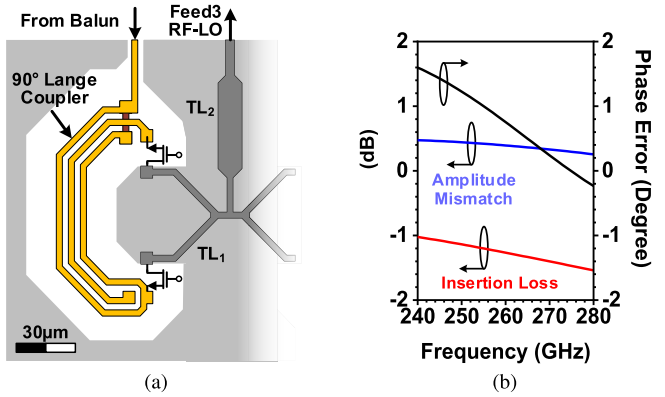



Fig. 7. (a) Structure of the 260-GHz Lange coupler in the backscatter module. (b) Simulated insertion loss and output mismatch of the coupler.

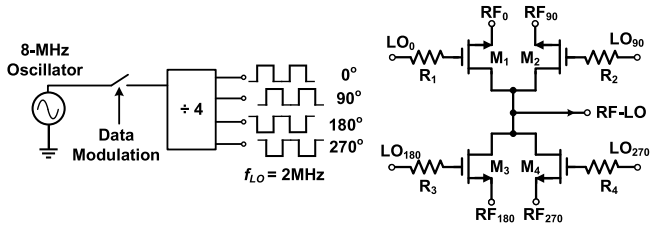



Fig. 8. Schematic of the 260-GHz passive SSB mixer.

The electromagnetic simulation results are shown in Fig. 7(b); 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-$\mu$m-wide lines and 3-$\mu$m spacing among the lines. The couplers are also enclosed by a ground plane (with a spacing of 15 $\mu$m to provide the signal's return path and to minimize the coupling to surrounding structures.

*3) Passive 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 beamsteering. This lowers the security and causes signal loss and interference. In our design, an 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. As shown in Fig. 8, 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.[2] 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, whereas the upper sidebands cancel. MOSFETs in the 65-nm bulk CMOS process have poor switching performance at THz; although wider channel provides smaller ON-resistance, there is also 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-k$\Omega$ resistors ($R_1 \sim R_4$ in Fig. 8) are added in series with the transistor gates, which improves the mixer insertion loss from 15.5 to 13.5 dB in the simulation. Lastly, the OOK uplink modulation is realized by a data-controlled gating of the LO signals.

As shown in Fig. 7(a), 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. However, $TL_2$ 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.

The simulated differential impedance of the whole backscattered module is very close to the desired 150 $\Omega$ (see Section III-A) 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. 6(a)] of the transmission lines connecting the balun to the antenna and coupler, respectively. The simulated common-mode impedance of the backscattering module is largely capacitive (4.2-347.4j $\Omega$). The small real impedance ensures that the radiation efficiency for uplink signal is not affected by the loading at Feed 1.

In Fig. 9, we show the electromagnetic-circuit co-simulation results of the entire backscatter 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

[2]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°, and 315° in Fig. 8) provided in our divide-by-4 scheme is utilized to demonstrate the beamsteering of uplink wave.

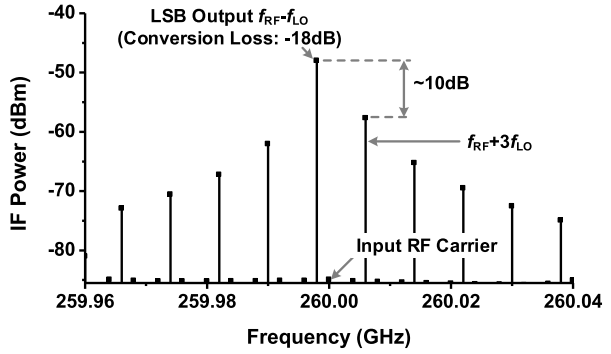



Fig. 9. Simulated output spectrum of the THz backscatter module with a −30-dBm RF input ($f_{RF} = 260$ GHz) and quadrature LO signals at $f_{LO} = 2$ MHz.

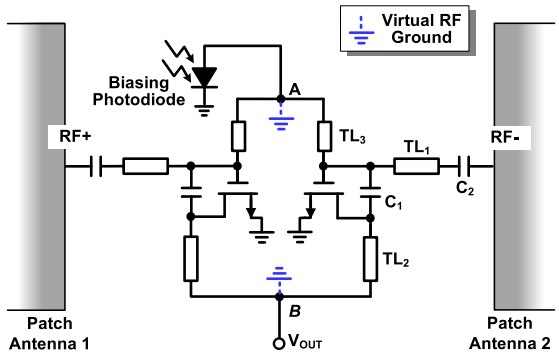



Fig. 10. Schematic of a photovoltaically biased THz square-law detector pair.

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 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 backscattered signal, being the sum of the RF and LO phase noise, is not deteriorated by the ultra-low-power tag LO because the 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).

### *C. THz Downlink Circuits*

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

*1) THz Square-Law Detector:* To achieve zero DC power and low flicker noise, our 260-GHz square-law detector is based on a 2.4-$\mu$m/65-nm NMOS device with zero drain bias. Similar to other FET-based THz detectors [14], [15], the optimal responsivity and noise-equivalent power (NEP) occur at a gate bias around the threshold voltage $V_T$ of the transistor. Conventional VDD-powered circuits, due to the tag's energy harvesting operation, have large bias voltage fluctuation. Fortunately, in our CMOS process, the threshold voltage ($V_T \approx 0.4$ V) is close to the light-insensitive, open-circuit

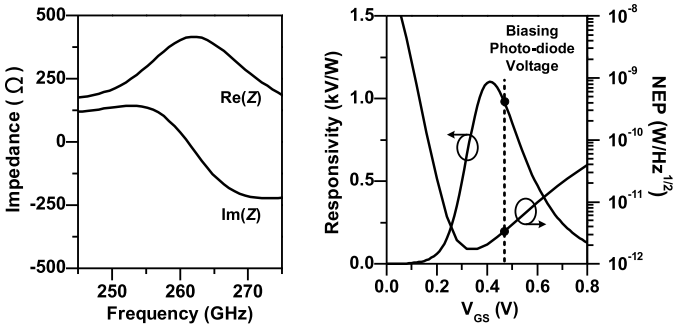



Fig. 11. (a) Simulated impedance of the detector presented to Feed 2 of the antenna. (b) Simulated responsivity and NEP of the detector.

voltage of a p-n photodiode ($V_{PD} \approx 0.47$ V). Therefore, a simple photovoltaic-biasing circuit shown in Fig. 10 is 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. 10 is used, which utilizes the property that the THz downlink signals extracted, respectively, from the adjacent edges of two patch antennas (see Fig. 2) are differential. As a result, in the symmetric circuit topology in Fig. 10, virtual RF grounds are formed at nodes 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. 10, $C_1$ (∼50 fF) creates an ac short and therefore facilitates THz self-mixing in the diode-connected MOSFET. $C_2$ (∼15 fF) provides DC isolation from the uplink backscatter module and together with $TL_1$ (0.35$\lambda$) form a matching network to present an impedance that is derived in Section III-A for equal power splitting. The insertion loss of matching network is 1 dB. $TL_1$∼$TL_3$ are 75 Ω coplanar-waveguide (CPW) transmission lines implemented using the M9 layer. As shown in Fig. 11(a), the simulated overall impedance of the detector circuit is close to the desired impedance value of 450 Ω. Lastly, Fig. 11(b) shows that at the photodiode bias voltage of ∼470 mV, the simulated responsivity and 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 the Appendix, is small and does not transfer to the transistor output, given that the transistor is in the triode mode.

*2) Ultra-Low-Power Amplifier:* As shown in Fig. 12(a), 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 cutoff 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 is 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.

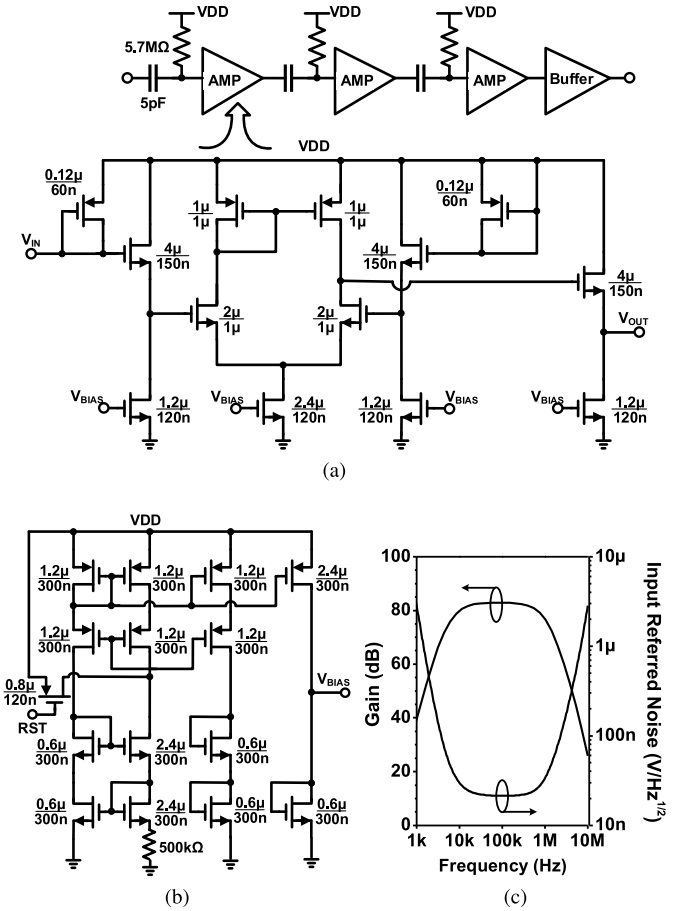



Fig. 12. Ultra-low-power amplifier in the tag downlink. (a) Schematic of the main amplifier chain. (b) Cascode constant-$g_m$ bias generation circuit. (c) Simulated voltage gain.

Each amplifier stage consists of an input NMOS differential pair, which is preceded 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 $V_{\mathrm{BIAS}}$ in Fig. 12(a) is generated from a cascode constant-$g_m$ circuit [see Fig. 12(b)]. 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 ∼1 V. As shown in Fig. 12, 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 $\mu$W.

The high gain is to ensure the 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.

## IV. Cryptographic Security Processor

Fig. 13 shows the cryptographic processor, which implements a 128-bit secure ECC-based private ID

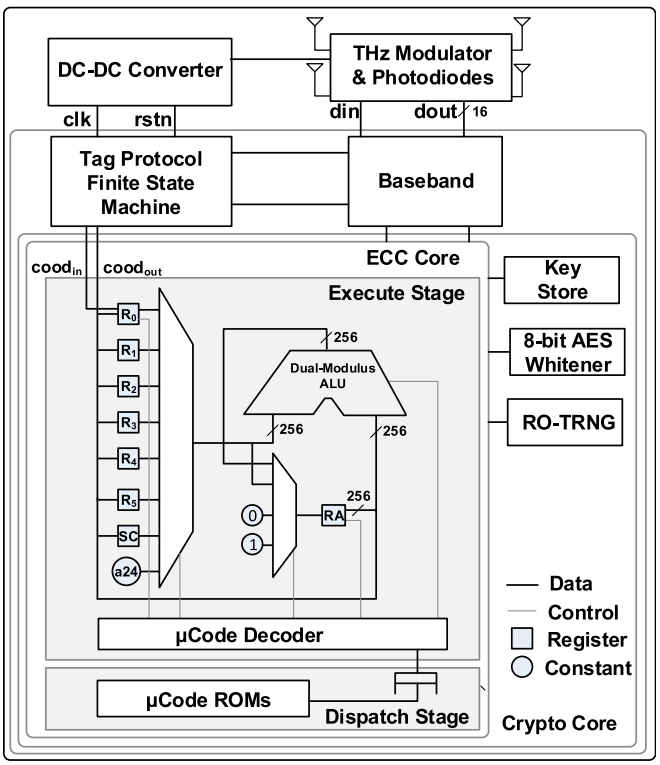



Fig. 13. Block diagram of the processor on the THz ID.

scheme [10], [16]. The scheme is a three-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. First, we narrowed the choice of authentication protocols, to those that did not require any hash functions to reduce die area. Second, a protocol using $x$-coordinate only arithmetic was chosen to enable a compact architecture for the ECC hardware accelerator (ECHA). Finally, Curve25519 was chosen since it allowed for an especially efficient $x$-coordinate only Montgomery ladder [17]. Since the authentication protocol requires a secret-scalar multiplication, using the Montgomery ladder has the added benefit of providing side-channel resistance [18].

The chip has a ring-oscillator-based true-random-number generator (RO-TRNG) with a 3.3 kGE[3] 8-bit advanced encryption standard (AES) whitener and a compact 25-kGE 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 2.8-kGE 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 earlier,

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

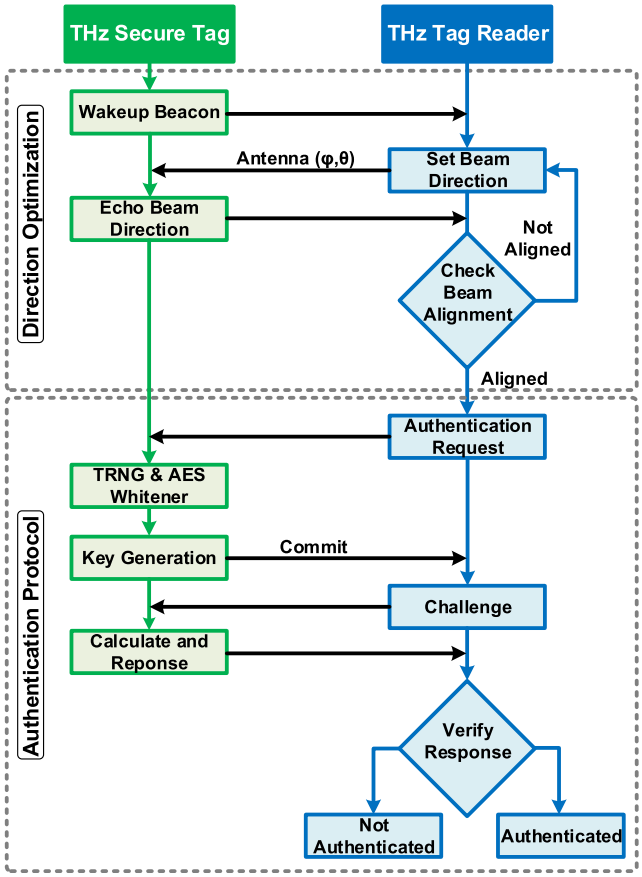



Fig. 14. Security protocol between the THz secure tag and the tag reader.

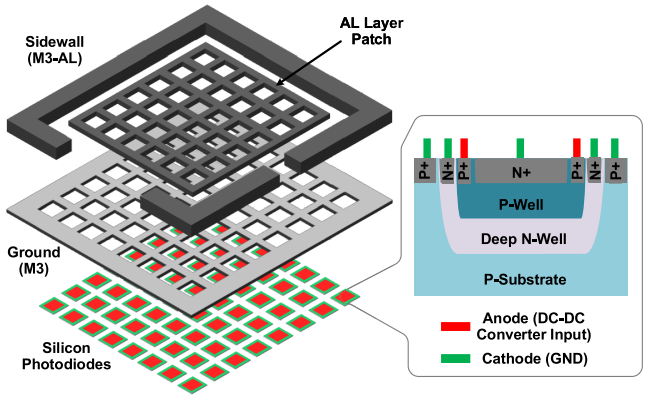



Fig. 15. Photodiodes placed below patch antenna with fishnet pattern.

elliptic-curve scalar multiplication (ECSM) is implemented using a constant time 650 k-cycle projective coordinate Montgomery ladder that is secure against simple power analysis. Register savings in the ECHA design and optimized ECSM microcode result in a 22% lower area and 18% lower cycle count compared to [19]. Storing the entire ECSM state in registers allows for low-voltage operation down to 0.85 V and improves the energy efficiency of the core to 14.4 $\mu$J/ECSM.

Fig. 14 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 ($\phi$) and elevation angle ($\theta$), 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 $\phi = 0°$ and $\theta = 90°$ by default and then starts scanning. It takes ~20 ms (limited by the uplink data rate of 2 kb/s) to complete the exchange of one beam direction message between the reader and the tag. The total time for the beam search is, therefore, ~500 ms.

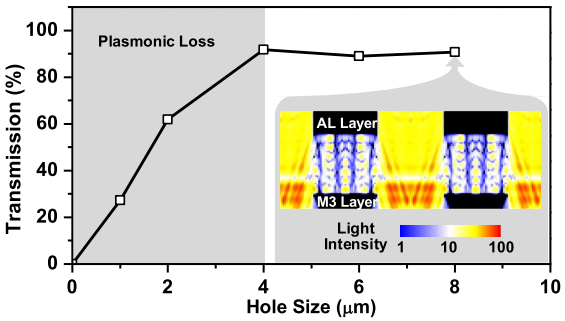
All THz tags are initialized with a unique private and public key pair ($t$, $T = tP$), and the reader has the tag's public key ($T$) registered in its database. The reader also has a private and public key pair ($y$, $Y = yP$), and the reader's public key $Y$ is known to all tags. If the reader requests authentication of the THz tag, the tag commits a fresh random value ($R_1 = r_1 P$) where the randomness ($r_1$) is generated using the RO-TRNG and the 8-bit AES whitener. The reader responds to tag's commit message with a random challenge ($R_2 = r_2 P$) that is utilized by the tag to compute a Diffie–Hellman share ($r_1 r_2 P$). 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.

## V. Integrated Photo-Voltaic Powering

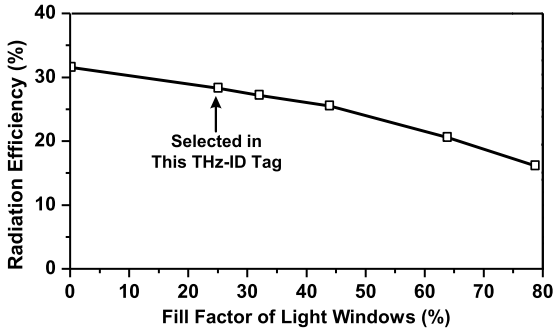
The antenna array, when incorporated on the tag chip, occupies most of the die area. In this section, we describe how the silicon under the antennas, along with an integrated DC–DC converter, is exploited to perform photo-voltaic powering for the tag.

### A. Photodiodes

The CMOS technology used for the chip provides a deep n-well structure, normally for increased isolation between the 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. 15. As a result, three p-n junctions are formed, which maximizes 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 (see Fig. 15). A simulation tool based on a finite-difference time-domain (FDTD) method, Lumerical [20], is used to examine the hole size of the fishnet pattern. The simulation results in Fig. 16(a) assume that 25% of the antenna area is holes to allow light transmission (refereed as fill factor of holes henceforth) and show that the through-hole light transmission for hole size smaller than 4 $\mu$m 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, a hole size of 8 $\mu$m, which leads to a through-hole light transmission rate of 92% that is selected. For a larger effective illumination area, the fill factor of the holes should increase. This, however, decreases the equivalent conductivity of the antenna metal layers and lowers the radiation efficiency, as is shown in the HFSS simulation in Fig. 16(b). In the tag chip, a fill factor of 25%




(a)




(b)

Fig. 16. (a) FDTD-simulated light ($\lambda$ = 700 nm) transmission through different hole size. The cross-sectional view of intensity distribution for the hole size of 8 $\mu$m is also shown. (b) Simulated antenna radiation efficiency with different hole opening fill factors while keeping 8-$\mu$m hole size.

is used, which slightly degrades the antenna efficiency from 31% to 27%.

### B. 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 (startup and main converters) that are connected between $V_{\rm IN}$ and $V_{{\rm OUT},I}$ in parallel, switching clock generators, and other small blocks for control (see Fig. 17). When the converter is powered by the photodiode from the cold state, the startup converter [see Fig. 18(a)] is first turned on and generates 3× up-converted voltage at $V_{{\rm OUT},I}$. When $V_{{\rm OUT},I}$ exceeds 0.8 V, it triggers the main converter to generate the 1-V output. If the main converter raises $V_{{\rm OUT},I}$ over 1 V, the output controller is triggered and turns on the output switch that connects $V_{{\rm OUT},I}$ and $V_{\rm OUT}$, starting power supply to load circuits. The output controller also provides a reset signal (RST in Fig. 17) to load circuits so as to initialize them properly during startup. RST is being asserted during the whole startup process and is de-asserted after the output switch is on and $V_{\rm OUT}$ is stabilized at 1 V.

For cold start, the startup 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. 17). 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 (see Fig. 18) is optimized for the power conversion of the peak system power, which can be estimated

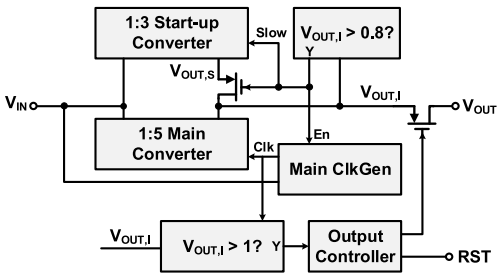
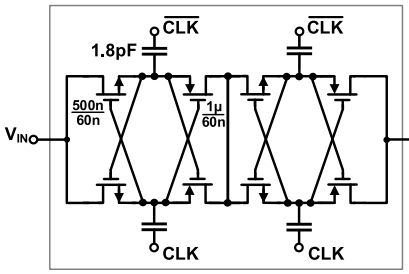
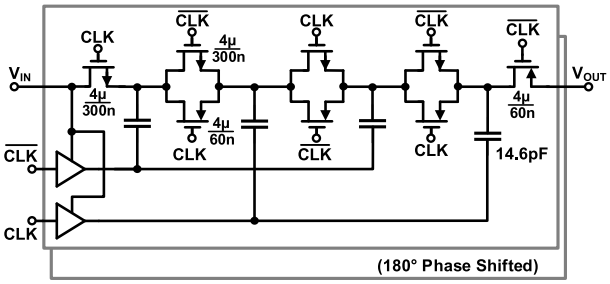



Fig. 17. Block diagram of the on-chip DC–DC converter.




(a)




(b)

Fig. 18. Schematics of (a) DC–DC converter startup circuit and (b) main DC–DC converter.

during the design time by simulation. It has a higher conversion ratio of 1:5 to provide 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 and efficient power output, a feedback loop controls the switching frequency of the main converter, so that the photodiode output voltage $V_{\rm OUT}$ 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, $V_{\rm OUT}$ output switch is turned on to connect converter's $V_{\rm OUT}$ to the supply voltage of other blocks. For regulating the output voltage at 1 V, another control loop is attached at $V_{\rm OUT}$ 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.

## VI. Experimental Results

The tag chip is fabricated using a TSMC 65-nm bulk CMOS process. The micrograph of the chip is shown in Fig. 19. The chip has an area of 1.2 × 1.3 mm$^2$. The two rows of pads,

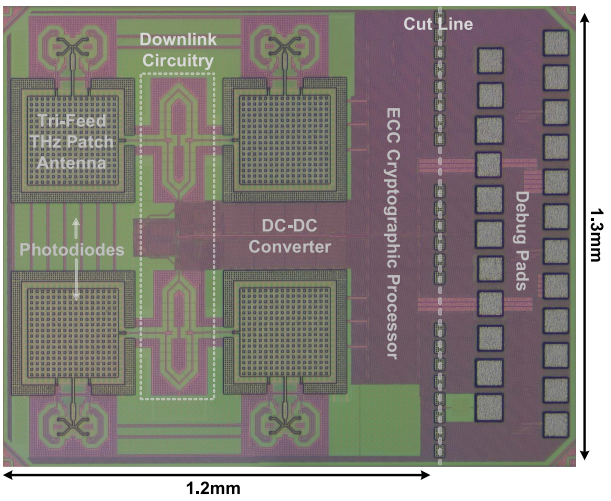



Fig. 19. Chip micrograph.

which can be cut, are for debugging purposes. In our testing, the chip is mounted and wire-bonded on a PCB.

### A. Measurement Setup

First, a custom-designed THz-ID reader is constructed, as shown in Fig. 20(a). It communicates with the chip at a distance of 5 cm using two WR-3.4 horn antennas. The antennas are placed in the way that their *E*-planes are orthogonal to each other, in order to match the cross-polarizations of the THz-ID antennas (see Fig. 3). 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-kb/s data generated from an FPGA board (XEM 7001). According to the Friis formula [21], 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 the tag-backscattered signal with the 48th harmonic of its 5.4632-GHz LO and downconverts 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 downconverted to 1 MHz, amplified by 60 dB and bandpass filtered. Finally, an envelope detector cascaded by a comparator recovers the 2-kb/s data and feeds to the FPGA [see Fig. 20(a)]. Fig. 20(b) 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 converge the light to $\sim$1 cm$^2$ spot on the PCB. The chip PCB is mounted on a rotational stage, which is used for the beamsteering measurement. In the uplink and downlink modes, the tag consumes 13 $\mu$W of power, which includes 4 $\mu$W 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 $\mu$W.

### B. Characterization of the Circuits

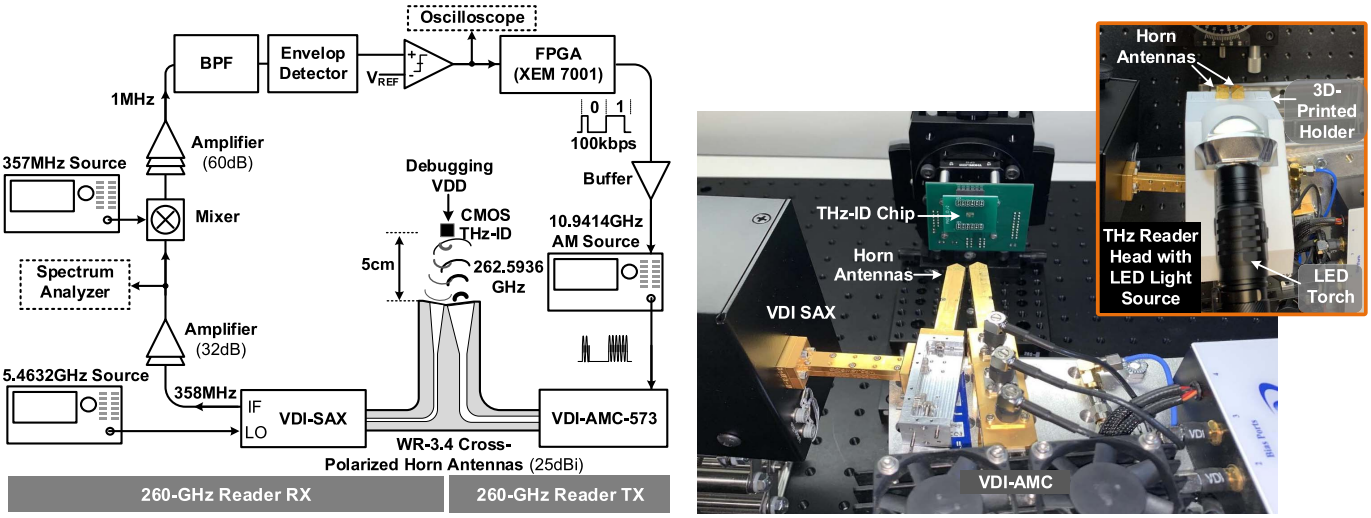
First, to characterize the 260-GHz backscatter module in a basic continuous-wave mode, the chip is externally powered and clocked (at $f_{\mathrm{LO}} = 2$ MHz) via the debugging pads. With the incident wave generated by the VDI AMC, a downconverted spectrum shown in Fig. 21 is obtained from the VDI SAX. The tone at 358 MHz is the expected signal backscattered by the THz-ID. It has an SNR of 36 dB at 1-kHz bandwidth, indicating the feasibility of an uplink with the designed 2-kb/s data rate. The tone at 362 MHz is the upper sideband image due to the limited image rejection ($\sim$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 $\sim$25 dB due to the cross polarization of the reader antennas, it is still $>$30 dB higher than the tag-backscattered signal in Fig. 21. This, in turn, justifies our backscatter 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 and hence does 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.

Then, with OOK modulation to the VDI AMC, the tag downlink output is measured via a debugging pad. Pulsewidth 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 a 40% duty cycle for bit 0 and 75% for bit 1. The results in Fig. 22 indicate that the tag downlink correctly recovers the original data created by the FPGA in the THz reader [see Fig. 20(a)]. To achieve the gate bias of the downlink MOSFET detector, ambient lighting is found to be sufficient in the testing.

Next, we test the beamsteering capability of the THz-ID chip. Note that it is different from conventional beamsteering of phased arrays, due to the unique backscattering operation of the chip, and the co-location of the reader's Tx and Rx. As shown in Fig. 23(a), the goal of the beamsteering of this tag is to ensure that when the chip does not face the reader perpendicularly, its backscattered wave can still be re-directed toward the reader. Fig. 23(a) shows that, with a chip tilting angle of $\theta$ 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:

$$\varphi_A - \varphi_B = 2 \cdot \left(\frac{\lambda}{2}\sin\theta\right) \cdot \frac{360^\circ}{\lambda} = (\sin\theta) \cdot 360^\circ. \qquad (4)$$

This is verified in our experiment, where the LO phase of each THz SSB mixer is digitally controlled by the on-chip processor. Fig. 23 shows the backscatter-wave power, which is received by the reader in the measurement, at varying chip tilting angle $\theta$. Two tag phase-gradient settings requested by the reader, $\varphi_A = \varphi_B$ and $\varphi_A - \varphi_B = 180^\circ$, are tested. The measured peak responses of the reader occur at $\theta = 0^\circ$ and $\theta = 30^\circ$, respectively, which well agree with (4). This also shows that the maximum beamsteering angle (in both azimuth and elevation directions) is $\pm 30^\circ$. It should be noted here that when an antenna is tilted, the effective aperture decreases by a factor of $\cos\theta$. At $\theta = 30^\circ$, $\sim$1.2-dB two-way power loss should occur. However, in the measurements,




(a) (b)

Fig. 20. (a) Diagram of the testing setup. Note that when light powering is used, the debugging VDD is disconnected. (b) Photographs of the testing setup with and without an 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.

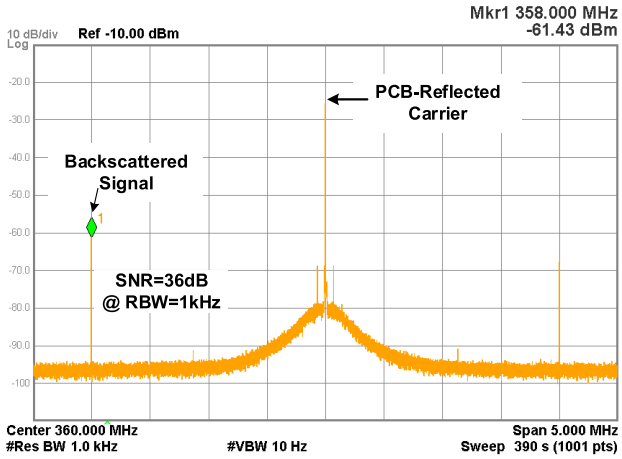



Fig. 21. Measured spectrum of the backscattered signal.

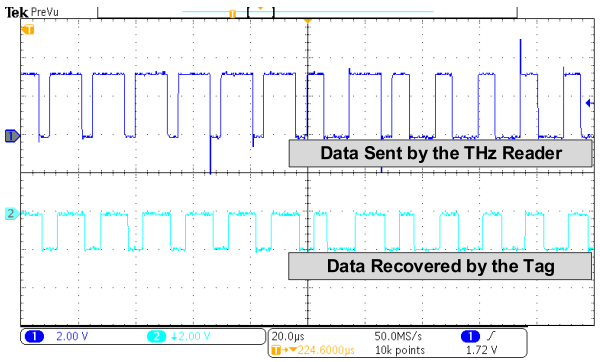
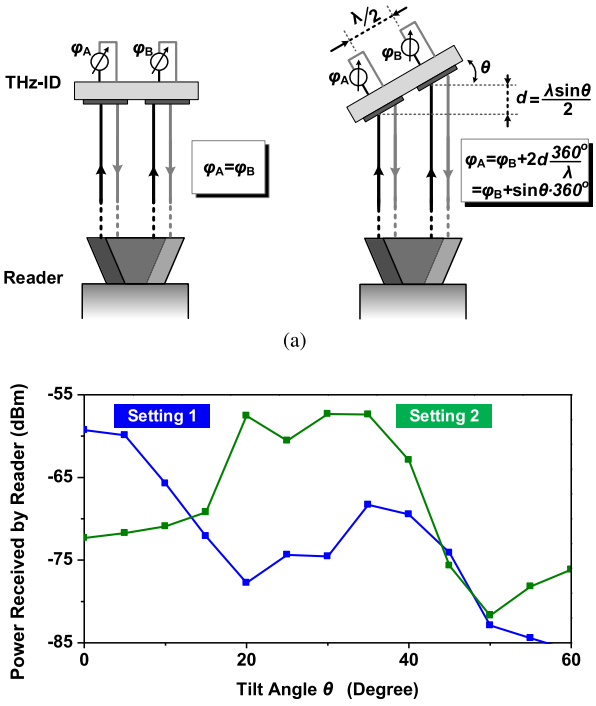



Fig. 22. Measured downlink waveform from the tag.

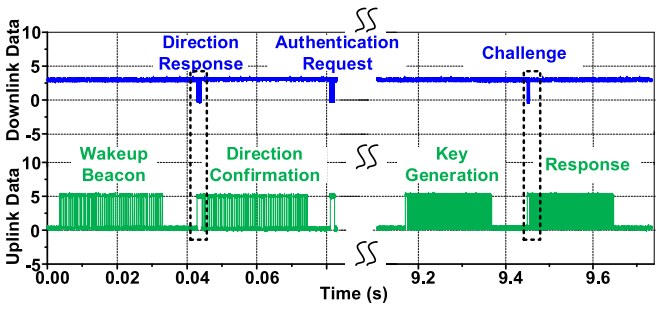



(a) (b)

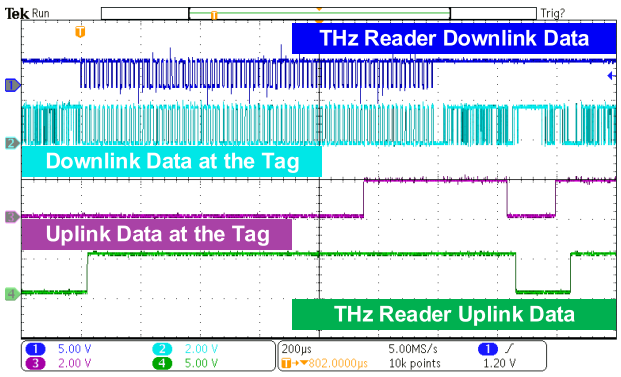
Fig. 23. (a) Phase-shifting ($\varphi_A - \varphi_B$) conditions in the tag to ensure that the backscattered wave points to the reader when the tag is tilted by $\theta$. (b) Measured backscattered-wave power, which is received by the reader, at different chip tilting angles $\theta$. Here, two digital settings of $\varphi_A - \varphi_B$ are applied.

we received almost the same peak power in both settings. This can be attributed to either a better alignment in setting 2 or measurement error.

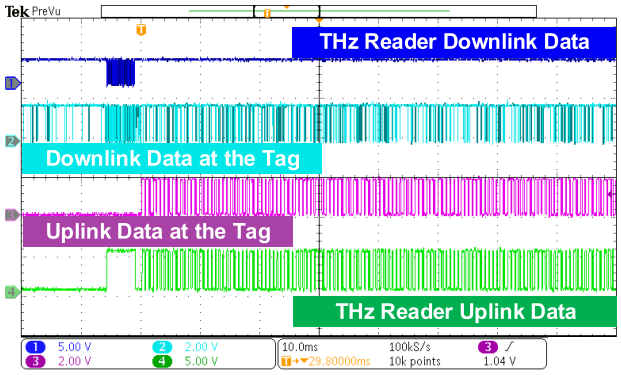
We also verified the protocol and the cryptographic function with an external power and the tag internal clock [see Fig. 24(a)]. When the reader receives the tag's beacon message, the FPGA starts a feedback loop to request a change of uplink beam angle until the SNR is maximized. The measured waveforms associated with this operation are shown in Fig. 24(b). Then, the reader sends a trigger to the chip to start the authentication process described in Section IV. Fig. 24(c) shows the measured waveforms of the challenge-response protocol that the tag takes toward the end of the authentication process, in order to identify itself to the valid reader. In Fig. 24(b), when THz reader is transmitting data, tag's




(a)

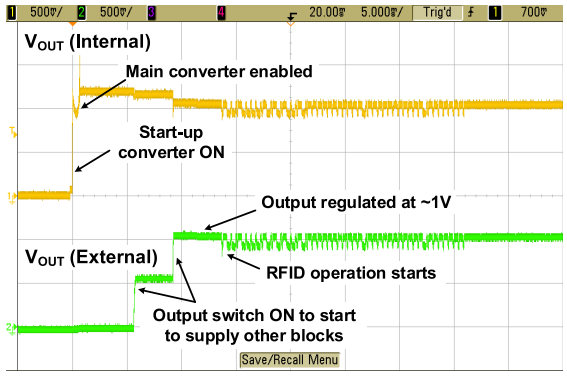



(b)

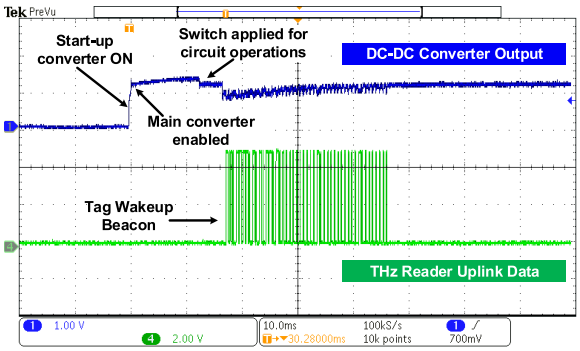



(c)

Fig. 24. (a) Measured downlink and uplink data in the protocol. Zoomed-in views of dotted regions representing the phases of (b) direction response and confirmation and (c) challenge and response message.




(a)




(b)

Fig. 25. (a) Measured startup behavior of the DC–DC converter. (b) Measured startup behavior of THz-ID with optical powering.

downlink circuit recovers the exact same data, and during idle time, random output pulses are observed, as explained in Section III-C. Due to the preamble validation in the processor, those random pulses are rejected.

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. 25(a). The first waveform presents the operations of the DC–DC converter, where the first peak shows the operation of the startup 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 $V_{\mathrm{OUT}}$ (external) with other circuit blocks of the tag, which is shown by the second waveform. The high-frequency fluctuations on $V_{\mathrm{OUT}}$ lines after the output voltage reaches $\sim$1 V indicate that the on-chip processor is activated. In Fig. 25(b), 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 backscatter 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 the 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 M1-to-Al stack.

## VII. Conclusion

In this article, we demonstrate 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 backscattering communication scheme is adopted. Meanwhile, our work demonstrates the feasibility of integrating asymmetric cryptography, such as elliptic-curve encryption, on a passive tag. A comparison of our work with the prior state of the arts is given in Table I. Our presented tag is built entirely on a low-cost CMOS chip and is around 3$\times$ smaller than the smallest package-less, far-field chip reported previously [6]. It also offers multi-antenna beamsteering functionality for

TABLE I
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 | 21$\mu$W | Yes (Elliptic Curve) | 5cm | Yes | 1.6 |
| [4]† ISSCC'17 | 180 nm | 0.915 | PPM | DL: 62.5kbps UL: 30.3kbps | 2mW | No | 20m | No | 9† |
| [5] ISSCC'18 | 65 nm | 5.8 | DL: <4% ASK UL: HIMIL | DL: 5Mbps UL: 4kbps | 10$\mu W$ | No | 1mm | No | 0.01 |
| [6] 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 |
| [7]§ ISSCC'16 | 130nm | 0.433 | DL:PPM UL:PWM | 125kbps | 16$\mu W$ | Yes (Symmetric) | 5mm | No | 64§ |

†Assembly of multiple functional layers (photo-voltaic powering, battery, antenna, etc.) is used. ‡The calculated value in [4] is cited.
§PCB-level components including off-chip coupler are required.

TABLE II
COMPARISON OF ELLIPTIC-CURVE HARDWARE ACCELERATORS

| Reference | CMOS Process | Technology Normalized Area | Cycle Count | ECSM Energy |
|---|---|---|---|---|
| [22] CRASH'05 | 350 nm | 31kGE | 1.1M | 550$\mu$J |
| [19] CHES'15 | 130 nm | 33kGE | 811.2k | 56$\mu$J |
| [23] ISSCC'18 | 65 nm | 65.5kGE+ 4kB SRAM | 496k | 17.6$\mu$J |
| This Work | 65 nm | 25kGE | 650k | 14.4$\mu$J |

the first time in RFIDs. Compared to [7], the asymmetric public-key cryptography provides higher level security and makes the THz-ID tag suitable for privacy-sensitive applications. Table II compares the proposed ECHA 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.

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. For example, to allow for embedding of the tag inside opaque materials, energy harvesting directly from the THz wave is desired. This requires high-speed rectifier devices in the CMOS process. To this end, the poly-gate-separate Schottky diodes in CMOS, which have ~2-THz cutoff frequency and are used in THz imaging [24], could possibly meet the above needs. Second, although 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 [25], the 200-to-255-GHz power amplifier using a 130-nm SiGe BiCMOS process ($f_{\max} \approx 500$ 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 light of recent developments of high-speed and high-power SiGe and CMOS processes [26]–[29] with up to 720-GHz $f_{\max}$ and up to 7.1-V breakdown voltage, achieving radiation power of 100 mW in the sub-THz regime is no longer unimaginable.

## APPENDIX
## NOISE VOLTAGE OF AN OPEN-CIRCUIT PHOTODIODE UNDER ILLUMINATION

In the downlink THz MOSFET detector (see Fig. 10), 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 [30]. 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

$$I_d = -I_p = I_0\left(e^{\frac{V_0}{V_t}} - 1\right) \tag{5}$$

where $I_0$ is the reverse saturation current of the p-n junction, $V_t$ is the thermal voltage ($V_t = kT/q \approx 26$ 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 [30], [31]

$$\tilde{i_n^2}/\Delta f = 4q\left(|I_p| + I_0\right) \approx 4q|I_p|. \tag{6}$$

The open-circuit noise voltage of the photodiode is then considered to be the product of (6) and the diode differential resistance at the bias ($R_d = V_t/|I_p|$)

$$\tilde{v_n^2} = \tilde{i_n^2} \cdot R_d^2 = 4q|I_p| \cdot \left(\frac{V_t}{|I_p|}\right)^2 \Delta f = 4q\frac{V_t^2}{|I_p|}\Delta f = 4\mathrm{kTR}_d\Delta f. \tag{7}$$

Interestingly, the generated noise is the same as 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. 10 is

$$\tilde{v}_{n,\mathrm{det}}^2 = g_m^2 \cdot \tilde{v_n^2} \cdot r_{\mathrm{ds}}^2 = g_m^2 r_{\mathrm{ds}}^2 \cdot 4\mathrm{kTR}_d\Delta f \tag{8}$$

where $g_m$ and $r_{\mathrm{ds}}$ are the transconductance and output resistance of the MOSFET, respectively. Note that (8) is much smaller than the MOSFET's own channel thermal noise ($\tilde{v}_{n,\mathrm{ch}}^2 = 4\mathrm{kTr}_{\mathrm{ds}}\Delta f$): for the MOSFET biased in the triode mode (see Fig. 10), the simulated $g_m$ and $r_{\mathrm{ds}}$ are 1.4 $\mu$S and 7.7 k$\Omega$, respectively, and $I_p$ in normal tag operation is ~0.1 $\mu$A (hence $R_d \approx 260$ k$\Omega$). Therefore, $\tilde{v}_{n,\mathrm{ch}}$ is ~11 nV/Hz$^{1/2}$, while $\tilde{v}_{n,\mathrm{det}}$ in (8) is ~0.7 nV/Hz$^{1/2}$.

## ACKNOWLEDGMENT

The authors acknowledge Virginia Diodes Inc. (VDI) for their generous support of some of the testing instruments. Authors also thank Prof. Donhee Ham and Dr. Houk Jang at Harvard University, and Prof. Tomas Palacios, Prof. Nicholas Fang, and Xinhao Li at MIT for providing assistance during our experiments.

## REFERENCES

[1] R. Want, "An introduction to RFID technology," *IEEE Pervasive Comput.*, vol. 5, no. 1, pp. 25–33, Jan./Mar. 2006.
[2] G. Swamy and S. Sarma, "Manufacturing cost simulations for low cost RFID systems," MIT Auto-ID Center, Cambridge, MA, USA, White Paper, 2003.
[3] H. Pristauz, "RFID chip assembly for 0.1 cents?" *OnBoard Technol.*, pp. 46–49, Sep. 2006.
[4] L.-X. Chuo *et al.*, "A 915MHz asymmetric radio using Q-enhanced amplifier for a fully integrated 3×3×3 mm$^3$ wireless sensor node with 20m non-line-of-sight communication," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2017, pp. 132–134.
[5] B. Zhao, N. C. Kuo, B. Liu, Y. A. Li, L. Lotti, and A. M. Niknejad, "A 5.8GHz power-harvesting 116$\mu$mx116$\mu$m 'dielet' near-field radio with on-chip coil antenna," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2018, pp. 456–458.
[6] M. Tabesh, M. Rangwala, A. M. Niknejad, and A. Arbabian, "A power-harvesting pad-less mm-sized 24/60GHz passive radio with on-chip antennas," in *Symp. VLSI Circuits Dig. Tech. Papers*, Jun. 2014, pp. 1–2.
[7] C. Juvekar, H.-M. Lee, J. Kwong, and A. P. Chandrakasan, "A Keccak-based wireless authentication tag with per-query key update and power-glitch attack countermeasures," in *IEEE ISSCC Dig. Tech. Papers*, Jan./Feb. 2016, pp. 290–292.
[8] T. Chi, H. Wang, M.-Y. Huang, F. F. Dai, and H. Wang, "A bidirectional lens-free digital-bits-in/-out 0.57 mm$^2$ Terahertz nano-radio in CMOS with 49.3mW peak power consumption supporting 50cm Internet-of-Things communication," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, Apr./May 2017, pp. 1–4.
[9] M. I. Ibrahim *et al.*, "THzID: A 1.6 mm2 package-less cryptographic identification tag with backscattering and beam-steering at 260GHz," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2020, pp. 24–26.
[10] J. Hermans, R. Peeters, and C. Onete, "Efficient, secure, private distance bounding without key updates," in *Proc. 6th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WiSec)*, 2013, pp. 207–218.
[11] C. Balanis, *Antenna Theory*, 3rd ed. Hoboken, NJ, USA: Wiley, 2005.
[12] Ansys HFSS. *High Frequency Structure Simulator (HFSS) User Guide, Version 19.4*. Accessed: Sep. 2019. [Online]. Available: http://www.ansys.com/
[13] C. Wang and R. Han, "Dual-Terahertz-Comb spectrometer on CMOS for rapid, wide-range gas detection with absolute specificity," *IEEE J. Solid-State Circuits*, vol. 52, no. 12, pp. 3361–3372, Dec. 2017.
[14] E. Ojefors, U. R. Pfeiffer, A. Lisauskas, and H. G. Roskos, "A 0.65 THz focal-plane array in a quarter-micron CMOS process technology," *IEEE J. Solid-State Circuits*, vol. 44, no. 7, pp. 1968–1976, Jul. 2009.
[15] M. I. W. Khan, S. Kim, D.-W. Park, H.-J. Kim, S.-K. Han, and S.-G. Lee, "Nonlinear analysis of nonresonant THz response of MOSFET and implementation of a high-responsivity cross-coupled THz detector," *IEEE Trans. Terahertz Sci. Technol.*, vol. 8, no. 1, pp. 108–120, Jan. 2018.
[16] R. Peeters and J. Hermans, "Wide strong private RFID identification based on zero-knowledge," in *Proc. Crypto*, Lyon, France, vol. 2012. Santa Barbara, CA, USA: Univ. California, Santa Barbara, 2012, p. 389.
[17] P. L. Montgomery, "Speeding the Pollard and elliptic curve methods of factorization," *Math. Comput.*, vol. 48, no. 177, pp. 243–264, Jan. 1987.
[18] M. Joye and S.-M. Yen, "The Montgomery powering ladder," presented at the Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES), San Francisco, CA, USA. Berlin, Germany: Springer, Aug. 2002, pp. 291–302.
[19] M. Hutter, J. Schilling, P. Schwabe, and W. Wieser, "NaCl's Crypto_box in Hardware," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)*, Saint-Malo, France, 2015, pp. 81–101.
[20] Lumerical. *FDTD Product Reference Manual*. Accessed: Sep. 2019. [Online]. Available: htpps//:www.lumerical.com
[21] H. T. Friis, "A note on a simple transmission formula," *Proc. IRE*, vol. 34, no. 5, pp. 254–256, May 1946.
[22] J. Wolkerstorfer, "Scaling ECC hardware to a minimum," in *Proc. Cryptograph. Adv. Secure Hardw. (CRASH)*, Leuven, Belgium, 2005, pp. 207–214.
[23] U. Banerjee, C. Juvekar, A. Wright, Arvind, and A. P. Chandrakasan, "An energy-efficient reconfigurable DTLS cryptographic engine for End-to-End security in IoT applications," in *IEEE ISSCC Dig. Tech. Papers*, San Francisco, CA, USA, Feb. 2018, pp. 42–44.
[24] R. Han *et al.*, "Active terahertz imaging using Schottky diodes in CMOS: Array and 860-GHz pixel," *IEEE J. Solid-State Circuits*, vol. 48, no. 10, pp. 2296–2308, Oct. 2013.
[25] M. H. Eissa and D. Kissinger, "A 13.5dBm Fully Integrated 200-to-255GHz Power Amplifier with a 4-Way Power Combiner in SiGe:C BiCMOS," in *IEEE ISSCC Dig. Tech. Papers*. San Francisco, CA, USA, Feb. 2019, pp. 82–84.
[26] B. Heinemann *et al.*, "SiGe HBT with fx/fmax of 505 GHz/720 GHz," in *IEDM Tech. Dig.*, San Francisco, CA, USA, Dec. 2016, pp. 51–54.
[27] S. N. Ong *et al.*, "A 22nm FDSOI technology optimized for RF/mmWave applications," in *Proc. IEEE Radio Freq. Integr. Circuits Symp. (RFIC)*, Jun. 2018, pp. 72–75.
[28] H. Lee *et al.*, "Intel 22 nm FinFET (22FFL) process technology for RF and mm wave applications and circuit design optimization for FinFET technology," in *IEDM Tech. Dig.*, San Francisco, CA, USA, Dec. 2018, pp. 316–319.
[29] H.-J. Lee *et al.*, "Implementation of high power RF devices with hybrid workfunction and OxideThickness in 22nm low-power FinFET technology," in *IEDM Tech. Dig.*, San Francisco, CA, USA, Dec. 2019, pp. 610–613.
[30] A. van der Ziel, "Noise in solid-state devices and lasers," *Proc. IEEE*, vol. 58, no. 8, pp. 1178–1206, Aug. 1970.
[31] U. F. Gianola, "Photovoltaic noise in silicon broad area $p-n$ junctions," *J. Appl. Phys.*, vol. 27, no. 1, pp. 51–54, 1956.

**Muhammad Ibrahim Wasiq Khan** (Graduate Student Member, IEEE) received the B.E. degree (Hons.) in electrical engineering from the National University of Science and Technology (NUST), Islamabad, Pakistan, in 2012, and the M.Sc. degree in electrical engineering from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea, in 2016, where he worked on THz detectors and THz imaging systems based on CMOS technology. He is currently pursuing the Ph.D. degree with the Electrical Engineering and Computer Science (EECS) Department, Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, where he is working on CMOS-based THz identification tags and THz energy-harvesting systems.

His research interests include mm-wave and THz-integrated wireless systems.

Mr. Khan received the Rector's Bronze Medal for his B.E. degree.

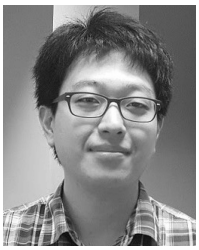
**Mohamed I. Ibrahim** (Student Member, IEEE) received the B.Sc. (Hons.) and M.Sc. degrees in electrical engineering from Ain Shams University, Cairo, Egypt, in 2012 and 2016, respectively. He is currently pursuing the Ph.D. degree with the Electrical Engineering and Computer Science (EECS) Department, Massachusetts Institute of Technology (MIT), Cambridge, MA, USA,

From 2012 to 2016, he was a Teaching and Research Assistant with Ain Shams University. During this period, he was developing metamaterial-inspired antennas and microwave passive structures. He is working on CMOS-integrated quantum-enhanced sensing and information processing systems and terahertz wireless systems. His research interests include RF-integrated circuit design, microwave passive planar structures, and novel electromagnetic materials and devices.

**Chiraag S. Juvekar** (Member, IEEE) received the B.Tech. and M.Tech. degrees in electrical engineering from IIT Bombay, Mumbai, India, in 2012, and the Ph.D. and S.M. degrees in electrical engineering and computer science from the Massachusetts Institute of Technology, Cambridge, MA, USA, in 2014 and 2018, respectively.

In 2014, he worked in the Embedded Processing Lab, Texas Instruments, Dallas, TX, USA, designing authentication circuits using emerging memories. He is currently a Hardware Security Architect and Researcher with the Security Center of Excellence, Analog Devices Inc., Boston, MA, USA. His research focuses on low-power system design, hardware security, and neural network acceleration.

Dr. Juvekar was a recipient of the MIT Presidential Fellowship in 2012 and the Qualcomm Innovation Fellowship in 2016. He was also a recipient of the Chorafas Foundation Award for 2018 and the 2018 Jin-Au Kong Award for the Best Ph.D. Theses in electrical engineering at MIT.



**Wanyeong Jung** (Member, IEEE) received the B.S. degree from Seoul National University, Seoul, South Korea, in 2012, and the M.S. and Ph.D. degrees in electrical engineering from the University of Michigan, Ann Arbor, MI, USA, in 2014 and 2017, respectively.

He was a Research Intern with NVIDIA Research, Austin, TX, USA, in 2016. From 2017 to 2019, he was a Post-Doctoral Associate with Microsystems Technology Laboratories, Massachusetts Institute of Technology, Cambridge, MA, USA. Since 2019, he has been an Assistant Professor with the School of Electrical Engineering, Korea Advanced Institute of Science and Technology, Daejeon, South Korea. His research interests include low-power circuits and systems, energy-efficient edge computing, and Internet of Things (IoT).

**Rabia Tugce Yazicigil** (Member, IEEE) received the B.S. degree in electronics engineering from Sabanci University, Istanbul, Turkey, in 2009, the M.S. degree in electrical and electronics engineering from the École Polytechnique Fédérale de Lausanne (EPFL), Lausanne, Switzerland, in 2011, and the Ph.D. degree in electrical engineering from Columbia University, NYC, NY, USA, in 2016.

She was a Post-Doctoral Research Associate with the EECS Department, MIT, Cambridge, MA, USA, from 2016 to 2018. She is currently an Assistant Professor with the Electrical and Computer Engineering Department, Boston University, Boston, MA, USA, and a Visiting Scholar with MIT. Her research interests lie at the interface of integrated circuits, signal processing, security, bio-sensing, and wireless communications to innovate system-level solutions for future energy-constrained applications.

Dr. Yazicigil was a recipient of a number of awards, including the "Electrical Engineering Collaborative Research Award" for her Ph.D. research on compressive sampling applications in rapid RF spectrum sensing in 2016, the Second Place at the Bell Labs Future X Days Student Research Competition in 2015, the Analog Devices Inc. Outstanding Student Designer Award in 2015, and the 2014 Millman Teaching Assistant Award of Columbia University. She served as the Vice Chair of the Rising Stars 2020 Workshop at the IEEE International Solid-State Circuits Conference (ISSCC) and she is a member of the 2015 MIT EECS Rising Stars Cohort. She also serves on the Technical Program Committee (TPC) of the IEEE ISSCC and TPC of the IEEE European Solid-State Circuits Conference (ESSCIRC).

**Anantha P. Chandrakasan** (Fellow, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical engineering and computer science from the University of California at Berkeley (UC Berkeley), Berkeley, CA, USA, in 1989, 1990, and 1994, respectively.

Since September 1994, he has been with the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, where he is currently the Vannevar Bush Professor of electrical engineering and computer science. He was the Director of the MIT Microsystems Technology Laboratories from 2006 to 2011. From July 2011 to June 2017, he was the Head of the MIT Department of Electrical Engineering and Computer Science. Since July 2017, he has been the Dean of the MIT School of Engineering. He has coauthored *Low Power Digital CMOS Design* (Kluwer Academic Publishers, 1995), *Digital Integrated Circuits* (Pearson Prentice-Hall, 2003, Second Edition), and *Sub-threshold Design for Ultra-Low Power Systems* (Springer, 2006). His research interests include ultra-low-power circuit and system design, energy harvesting, energy-efficient RF circuits, and hardware security.

Dr. Chandrakasan was a co-recipient of several awards, including the 2007 ISSCC Beatrice Winner Award for Editorial Excellence and the ISSCC Jack Kilby Award for Outstanding Student Paper (2007–2009). He received the 2009 Semiconductor Industry Association (SIA) University Researcher Award, the 2013 IEEE Donald O. Pederson Award in Solid-State Circuits, an Honorary Doctorate from KU Leuven in 2016, the UC Berkeley EE Distinguished Alumni Award in 2017, and the 2019 IEEE Solid-State Circuits Society Distinguished Service Award. In 2015, he was elected to the National Academy of Engineering, and in 2019, he was elected to the American Academy of Arts and Sciences. He has served in various roles for the IEEE ISSCC, including the Program Chair, the Signal Processing Sub-Committee Chair, and the Technology Directions Sub-Committee Chair. He served as the Conference Chair of ISSCC from 2010 to 2018. He serves as the Senior Technical Advisor for ISSCC 2019.

**Ruonan Han** (Senior Member, IEEE) received the B.Sc. degree in microelectronics from Fudan University, Shanghai, China, in 2007, the M.Sc. degree in electrical engineering from the University of Florida, Gainesville, FL, USA, in 2009, and the Ph.D. degree in electrical and computer engineering from Cornell University, Ithaca, NY, USA, in 2014.

He is currently an Associate Professor with the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA. His research interests include microelectronic circuits and systems operating at millimeter-wave and terahertz frequencies.

Dr. Han was a recipient of the Cornell ECE Director's Ph.D. Thesis Research Award, the Cornell ECE Innovation Award, two Best Student Paper Awards of the IEEE Radio Frequency Integrated Circuits Symposium in 2012 and 2017, the IEEE Microwave Theory and Techniques Society (MTT-S) Graduate Fellowship Award, and the IEEE Solid-State Circuits Society (SSC-S) Predoctoral Achievement Award. He is the winner of the National Science Foundation (NSF) CAREER Award in 2017 and the Intel Outstanding Researcher Award in 2019. He has been serving an Associate Editor for the IEEE TRANSACTIONS ON VERY-LARGE-SCALE INTEGRATION SYSTEM since 2019 and the IEEE TRANSACTIONS ON QUANTUM ENGINEERING since 2020, has served as a Guest Associate Editor for the IEEE TRANSACTIONS ON MICROWAVE THEORY AND TECHNIQUES in 2019, and also serves on the Technical Program Committee (TPC) of the IEEE RFIC Symposium and the 2019 Steering Committee and TPC of the IEEE International Microwave Symposium. He is the IEEE MTT-S Distinguished Lecturer (2020–2022).