29.8 THzID: A 1.6mm² Package-Less Cryptographic Identification Tag with Backscattering and Beam-Steering at 260GHz

Mohamed I. Ibrahim[1], Muhammad Ibrahim Wasiq Khan[1], Chiraag S. Juvekar[2], Wanyeong Jung[1], Rabia Tugce Yazicigil[3], Anantha P. Chandrakasan[1], Ruonan Han[1]

[1]Massachusetts Institute of Technology, Cambridge, MA
[2]Analog Devices, Boston, MA
[3]Boston University, Boston, MA

Energy-autonomous wireless tags have been adopted in authentication and supply-chain management. At present, their size and cost, limited by packaging, prevent the tagging for small or inexpensive industrial/medical components. At the same time, pervasive electronic tagging raises serious privacy concerns related to inadvertent and malicious tracking of the tagged assets. In order to enable secure and ubiquitous asset tagging, fully passive particle-sized cryptographic chips without external packaging are highly desired. Recent prototypes [1-4] that aim to address this challenge face either size, energy, communication, or security limitations. [1] demonstrates a 9mm² sensor node, which requires a stacked packaging of multiple functionality layers for photovoltaic powering, battery, antenna, etc. In [2], a 116×116µm² radio chip is demonstrated, but its operating range of 1mm is limited by the near-field coupling at 5.8GHz for power delivery and communication. Using far-field downlink/uplink at 24 and 60GHz, the package-less chip in [3] boosts the range to 50cm, but the chip size also increases to 4.4mm² to accommodate two antennas at 24 and 60GHz. Additionally, [1-3] do not support cryptographically secure identification. [4] demonstrates a 0.77mm² secure authentication tag that requires an 8mm² external antenna, but the size and the energy constraints limit it to symmetric-key cryptography. In this paper, we present a package-less, monolithic tag chip with built-in photovoltaic powering and a compact elliptic-curve-cryptography (ECC) processor. Using far-field backscatter communication at 260GHz, the CMOS tag, while integrating a 2×2 antenna array with beam-steering capability, has a size of only 1.6mm².

The chip architecture of the tag is shown in Fig. 29.8.1. A 260GHz wave from the tag reader is coupled to 2×2 tri-feed patch antennas. At each antenna, the input 260GHz power is split (~1:1) between a chain of a square-law detector and amplifier and a passive single-sideband (SSB) mixer (Fig. 29.8.2). The former is for downlink demodulation when the 260GHz wave is AM modulated at ~100kb/s. The latter enables ~2kb/s uplink, for which the 260GHz wave is down-shifted by $f_{LO} \approx$ 2MHz, AM modulated by the tag data and is then re-radiated through the same antenna with an orthogonal polarization. Prior compact THz transceivers [5] use the single polarization of the shared antenna for time-duplexed transmit/receive operations. Our approach supports simultaneous bi-directional wave transmission and effectively reduces the interference to the uplink caused by the direct 260GHz wave reflection from the tagged object. A chip-wide array of photodiodes and a DC-DC converter are integrated to power the tag. The ECC cryptographic processor is based on a narrow-strong private identification protocol [6].

The TM_{10} and TM_{01} modes of the patch antenna can be excited by either a single-ended feed along the side wall with a uniform electric field, or a differential feed along the one with a half-wavelength electric field. Shown in Fig. 29.8.2, this property is utilized for the aforementioned power splitting of the received signal polarized in *x*-axis. For the uplink, the antenna differential feed (Feed1) connects to the SSB-mixer input through a pair of 90° Lange couplers. The quadrature LO signal of the mixer comes from a ~2MHz oscillator, which is ON/OFF controlled by the uplink data stream. The mixer output is fed back to the antenna via a single-ended feed (Feed2) at the same antenna edge, which then excites radiation in *y*-axis. A balun allowing for only differential-mode transmission is inserted between Feed1 and the Lange couplers, in order to prevent the common-mode leakage of the mixer output signal to the couplers. Through phase shifting of the 2MHz LOs among the four antennas, beam-steering of the backscattered wave is also achieved, which improves the link budget for non-perpendicular reader positions. For the downlink, the single-ended feed (Feed3) of each antenna is connected to a MOSFET detector biased slightly above the threshold by a photodiode (Fig. 29.8.2). The demodulated signal is then fed to a subthreshold amplifier (P_{DC}=1.5µW) to control the security processor.

The photodiodes for chip powering are based on a N+/Pwell/Deep-Nwell structure (Fig. 29.8.3). For compactness, they are placed both beside and underneath the antennas. Correspondingly, the patch radiator and the ground of the antenna are implemented with a fishnet pattern (Fig. 29.8.3). With 8µm hole size and spacing, the antenna has an FDTD-simulated light transmission of 22% and a simulated radiation efficiency of 27%. The operating output voltage (~0.3V) of the photodiodes is converted to 1V by two switched-capacitor converters (Fig. 29.8.3). First, a start-up converter operates when the photodiode output power is available and generates 3× up-converted voltage at V_{OUT}. When V_{OUT} exceeds 0.8V, it triggers a main converter to generate the 1V output and is disconnected from V_{OUT} for minimum power waste. A feedback loop controlling the clock of the main converter is used to extract maximum power from the photodiodes with a simulated efficiency of 60%.

Figure 29.8.3 also shows the cryptographic processor, which implements a 128b secure ECC-based private ID scheme. The scheme [6] is a 3-move protocol, where the tag chip uses its private key and the reader public key in order to identify itself to the valid readers. The scheme guarantees that any eavesdropper who does not possess the reader private key cannot identify which tag participates in the protocol by merely monitoring the wireless link. The chip has a ring-oscillator-based true-random-number generator (RO-TRNG) with a 3.3kGE 8b advanced-encryption-standard (AES) whitener and a compact 25kGE Curve25519 ECC hardware accelerator (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. It supports a dual-modulus ALU that allows arithmetic over both the base field and the scalar field. Elliptic-curve scalar multiplication (ECSM) is implemented using a 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 [7]. 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.

The test setup in Fig. 29.8.4 is used to communicate with the chip with two horn antennas with orthogonal polarizations. A VDI amplifier-multiplier chain (AMC) generates the 260GHz signal, and a spectrum analyzer extender (SAX) detects the backscattered signal. With 5cm distance, the measured backscattered spectrum and the recovered downlink data by the chip are shown in Fig. 29.8.4. Figure 29.8.5 shows the detailed protocol of the chip and the measured time-domain waveform with an external power. First, a beacon message is sent by the tag and then the reader starts a feedback loop to request a change of uplink beam angle until the SNR is maximized. The measured beam patterns from the chip at two settings requested by the reader are shown in Fig. 29.8.5. Next, the reader sends a trigger to the chip to start the authentication process. The tag sets up keys by utilizing the RO-TRNG with the 8b AES whitener for the randomness and then commits them to the reader. Lastly, the tag participates in a challenge-response protocol to identify itself to valid readers.

The chip is fabricated using a TSMC 65nm bulk CMOS process. As is shown in Fig. 29.8.6, the chip consumes ~20µW power in its most power-hungry mode (security mode). In Fig. 29.8.6, the 260GHz backscattering is demonstrated with the chip fully powered by a CREE XP-L-V6 LED. A comparison with the prior work is also provided in Fig. 29.8.6. From Fig. 29.8.6, the chip is around 3× smaller than the smallest package-less far-field chip reported earlier [3], with additional beam-steering functionality. The usage of public-key cryptography further makes it suitable for privacy-sensitive applications.

Acknowledgement:
This work is supported by the National Science Foundation (SpecEES ECCS-1824360). The authors acknowledge Prof. Donhee Ham and Dr. Houk Jang at Harvard University, Prof. Nicholas Fang and Xinhao Li at MIT for their technical assistance during the testing, and Virginia Diodes Inc. (VDI) for providing testing instruments.

References:

[1] L. Chuo et al., "A 915MHz Asymmetric Radio Using Q-Enhanced Amplifier for a Fully Integrated 3×3×3mm³ Wireless Sensor Node with 20m Non-Line-of-Sight Communication," *ISSCC*, pp. 132-133, Feb. 2017.
[2] B. Zhao et al., "A 5.8GHz Power-Harvesting 116µm×116µm "Dielet" Near-Field Radio with On-Chip Coil Antenna," *ISSCC*, pp. 456-458, Feb. 2018.
[3] M. Tabesh et al., "A Power-Harvesting Pad-Less mm-Sized 24/60GHz Passive Radio with On-Chip Antennas," *IEEE Symp. VLSI Circuits,* pp. 1-2, 2014.
[4] C. Juvekar et al. "A Keccak-Based Wireless Authentication Tag with Per-Query Key Update and Power-Glitch Attack Countermeasures," *ISSCC*, pp. 290-292, Feb. 2016.
[5] T. Chi et al., "A Bidirectional Lens-Free Digital-Bits-in/-out 0.57mm² Terahertz Nano-Radio in CMOS with 49.3mW Peak Power Consumption Supporting 50cm Internet-of-Things Communication," *IEEE CICC,* pp. 1-4, May 2017.

 978-1-7281-3205-1/20/$31.00

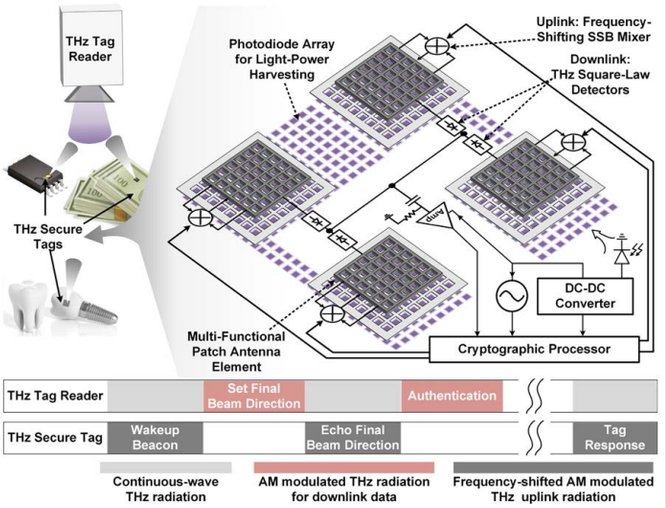


Figure 29.8.1: Schematic and basic operations of the cryptographic THzID chip system.

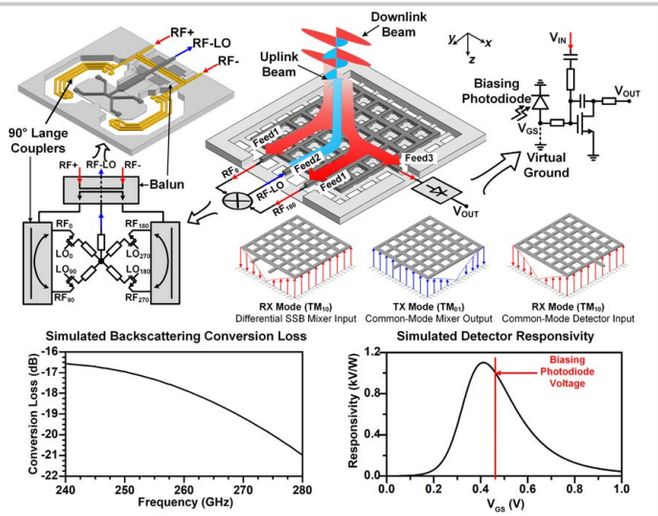


Figure 29.8.2: The design and simulated performance of the multifunctional antenna and the THz front-end circuits.

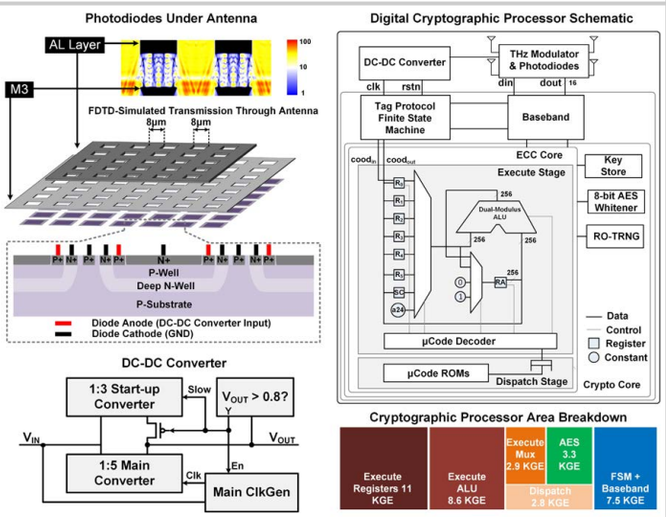


Figure 29.8.3: Chip-powering circuits (the antenna-integrated photodiodes and DC-DC converter), and the cryptographic processor.

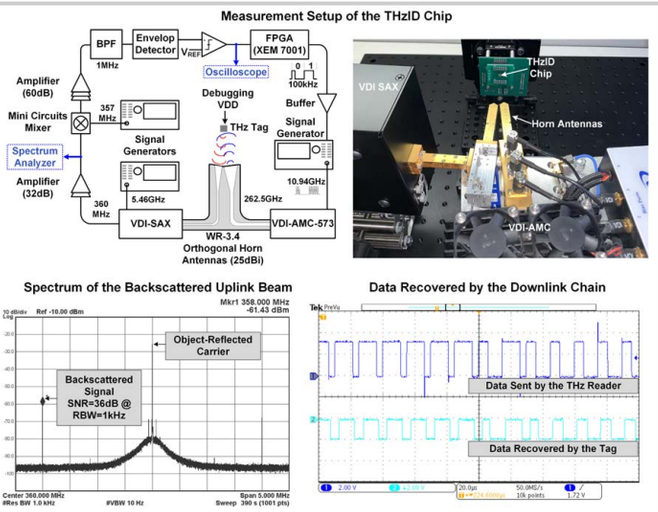


Figure 29.8.4: Chip testing setup, the measured spectrum of the uplink signal, and the measured downlink time-domain data.

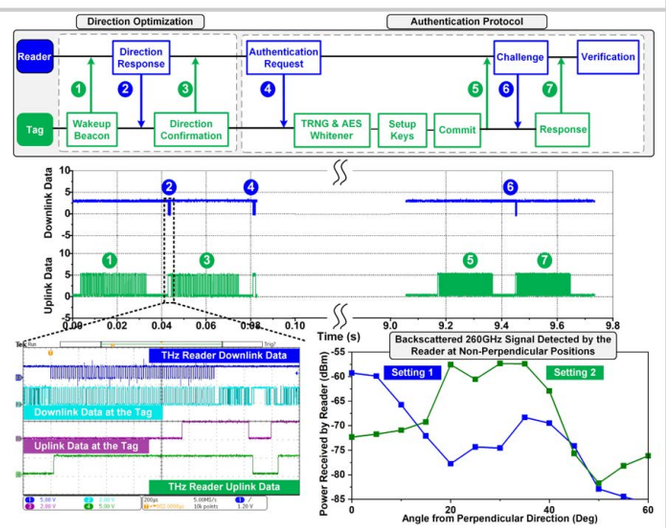
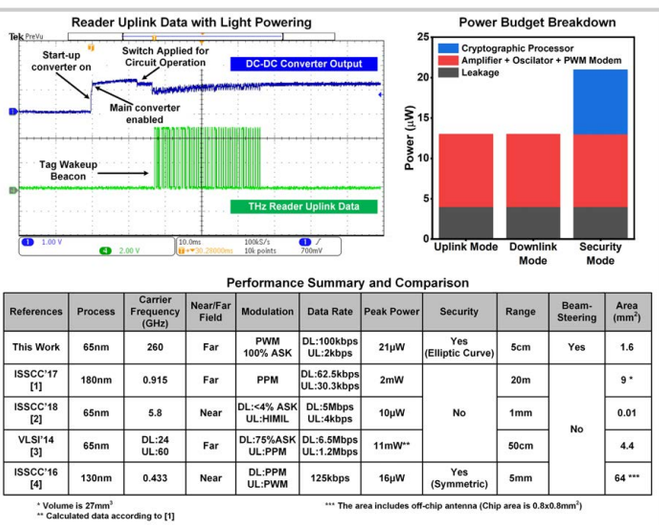


Figure 29.8.5: Measured time-domain communication/security protocol and beam-steering of the tag chip.



Performance Summary and Comparison

References	Process	Carrier Frequency (GHz)	Near/Far Field	Modulation	Data Rate	Peak Power	Security	Range	Beam-Steering	Area (mm²)
This Work	65nm	260	Far	PWM 100% ASK	DL:100kbps UL:2kbps	21µW	Yes (Elliptic Curve)	5cm	Yes	1.6
ISSCC'17 [1]	180nm	0.915	Far	PPM	DL:62.5kbps UL:30.3kbps	2mW	No	20m	No	9 *
ISSCC'18 [2]	65nm	5.8	Near	DL:<4% ASK UL:HIMIL	DL:5Mbps UL:4kbps	10µW		1mm		0.01
VLSI'14 [3]	65nm	DL:24 UL:60	Far	DL:75%ASK UL:PPM	DL:6.5Mbps UL:1.2Mbps	11mW**		50cm		4.4
ISSCC'16 [4]	130nm	0.433	Near	DL:PPM UL:PWM	125kbps	16µW	Yes (Symmetric)	5mm		64 ***

* Volume is 27mm³
** Calculated data according to [1]
*** The area includes off-chip antenna (Chip area is 0.8x0.8mm²)

Figure 29.8.6: Chip startup and uplink operations when the chip is fully powered by light, power budget breakdown, and performance comparison table.

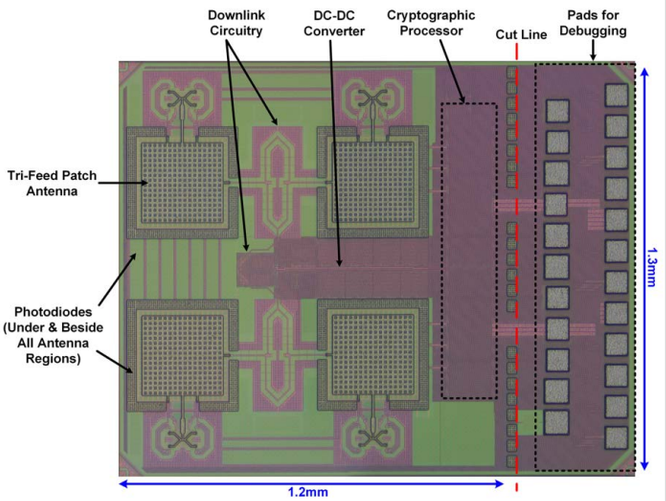


Figure 29.8.7: Die micrograph.

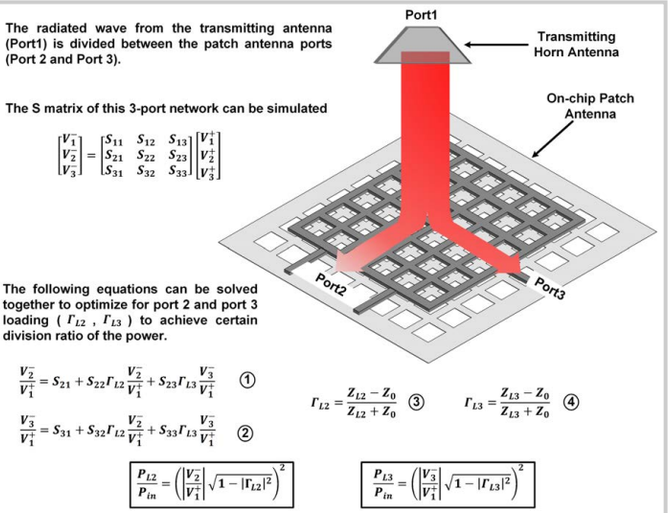


Figure 29.8.S1: Techniques of choosing the termination impedance at Port 2 and Port 3 to achieve certain power splitting ratio.

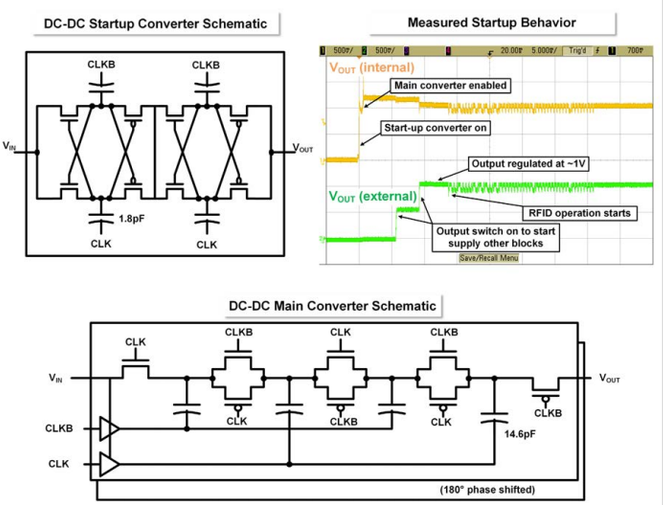


Figure 29.8.S2: DC-DC converter circuits and the measured startup behavior.

	Technology Node	Technology Normalized Area	Cycle Count	ECSM Energy
J.Wolkerstorfer (CRASH'05) [8]	350nm	31kGE	1.1M	550µJ
M. Hutter (CHES'15) [7]	130nm	33kGE	811.2k	56µJ
U. Banerjee (ISSCC'18 [9], JSSC'19 [10])	65nm	65.5kGE + 4KB SRAM	496k	17.6µJ
This work	65nm	25kGE	650k	14.4µJ

Figure 29.8.S3: Comparison with prior-art cryptographic processors.

Aditional References:
[6] J. Hermans et al., "Efficient, Secure, Private Distance Bounding Without Key Updates," *Proc.* 6th ACM Conf.Security Privacy Wireless Mobile Netw., pp. 207–218, Apr. 2013.
[7] M. Hutter et al., "NaCl's crypto_box in Hardware," *Intl. Workshop on Cryptographic Hardware and Embedded Systems*, pp. 81-101, Sept. 2015.
[8] J. Wolkerstorfer et al., "Scaling ECC Hardware to a Minimum," Cryptographic Advances in Secure Hardware (CRASH), pp. 207-214, Sept. 2005.
[9] U. Banerjee et al., "An Energy-Efficient Reconfigurable DTLS Cryptographic Engine for End-to-End Security in IoT Applications," ISSCC, pp. 42-44, Feb. 2018.
[10] U. Banerjee et al., "An Energy-Efficient Reconfigurable DTLS Cryptographic Engine for Securing Internet-of-Things Applications," IEEE JSSC, vol. 54, no. 8, pp. 2339-2352, Aug. 2019.

978-1-7281-3205-1/20/$31.00 ©2020 IEEE