12.5 A Packageless Anti-Tampering Tag Utilizing Unclonable Sub-THz Wave Scattering at the Chip-Item Interface

Eunseok Lee, Xibi Chen, Maitreyi Ashok, Jaeyeon Won, Anantha Chandrakasan, Ruonan Han

Massachusetts Institute of Technology, Cambridge, MA

2024 IEEE International Solid-State Circuits Conference (ISSCC) | 979-8-3503-0620-0/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISSCC49657.2024.10454498

RFID technologies have been widely deployed in supply-chain management for logistics tracking and goods integrity. Recently, millimeter-wave and sub-THz carriers are used to enable on-chip antenna integration and hence packageless, miniature RFID form factors. In [1], a 4.4mm^2 chip with 24GHz downlink and 60GHz uplink is presented. In [2], the tag size is further reduced to 1.6mm^2 by pushing the carrier frequency to 260GHz. While these tiny tags allow for non-intrusive labeling, they still share one drawback with other RFIDs in anti-counterfeiting of goods (Fig. 12.5.1): if an RFID (even if the ID itself is unclonable) is detached from the genuine item and reattached to a fake item, the authentication fails. Unlike in other anti-tampering digital systems, the low power, cost and size budgets in RFIDs pose great challenges to implementing effective anti-tampering capabilities. Current solutions are based on fragile packaging materials that can easily break if physical tampering occurs [3-4]. This mechanism is, however, not reliable (e.g. under gentle or solvent-assisted detachments, and the damage can be recovered) and prevents the monolithic integration and tag miniaturization shown in [1-2]. In comparison, the anti-tampering is significantly enhanced if the fingerprinting for tampering detection is inherent to the "attachment" itself, such as the random glue distribution and the roughness of the item surface, which are very difficult to clone. Based on this principle, in this paper, we present a monolithic tag chip that utilizes a sub-THz wave not only to perform uplink/downlink communications with a compact 4.2mm^2 tag size, but also to detect tampering through the unique sub-THz wave scattering at the chip-item interface with random variation at tens to hundreds of μm scale (Fig. 12.5.1).

The sub-THz fingerprinting approach is illustrated in Fig. 12.5.1. The backside of the CMOS tag chip is attached onto the item surface using epoxy or silicone glue mixed with ~300μm-sized metal particles. The tag routes the reader-radiated sub-THz signal to a metal slot (i.e. radiating slot), which then launches the wave into the silicon substrate (i.e. substrate-mode wave due to the large dielectric constant of silicon $\varepsilon_{Si,r}$=12). The 3D material distribution beneath the chip's surface then causes complex scattering of the wave, which is then partially collected by another metal slot (i.e., sensing slot) and finally backscattered to the reader. Multiple radiating and sensing slots across the 2×2mm^2 chip are deployed, generating a spatial diversity of inter-slot coupling responses within a frequency band. These responses then compose an analog fingerprint for the detection of tampering, which alters the above coupling responses.

The architecture of the tag, operating at f_{RF}=263GHz, is shown in Fig. 12.5.2. The reception and backscattering of the carrier wave from/to the tag reader is achieved using the cross-polarizations of a single on-chip patch antenna. Compared to the standard two-antenna scheme [1], this configuration reduces the chip area and the impact of tag-reader alignment. Correspondingly, the patch antenna has a square shape, in order to provide identical resonance frequency when excited at the orthogonal edges. To distinguish the chip-backscattered signal from the wave directly reflected from the goods' surface, the frequency of the former is shifted by f_m (100s of kHz). To enable precise f_m, the 263GHz input wave is OOK modulated at $2f_m$ in the reader; half of its power is then injected into a MOSFET-based THz square-law detector. The detector output is then amplified and frequency-divided (÷2), and the resultant f_m signal is used as the LO of a BPSK modulator feeding the differential backscatter signal (at $f_{RF}\pm f_m$) back to the patch antenna. The tag is powered by photovoltaic energy, which is provided by on-chip photodiode arrays cascaded with a DC-DC converter.

For the aforementioned glue-pattern probing, another half of the injected sub-THz power is routed to one of the two radiating slot pairs through an SPDT switch (Fig. 12.5.2). The radiation pattern of each radiating slot pair is reconfigurable with a set of two-state phase shifters, allowing for wave steering towards the upper or lower side of the chip substrate (Fig. 12.5.2), as is shown in the simulations in Fig. 12.5.3. On each side that the wave is steered to, the scattered wave is captured by four sensing slots (Fig. 12.5.2). Through three SPDT switches, one of the sensing slots is selected and feeds to the BPSK modulator. The unselected slots are terminated with matching loads to avoid wave re-scattering. Hence, there are 2×2×4=16 inter-slot combinations that provide spatial diversity in the launching and detection of the wave scattering. Since the sensing slots are located near the edges of the chip, a parasitic slot with an open termination is added near each of them (Fig. 12.5.2), so that its re-scattering wave interferes with the radiation of the sensing slot and creates an overall beam pattern that tilts towards the radiating slots at the chip center (simulated pattern shown in Fig. 12.5.3) [5]. That increases the influence from the adhesives and metal particles underneath the chip. Figure 12.5.3 shows the electromagnetic simulations of distinct inter-slot responses from two different silicone glue and iron particle patterns. In Fig. 12.5.2, a digital counter is deployed, so that the SPDT control codes are changed every 1000 clock cycles, and the 16 inter-slot responses are sequentially collected and backscattered to the reader.

Figure 12.5.4 shows the sub-THz BPSK modulator based on a pair of SPDT switches that route the modulator input signal to one of the opposite edges of the patch antenna. The radiation phase is therefore digitally flipped at a rate of f_m. The simulated conversion loss of the BPSK mixer is -14.5dB. Note that the tag input wave at $f_{RF}\pm 2f_m$, although mostly orthogonal to this patch antenna polarization direction, may still inject a cross-polarization leakage into the patch. Then any toggling of the antenna termination impedance due to the BPSK modulator operation will convert this leakage to $f_{RF}\pm f_m$ and backscatter it to the reader, causing blockage of the desired but weak signal containing the glue-pattern information. To avoid this, in Fig. 12.5.4, we ensure that for either "SW=1" or "SW=0", the un-driven edge of the patch is always connected to a matching load through the SPDT switch, so that the above frequency conversion and backscattering of the cross-polarization leakage is suppressed. Compared to a conventional mixer without such leakage suppression, our technique reduces the blocker signals at $f_{RF}\pm f_m$ by 70dB in the simulation.

The chip is fabricated using TSMC 65nm process and has a size of 4.2mm^2. Two orthogonally polarized horn antennas are used to validate the uplink/downlink operations (Fig. 12.5.4). The communication distance is about 4cm. Figure 12.5.5 shows the chip frequency divider clock output, when the tag is powered by the photovoltaic cells and is radiated by an OOK-modulated 263GHz signal from a VDI source. For the uplink, the backscattered THz signal is captured by a WR3.4-subharmonic mixer and a spectrum analyzer. To statistically characterize the sub-THz fingerprint acquisition, the setup in Fig. 12.5.4 is used, where the chip is fed with an external clock and driven by a continuous wave from a VDI-WR3.4-VNAX source sweeping from 261-to-265GHz. Based on the measured spectrum from the WR3.4-mixer (Fig. 12.5.5), the amplitude values at different inter-slot control codes and frequencies are recorded. The edges of the chip are wire-bonded to a PCB; and through a hole on the PCB, the bottom of the chip is pressed against a variety of glue surface patterns applied onto a set of 3D-printed handlers that can be easily swapped (Fig. 12.5.4). The glue surface is based on a mixture of silicone rubber glue and iron powder with a diameter of 250-to-380μm. Figure 12.5.5 shows the measured amplitude variations from different glue samples and different control codes. To de-embed possible variations of frequency response among different readers, the data from each code (1-16) is normalized at each frequency. To show the uniqueness and the randomized variation of samples, inter-sample and intra-sample Euclidean distances (in dB) are plotted in Fig. 12.5.6, of which the mean ratio is 3.6×. With 3× time-averaging, the ratio boosts to 5.5×. Figure 12.5.6 also shows the angle sensitivity of the chip-reader alignment. Next, we used Siamese Neural Networks to distinguish between tag responses effectively. These networks, commonly employed in deep learning for comparing images, were adapted for measuring the similarity between different tag responses. Siamese Neural Networks [6] take a tag response (X) and convert it into a feature vector ($f(X)$). During training, the network efficiently differentiated tag responses by minimizing the Euclidean distance between feature vectors for intra-tag responses (X_1, X_2) and maximizing it for inter-tag responses. 820 pairs of data are used for model training and 153 pairs are used for testing. Figure 12.5.6 provides the Euclidean distances between feature vectors at intra-samples and inter-samples. The measured accuracy is 99.34%. Note that the amount of available data sets is limited at this point, more data collection and model training are needed for future practical applications. The performance summary of the chip is provided in Fig. 12.5.6.

Acknowledgement:
The work is supported by the National Science Foundation (SpecEES ECCS-1824360) and Korea Foundation for Advanced Studies. The authors also would like to thank Virginia Diodes Inc. for supports in instruments.

References:

[1] 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.
[2] M. I. Ibrahim et al., "THzID: A 1.6mm^2 Package-Less Cryptographic Identification Tag with Backscattering and Beam-Steering at 260GHz", *ISSCC*, pp. 454-455, 2020.
[3] R. Y. Shah et al., "Anticounterfeit packaging technologies", J. Adv. Pharm. Technol. Res., vol. 1, no. 4, pp. 368-373, 2010.
[4] XMiNNOV, "Tamper Proof Printable UHF Tag", UY150068A datasheet, 2021.
[5] A. Babakhani et al., "Transmitter Architectures Based on Near-Field Direct Antenna Modulation," *IEEE JSSC*, vol. 43, no. 12, pp. 2674-2692, 2008.
[6] J. Bromley et al., "Signature verification using a "Siamese" time delay neural network," Advances in neural information processing systems, vol. 6, 1993.

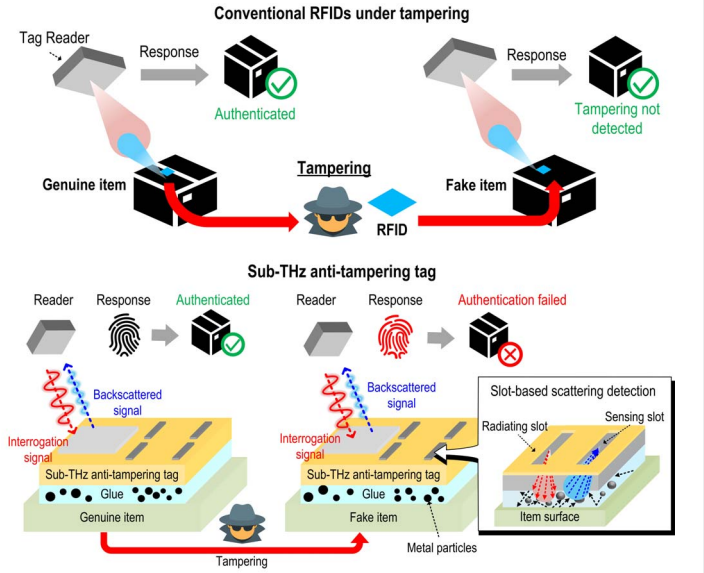


Figure 12.5.1: A tampering attack scenario within a supply chain (top), and the concept of sub-THz unclonable anti-tampering tag (bottom).

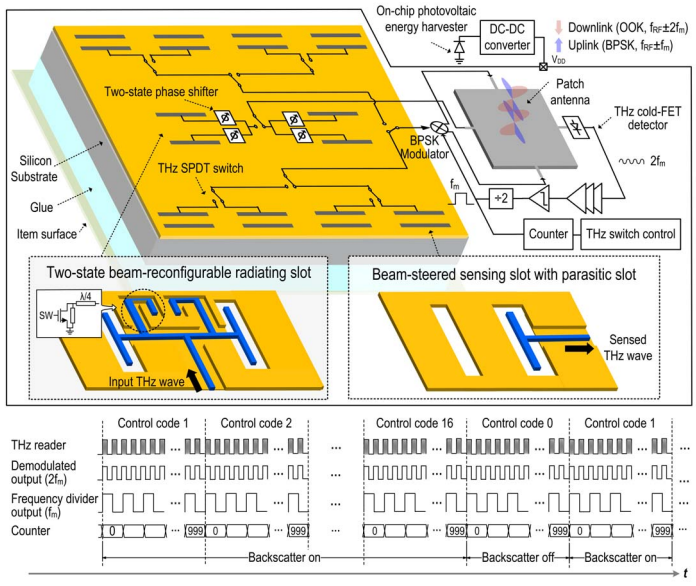


Figure 12.5.2: System diagram and operation of the sub-THz anti-tampering tag.

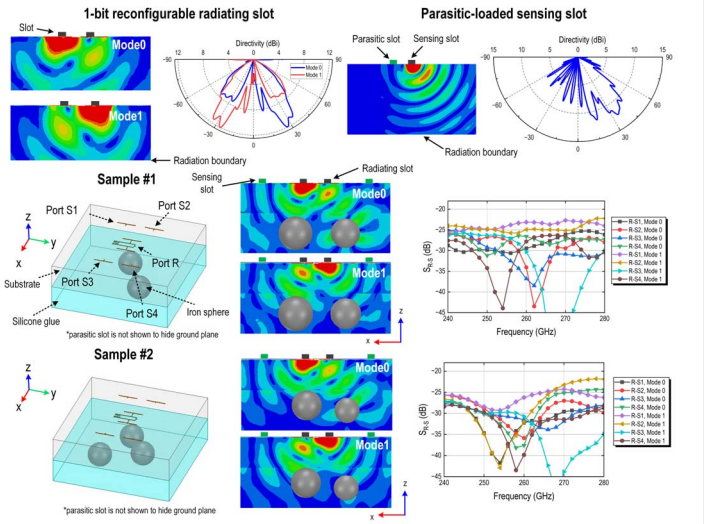


Figure 12.5.3: Simulated radiation patterns of the two-state reconfigurable radiating slot (top left), simulated radiation pattern of the parasitic-loaded sensing slot (top right), and the simulated inter-slot frequency responses of two glue patterns (bottom).

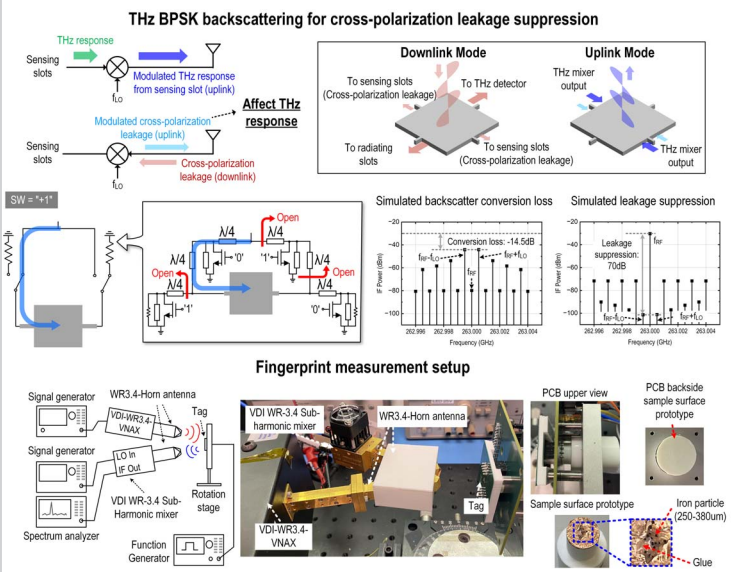


Figure 12.5.4: THz BPSK backscattering for cross-polarization leakage suppression, and the fingerprinting measurement setup.

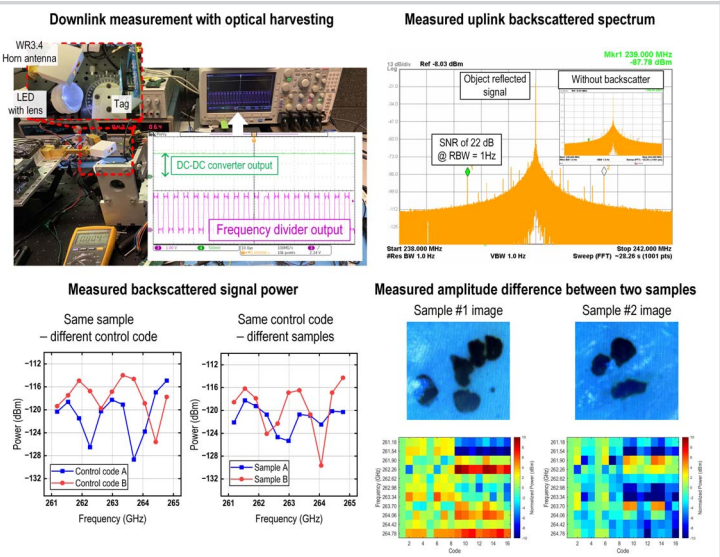
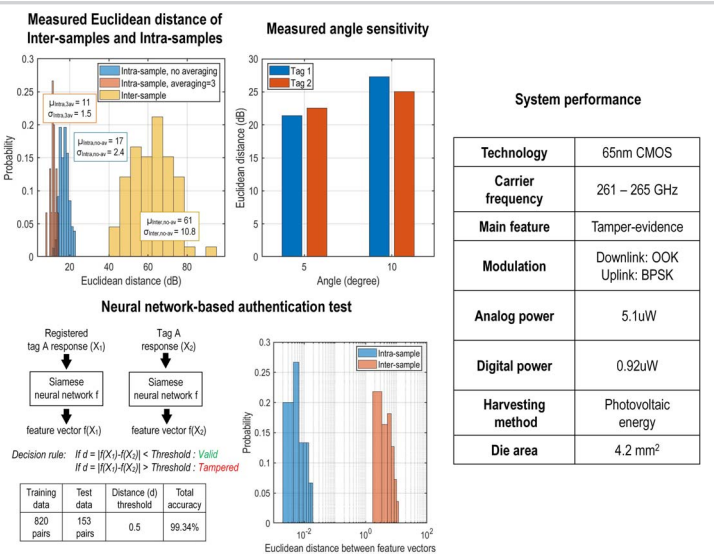


Figure 12.5.5: Downlink time-domain measurement with optical harvesting, measured backscattered spectrum of uplink, measured backscattered signal power, and the amplitude difference between two glue patterns.



System performance	
Technology	65nm CMOS
Carrier frequency	261 – 265 GHz
Main feature	Tamper-evidence
Modulation	Downlink: OOK Uplink: BPSK
Analog power	5.1uW
Digital power	0.92uW
Harvesting method	Photovoltaic energy
Die area	4.2 mm²

Figure 12.5.6: Measured Euclidean distance between intra/inter samples, measured angle sensitivity in Euclidean distance, neural-network-based authentication test results, and the system performance.

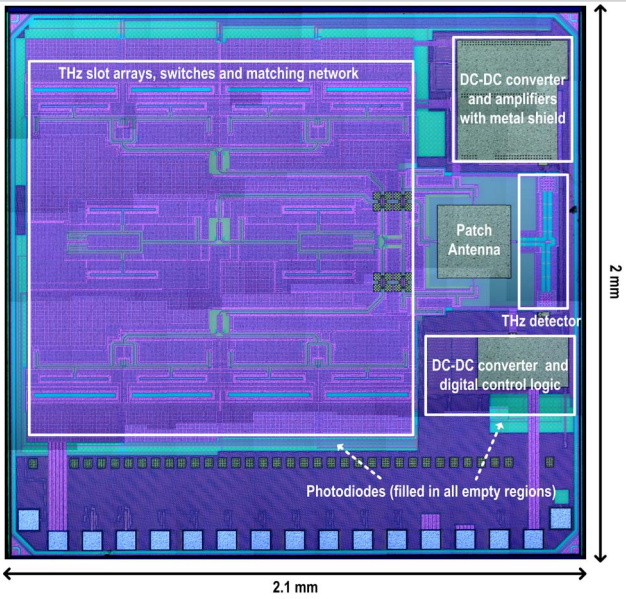


Figure 12.5.7: Die micrograph.

979-8-3503-0620-0/24/$31.00