Wireless Anti-Counterfeiting Labels Using RF Oscillators With Graphene Quantum Capacitors

Yichong Ren, *Graduate Student Member, IEEE*, Chia-Heng Sun, Chien-Hao Liu, *Member, IEEE*, Chung-Tse Michael Wu, *Senior Member, IEEE*, and Pai-Yen Chen, *Fellow, IEEE*

***Abstract*—We propose here a lightweight, reconfigurable graphene-based physical unclonable function (PUF) for wireless identification and authentication applications. Specifically, the PUF-based anti-counterfeiting label consists of a micro-coil antenna and a graphene quantum capacitor, forming an *LC* oscillator. Natural fluctuations in the Dirac point and residue charge density of graphene enable each graphene oscillator to have a unique radio-frequency (RF) response (i.e., electromagnetic fingerprint), whose uniqueness and entropy can be further enhanced by exploiting the exceptional point (EP)-based (near-field) wireless interrogation system. These randomized and irreproducible RF responses can be properly discretized and digitized to form a binary bitmap of cryptographic keys. Our simulation results show that PUF keys generated by graphene oscillators can exhibit high uniqueness and randomness, large encoding capacity, as well as reconfigurability enabled by electrostatically or chemically tuning the graphene's Fermi energy. The proposed PUF-based wireless anti-counterfeiting labels may open a new pathway for the development of lightweight security protocol for radio-frequency identification (RFID), near-field communications (NFC), wireless access control, and Internet-of-things (IoTs), among other wireless applications.**

***Index Terms*—Physically unclonable function, graphene, graphene quantum capacitor, radio-frequency identification, anti-counterfeiting tags, wireless security.**

I. Introduction

In THE era of the Internet of Things (IoTs) and machine-to-machine (M2M) communications, a myriad of Internet-connected devices have been deployed to sense and share data, and identify information about the object. In the meantime, the vast amount of information exchanged between IoT devices has given rise to risks associated with privacy and security [1]. However, traditional cryptographic keys stored in non-volatile memories (NVMs) may be vulnerable to different cyberattacks, such as reverse engineering, malware attacks, direct physical probing, and machine learning-based modeling attacks, particularly for lightweight, resource-scarce IoTs and smart devices connected via near-field communication (NFC) and radio-frequency identification (RFID) techniques. Very recently, physical unclonable functions (PUFs) have been proposed and demonstrated to be an efficient and cost-effective hardware security solution without the need for relatively expensive NVMs, thus being particularly suitable for IoT security applications. The PUFs are generally based on unique physical variations occurring naturally during manufacturing processes, such that cryptographic keys are generated by leveraging the device-specific output "responses" triggered by a given input "challenge," i.e., a challenge-response pair (CRP). Currently, PUFs are mainly based on deep sub-micrometer level variations in complementary metal-oxide-semiconductor (CMOS) circuits, such as arbiters [2] and ring oscillators [3], [4]. Although PUFs composed of digital circuits have demonstrated satisfactory performance and reliability, their power consumption, scalability, and entropy used to generate random numbers (or keys) still require significant improvements. Moreover, most existing PUFs are susceptible to physical attacks, such as invasive probing or side-channel attacks, where an adversary can decipher cryptographic keys based on power consumption or electromagnetic radiation. It is, therefore, of paramount importance to develop new types of lightweight, low-cost, and potentially reconfigurable PUFs for securing communication and encryption in future IoT ecosystems and networks.

Two-dimensional (2D) materials, whose physical properties are sensitive to nanofabrication process variations, are regarded as ideal candidates for making PUF instances [5]. Due to the atomic thinness and high surface-to-volume ratio of 2D materials, even a low defect level on the material surface substantially influences the electrical characteristics of 2D material-based electronic devices [6], [7], [8]. Early works have shown that CRPs can be generated in graphene field-effect transistors (GFETs), of which the gate voltage and drain current correspond to the "challenge" and "response." In order to increase the encoding capacity, a PUF instance is built using a complex circuit consisting of tens of GFETs; this, however, results in increased cost and the calibration difficulty [9]. In this context, quantum capacitance uniquely induced in 2D electron gas (2DEG) devices or 2D materials have been found to be highly sensitive to chemical and electrostatic doping.

Received 23 November 2024; revised 22 December 2024; accepted 8 January 2025. Date of publication 13 January 2025; date of current version 28 January 2025. This work was supported by the National Science Foundation under Grant ECCS-2229659. The work of Chien-Hao Liu was supported by the National Taiwan University under Grant NTU-113L8518. The work of Chung-Tse Michael Wu was supported by the Ministry of Education (MOE), Taiwan, under Grant NTU-113V1042-1. *(Yichong Ren and Chia-Heng Sun are co-first author.) (Corresponding author: Pai-Yen Chen.)*

Yichong Ren, Chia-Heng Sun, and Pai-Yen Chen are with the Department of Electrical and Computer Engineering, University of Illinois Chicago, Chicago, IL 60607 USA (e-mail: yren27@uic.edu; csun42@uic.edu; pychen@uic.edu).

Chien-Hao Liu is with the Department of Mechanical Engineering, National Taiwan University, Taipei 10617, Taiwan (e-mail: cliu82@ntu.edu.tw).

Chung-Tse Michael Wu is with the Department of Electrical and Computer Engineering, Rutgers University, New Brunswick, NJ 08854 USA, and also with the Department of Electrical Engineering, National Taiwan University, Taipei 10617, Taiwan (e-mail: ctmwu@ntu.edu.tw).

Digital Object Identifier 10.1109/JRFID.2025.3529343

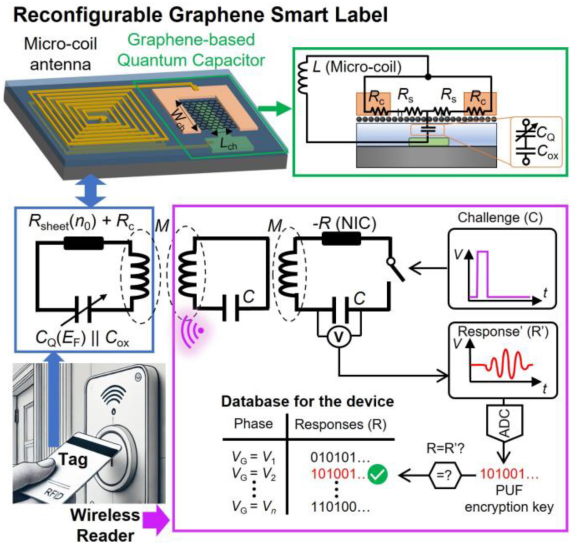

Fig. 1. Schematic of a graphene-based anti-counterfeiting label used in the wireless identification and authentication system. Here, a compact micro-coil antenna is connected to a reconfigurable graphene quantum capacitor.

Recent studies have reported that ultracompact capacitive sensors can be built using the variable graphene quantum capacitor [10], [11]. Moreover, by connecting a graphene quantum capacitor to a coil antenna, a wireless inductor-capacitor (*LC*) sensor for contactless (bio-) chemical and gas sensing can be realized [10], [12].

In this paper, we propose a lightweight, small-footprint, and cost-effective PUF based on an *RLC* oscillator consisting of a graphene quantum capacitor and a coil antenna, as shown in Fig. 1. The quantum capacitance in each graphene-based *RLC* oscillator could vary due to imperfections and uncertainties in nanofabrication, which result in highly random oscillatory motions that can be probed using an external coil antenna. As a result, graphene-based *RLC* oscillators can be regarded as simple, battery-free tags with encryption functionality, particularly suitable for wireless identification and authentication, and secured communication applications. Furthermore, the tunable quantum capacitance enables self-reconfigurability and reprogrammability, leading to abundant CRPs and enhanced encoding capacity of an encrypted tag. In this paper, we also propose the parity-time (*PT*)-symmetric wireless interrogation/readout system to maximize the uniqueness and randomness of PUF keys generated by graphene-based compact tags; here, the uniqueness and randomness are characterized by the Shannon and permutation entropy and the inter-device Hamming distance, respectively [13]. To validate the compatibility of the proposed PUF device and architecture with the short-range wireless communication modality, we will test the PUF performance under different digital modulation schemes, such as binary amplitude shift keying (BASK) and on-off keying (OOK) [14].

II. Graphene-Based PUF Labels and *PT*-Symmetric Wireless Readout Platform

A. Graphene-Based Reconfigurable RLC Oscillators

Fig. 1 shows the graphene-based anti-counterfeiting tag, consisting of a planar microstrip spiral inductor (self-inductance $L = 1.8\mu\text{H}$) and a graphene quantum capacitor. The device structure of a graphene quantum capacitor is similar to a GFET but with the joint source-drain electrode and the back-gate electrode connected to the two terminals of a coil antenna, as sketched in the inset of Fig. 1. The equivalent capacitance is a series combination of the geometric capacitance (C_{ox}) and the quantum capacitance (C_{Q}), and the equivalent resistance R considers the contact resistance at the interface between graphene and metal electrodes R_{c} and the sheet resistance of graphene R_{sh} [9]. Any variation in the Fermi energy of gated graphene is equivalent to a voltage drop across the quantum capacitance. The quantum capacitance per unit area can be formalized as [15]:

$$C_{\text{Q}} = \frac{2e^2}{\sqrt{\pi}\hbar^2 v_{\text{F}}^2}\sqrt{|E_{\text{F}}|^2/\pi\hbar v_{\text{F}} + n_0}, \tag{1}$$

where e denotes electron charge, $\hbar$ is the reduced Planck constant, E_{F} stands for the Fermi energy of graphene, v_{F} represents the Fermi velocity of graphene (10^6m/s), and n_0 is the residual carrier concentration originating from charge puddles and surface corrugations. The geometric capacitance per unit area is $C'_{\text{ox}} = \varepsilon_{\text{ox}}\varepsilon_0/t_{\text{ox}}$ where ε_{ox} and t_{ox} are the static dielectric constant and thickness of the gate oxide, and ε_0 is the free space permittivity; here, we assume an ultrathin HfO_2 gate oxide with $\varepsilon_{\text{ox}} = 20$ [16] and t_{ox}= 20 nm. The total capacitance is given by:

$$C = \left(\frac{C_{ox}C_{\text{Q}}}{C_{ox} + C_{\text{Q}}}\right) \times (W_{\text{ch}}L_{\text{ch}}). \tag{2}$$

The sheet resistance of graphene can be written as:

$$R_{\text{Sheet}} = \frac{1}{\mu e\sqrt{p^2 + n_0{}^2}}, \tag{3}$$

where μ is the carrier mobility (here, 3000 $\text{cm}^2/\text{V.s}$ is assumed without loss of generality), and the carrier sheet density $p = (E_{\text{F}}/\sqrt{\pi}\hbar v_{\text{F}})^2$ [15], [16], which is tuned by the graphene's Fermi level. It should be noted that E_{F} and n_0 are susceptible to environmental disorders, which in turn result in fluctuations in C_{Q} and R_{Sheet} between individual graphene devices. Figs. 2(a) and 2(b) report the experimental results of variations of E_{F} and n_0 for 50 p-type GFETs, respectively. E_{F} follows a Gaussian distribution with a mean value of -0.1178 eV and a standard deviation of 0.0151 eV. n_0 also displays a similar distribution with a mean value of $4.322 \times 10^{11}\text{cm}^{-2}$ and a standard deviation of $0.468 \times 10^{11}\text{cm}^{-2}$. As illustrated in Figs. 2(c) and 2(d), C_{Q} and R_{Sheet} calculated using Eqs. (1) and (3) are quite sensitive to fluctuations in residual carrier density and Fermi energy. Noticeably, the Fermi energy can be dynamically tuned through chemical doping and/or electrostatic gating. For example, the Fermi level shift ΔE_{F} can be related to the gate bias voltage that can be written as [19]: $V_{\text{G}} = en/C_{\text{OX}} + \Delta E_{\text{F}}/e$. From the equivalent circuit model in the upper panel of Fig. 1, the total resistance of the graphene-based *RLC* oscillator can be written as:

$$R = \frac{1}{2}\left(\frac{R_{\text{c}}}{W_{\text{ch}}} + \frac{1}{2}R_{\text{Sheet}}\frac{L_{\text{ch}}}{W_{\text{ch}}}\right), \tag{4}$$

where R_{c} is the width-normalized contact resistance (here $R_{\text{c}} = 1\ \text{k}\Omega\cdot\mu\text{m}$), the width and length of the graphene channel

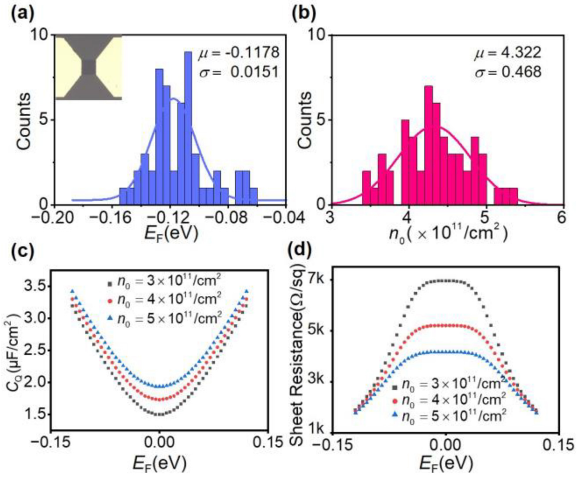

Fig. 2. Experimentally measured distributions of (a) Fermi energy E_{F} and (b) residue charge density n_0 among 50 graphene field-effect transistors. (c) quantum capacitance and (d) sheet resistance of graphene as a function of E_{F}.

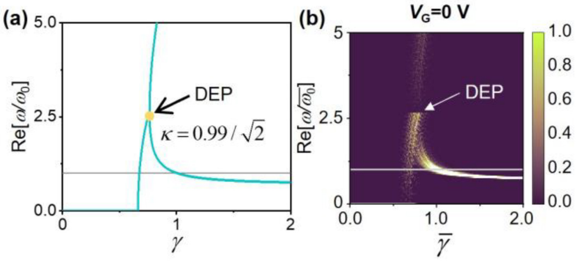

Fig. 3. (a) Real part of eigenfrequencies against the gain-loss parameter for the third-order PT-symmetric electronic system; here, $\kappa = 0.99/\sqrt{2}$ and $\omega_0 = 1/\sqrt{LC}$. (b) Probability contours of (a), which is obtained with 200 random graphene-based anti-counterfeiting labels with $V_{\mathrm{G}} = 0\ V$; here, $\overline{\gamma} = (1/\overline{R}) \times \sqrt{L/\overline{C}}$ and $\overline{\omega}_0 = 1/\sqrt{L\overline{C}}$, where $\overline{R}$ and $\overline{C}$ are the average total resistance and the averaged total capacitance of PUF labels, respectively.

are $W_{\mathrm{ch}} = 10.5\ \mu\mathrm{m}$ and $L_{\mathrm{ch}} = 7\ \mu\mathrm{m}$, respectively, and the sheet resistance R_{Sheet} is obtained from Eq. (3).

B. PT-Symmetric Electronic System for Wireless Readout

The concept of PT-symmetry or space-time inversion symmetry was first proposed in quantum physics by Bender in 1998 [20] and has been extended to different wave systems described by the Helmholtz equation. In the realm of electronics, PT-symmetry systems can be constituted by contactlessly coupled and balanced gain (active$-RLC$ oscillator) and loss (passive RLC oscillator) [21], [22]. It has been experimentally observed that the exceptional point (EP) found in PT-symmetric non-Hermitian electronic systems divides the parameter space into the exact symmetry phase and the broken symmetry phase, accompanied by the bifurcation effect around the EP [23], [24], [25], [26] In other words, the EP is a singular point where Taylor series expansion fails to converge in the multivalued complex eigenspectrum. Recent theoretical and experimental studies have reported that high entropy and flicker noises will be amplified near the EP, which could undermine the reliability and reproducibility of the EP-based circuits. Nonetheless, such property may be leveraged for building a high-entropy source for cryptographic random number generation [27].

The bottom panel of Fig. 1 shows the schematic of the proposed wireless identification and authentication system, comprising the graphene-based anti-counterfeiting labels and the wireless readout platform based on the third-order PT-symmetric electronic system, which is formed by an active $-RLC$ reader, a LC repeater, and a passive RLC tag (i.e., graphene-based PUF instance). By applying Kirchhoff's laws to the circuit in Fig. 1, an effective PT-symmetric non-Hermitian Hamiltonian H_{eff}can be obtained [23], and the eigenfrequencies of the system are roots of the characteristic polynomial $|H_{\mathrm{eff}} - \omega\mathbf{I}| = 0$, The eigenfrequencies in units of the natural frequency $\omega_0 = 1/\sqrt{LC}$ can be expressed as [26]:

$$\omega_n/\omega_0 = 1, \sqrt{\frac{2\gamma^2 - 1 \pm \sqrt{1 - 4\gamma^2 + 8\gamma^4\kappa^2}}{2\gamma^2\left(1 - 2\kappa^2\right)}}, \tag{5}$$

where $\kappa = M/L$ is the coupling strength between each oscillator and $\gamma = R^{-1}\sqrt{L/C}$ stands for the gain-loss parameter. Fig. 3(a) depicts the evolution of the real part of the eigenfrequencies for the third-order PT-symmetric electronic system. As can be seen from Fig. 3(a), the onset of a bifurcation effect associated with the spontaneous PT-symmetry-breaking is signified by the EP, given by [24], [26]:

$$\gamma_{\mathrm{EP}} = \frac{1}{2\kappa}\sqrt{1 + \sqrt{1 - 2\kappa^2}}. \tag{6}$$

As seen in Eq. (5), the system exhibits a divergent point (DP) at $\kappa = 1/\sqrt{2}$, which may further enhance the eigenfrequency bifurcation level at an EP [24], [26]. When an EP coincides with a DP (so-called divergent exceptional point or DEP), the bifurcation effect can become drastic, which in turn makes the system's eigenfrequencies and eigenmodes very sensitive to perturbations. When imposing a constant electromotive force through a switch on the reader (i.e., switching on a voltage pulse generator at the initial moment; see Fig. 1), the oscillatory motion seen in the temporal response is a superposition of multiple harmonics described in Eq. (5). The temporal voltage response on the reader's capacitor, which varies among graphene-based labels due to nanomanufacturing process variations (e.g., random dopant/strain fluctuations in graphene), can be digitized into a binary sequence with an analog-to-digital converter (ADC), as shown in Fig. 1. A DEP with inherently high entropy may augment the discrepancy between output responses of PUF-based anti-counterfeiting labels, thereby guaranteeing high uniqueness of keys. During the wireless identification and authentication process, a pulse signal (input challenge) is applied to the reader to trigger the oscillation, and then the temporal voltage waveform recorded on the reader (output response) is processed into a digital format.

III. Results and Discussions

In this section, we will conduct a detailed performance evaluation for the reconfigurable PUF cryptography based on the graphene anti-counterfeiting labels and the PT wireless readout platform operating near the DEP.

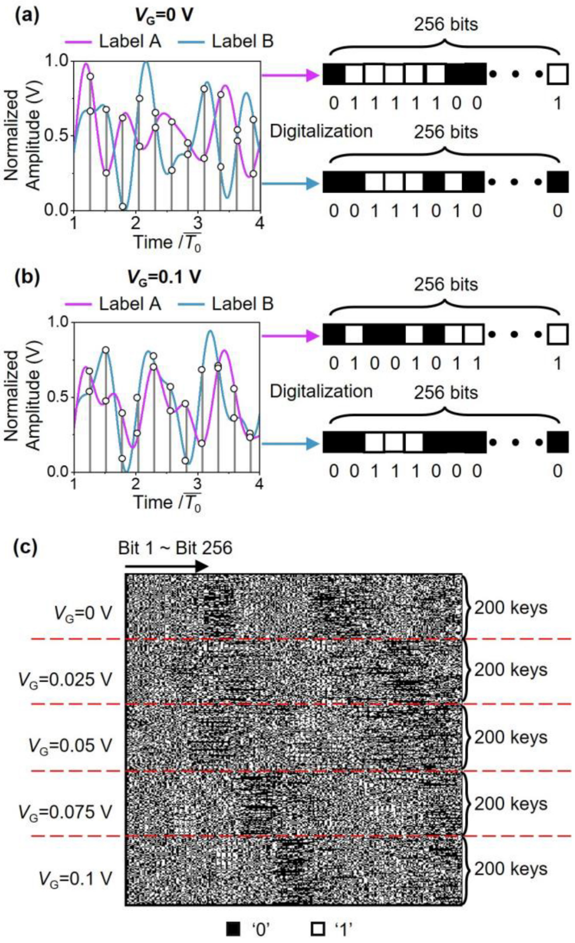

Fig. 4. (a) Normalized transient voltage responses of two randomly selected graphene-based PUF labels; here, $\overline{T}_0 = 1/\overline{f}_0 = 2\pi/\overline{\omega}_0$. (b) is similar to (a), but for the reconfigurable responses of the same labels B. (c) Bitmap formed by 200 digitized PUF keys (256 bits in each PUF); here, 5 sub-bitmaps are obtained by varying V_Gs from 0 V to 0.1 V.

A. Generation of Reconfigurable PUF Keys

In our numerical experiment, 200 graphene-based oscillators as PUF instances were randomly generated. Each oscillator is equipped with a coil antenna (self-inductance $L = 1.8$ μH) and a graphene quantum capacitor with randomized R and C. In our numerical experiment, realistic variations in γ values between graphene-based oscillators were assumed. The equivalent R and C values of quantum capacitors, which are calculated using Eqs. (2) and (4), are determined by E_F and n_0 that follow a Gaussian distribution fitted from measurement results in Fig. 2. The average total capacitance $\overline{C} \approx 0.525$ pF and the average total resistance $\overline{R} \approx 1.8$ kΩ. The coupling strength between the two coil antennas $\kappa = 0.635$. The circuit simulations were performed using the Advanced Design System (ADS). Fig. 4(a) plots the normalized temporal voltage responses of two out of 200 graphene-based RF labels (Label A and Label B); here, the graphene device is unbiased. Inevitable perturbations in γ between graphene-based RF labels can lead to quite different output responses. Moreover, the presence of DEP in the PT system amplifies the randomness of output responses, as can be seen in the probability distributions of eigenfrequencies in Fig. 3(b). From Fig. 3(b), we observe that near the DEP, complex-valued eigenfrequencies are hardly repeatable. Fig. 4(b) plots the temporal voltage responses for Label A and Label B in Fig. 4(a) under different external bias conditions ($V_G = 0.1$ V). As can be seen in Fig. 4(b), the output response can be uniquely reconfigured, depending on the Fermi energy in graphene. For each PUF instance, the temporal output response is converted to a 256-bit CRP sequence as a digitally encrypted key. During the period $0 < t < 4\overline{T}_0$, there is a total of 64 sampling points, and each sample is quantified into 4 bits. The detailed analog-to-digital conversion method can be found in [27]. Fig. 4(c) shows the combined bitmaps of all reconfigurable PUF keys acquired from the PT-symmetric wireless readout. For cryptographic applications, a preferred bitmap should have an equal distribution of 0s and 1s. From Fig. 4(c), it is visible that 0s and 1s is the bitmap are uniformly and randomly distributed, regardless of the external bias that reconfigures the CRP sequences.

B. Randomness of PUF Keys

Shannon Entropy is generally used to evaluate the randomness of binary PUF keys, given by:

$$\begin{aligned} E_x &= -\left[p_x \log_2 p_x + (1-p_x)\log_2(1-p_x)\right], \\ E_y &= -\left[p_y \log_2 p_y + \left(1-p_y\right)\log_2\left(1-p_y\right)\right], \end{aligned} \tag{7}$$

where p_x and p_y are probabilities of obtaining 1s along the x-axis and y-axis of the bitmap, respectively. Ideally, the probability of observing 1s and 0s in the response should be equal, namely the bit uniformity is 50%, yielding $E_x = E_y = 1$. Figs. 5(a) and 5(b) report the distributions of E_x and E_y for the bitmap in Fig. 4. It can be seen that E_x and E_y are close to unity (the mean values of E_x and E_y are 0.9809 and 0.9939, respectively) at different $V_G S$ values, demonstrating excellent randomness and reconfigurability.

Permutation entropy is another important metric for analyzing the randomness of binary PUF keys [28], which can be expressed as:

$$E_p = -\sum_{j=1}^{n!} p_j \ \log\left(p_j\right), \tag{8}$$

where n is the selected order for computation (usually more than 2), and p_j stands for the frequency of the permutation configuration normalized by the total number of subsequences (here $n = 3$ is chosen). Fig. 5(c) reports distributions of E_p under different bias conditions. In all cases, the mean E_p value is greater than 0.98. Based on the above entropy analyses, we conclude that the PUF keys exhibit nearly perfect uniformity and are reconfigurable, thanks to intrinsic random tendency and tunability of C_Q (E_F) and R_{Sheet} in graphene. Moreover, the high randomness can also be attributed to enhanced entropy in the vicinity of a DEP of the PT-symmetric wireless readout platform. Here, we also employ the National Institute of Standards and Technology (NIST) randomness test suite [29] to validate the randomness of binary sequences. Table I summarizes the NIST randomness test results at different $V_G S$ values. A true random number generator (TRNG)

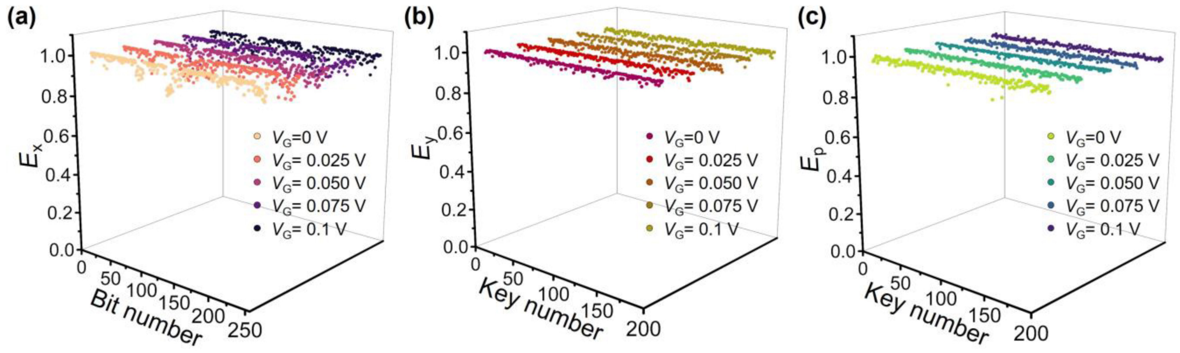

Fig. 5. Entropy E_{x} (a), E_{y} (b), and E_{p} (c) obtained from the bitmap in Fig. 4(c). All entropy values are close to unity, demonstrating excellent randomness between graphene-based PUF labels.

TABLE I
NIST Statistical Test Results for PUF Keys Obtained With Different Gate Voltages

NIST randomness test	$V_G = 0$ V		$V_G = 0.025$ V		$V_G = 0.05$ V		$V_G = 0.075$ V		$V_G = 0.1$ V	
	P-values	Pass?	P-values	Pass?	P-values	Pass?	P-values	Pass?	P-values	Pass?
Frequency	0.8666	Yes	0.8806	Yes	0.8806	Yes	0.8736	Yes	0.8736	Yes
FB	0.4294	Yes	0.4727	Yes	0.1630	Yes	0.3786	Yes	0.3422	Yes
Runs	0.3355	Yes	0.3276	Yes	0.2080	Yes	0.3291	Yes	0.3360	Yes
LOR	0.1090	Yes	0.1019	Yes	0.0753	Yes	0.1273	Yes	0.1126	Yes
FFT	0.2605	Yes	0.2749	Yes	0.3259	Yes	0.2872	Yes	0.3414	Yes
NOT(m=5)	0.9846	Yes	0.9889	Yes	0.9908	Yes	0.9876	Yes	0.9889	Yes
Serial(m=4)	0.3405	Yes	0.4875	Yes	0.2288	Yes	0.4872	Yes	0.3679	Yes
AppEn(m=3)	0.3371	Yes	0.3799	Yes	0.2005	Yes	0.4237	Yes	0.4061	Yes
Cum.Sum	0.4367	Yes	0.4556	Yes	0.2242	Yes	0.4183	Yes	0.4159	Yes

must have a P-value that exceeds the threshold of 0.01 for each test. It is evident that the proposed PUF passes all NIST statistical tests and is dynamically reconfigurable.

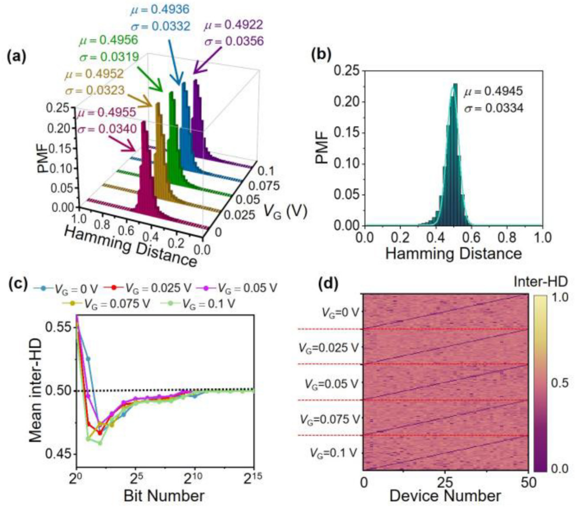

Fig. 6. (a) Inter-HD histograms for the reconfigurable PUF keys in Fig. 4(c) at different V_{G}s. (b) Inter-HD histogram of all PUF keys in Fig. 4(c). (c) Mean inter-HDs as the function of the number of bits under different bias conditions; here, the sampling rate is adaptive to study the convergence of uniqueness represented by the mean of inter-HD among PUF keys. (d) Pairwise comparison maps for the reconfigurable PUF.

C. Uniqueness of PUF Keys

The uniqueness characterized by the inter-device Hamming distance (inter-HD) represents the distinctiveness of one device compared to another. This indicator matters as every PUF instance should function as a distinct security primitive necessary for device-specific identification and verification. Ideally, fifty percent of the bits are identical, whereas the remaining half are different, namely the mean inter-HD should be 50%. The mean inter-HD can be formalized as:

$$\overline{\text{HD}_{\text{inter}}} = \frac{2}{N(N-1)} \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} \frac{\sum_{l=1}^{L_{\text{bit}}} \left(K_{i,l} \oplus K_{j,l}\right)}{L_{\text{bit}}}, \tag{9}$$

where $N = 200$ represents the number of CRPs, $L_{\text{bit}} = 256$ is the length of bitstrings translated from the transient temporal response, K_i stands for the ith cryptographic key, and ⊕ signifies the XOR logic operation. Fig. 6(a) reports the inter-HD distributions presented using the probability mass function (PMF) for the reconfigurable PUF keys. We find that the Gaussian fitting of average inter-HD (μ) and standard deviation (σ) are almost centered at 0.5 and 0, respectively, regardless of the applied bias voltage that reconfigures PUF keys. As the V_{G} increases from 0 V to 0.1 V, the mean inter-HD decreases slightly from 0.4955 and 0.4922, while the standard deviation increases slightly from 0.0340 to 0.0356.

TABLE II
ENCODING CAPACITY UNDER DIFFERENT BIAS CONDITIONS

V_G	Key size	Encoding capacity
0 V	216	1.25×10^{65}
0.025 V	239	1.34×10^{72}
0.050 V	246	8.90×10^{73}
0.075 V	227	1.84×10^{68}
0.1 V	197	2.33×10^{59}

Such results demonstrate that the reconfigurable PUF keys exhibit excellent uniqueness. Fig. 6(b) reports the inter-HD distributions for all reconfigurable PUF keys in Fig. 6(a). The mean and standard deviation of the inter-HD histogram are 0.4945 and 0.0334. Such results clearly show that the graphene-based PUF instances can exhibit strong security characteristics with reconfigurability, achievable with electrostatic and/or chemical gating that effectively varies the Fermi level in graphene. As the bit number increases, the mean inter-HD tends to converge toward 0.5 (shown in Fig. 6(c)). The results are consistent across a certain range of V_GS.

To demonstrate that each encrypted key is unique and uncorrelated, we also present the pairwise mapping of inter-HD in Fig. 6(d); here, the first 50 CRPs in the bitmap [Fig. 4(b)] are selected. In the pairwise comparison map, the diagonal line is 0, while the off-diagonal elements should be as close to 0.5 as possible. From Fig. 6(d), we find that almost all off-diagonal elements are ~0.5, indicating that there is a high degree of uncorrelation among all PUF keys. This is valid for all different reconfigurable operations.

D. Encoding Capacity

The encoding capacity of a cryptographic key generator (i.e., the maximum possible number of characters per PUF instance) manifests its compelling resistance to counterfeiting. For a binary response, the encoding capacity can be expressed as c^k, where c is 2, standing for “0” and “1”, $k = \mu(1-\mu)/\sigma^2$, μ and σ are the mean and standard deviation of the inter-HD histogram [30]. The key sizes k and the encoding capacity of the proposed PUF instances are summarized in Table II. We observe that the proposed graphene-based PUF tags and the PT-symmetric wireless readout platform can result in high encoding capacity and thus great immunity to possible cracking. Furthermore, the encoding capacity remains large when the PUF instances are reconfigured under different bias conditions. In most cases, the encoding capacity is larger than 200, which is not possible with conventional passive and chipless RFID tags.

IV. INTEGRATION WITH MODULATION TECHNIQUE FOR NEAR-FIELD WIRELESS COMMUNICATIONS

The proposed PUF labels can be utilized to secure NFC, RFID, and short-range wireless communication modalities that make use of amplitude modulation schemes, such as BASK and OOK [14]. Within the BASK modulation scheme, binary representations are determined by the presence or absence of the carrier signals. In this scenario, the reader and the PUF label can be equipped with a single-port single-through (SPST) switch to generate the amplitude-modulated waveform. Additionally, the bit period can be judiciously determined to ascertain the temporal viability of the PUF-secured system. In our numerical experiment, we assume the negative impedance converter (NIC) on the reader is switched on and off with different time intervals (bit rate): $(0.75\overline{T}_0, \overline{T}_0, 1.5\overline{T}_0)$,where $\overline{T}_0 = 1/\overline{f}_0 = 2\pi/\overline{\omega}_0$. Fig. 7(a) presents the voltage across the capacitor of the PUF label. Fig. 7(b) presents the inter-HD of the BASK-modulated waveform, for which the temporal voltage response in a period is digitized to extract the PUF key. As shown in Fig. 7(b), when the bit period is longer than $\overline{T}_0$, the mean value of inter-HD is close to 0.5, implying a large encoding capacity and key size. On the other hand, when the bit period is smaller than $\overline{T}_0$, the mean value of inter-HD somewhat decreases, namely the increase in data rate may come at the cost of sacrificing a bit of the key size. Here, we demonstrate that the proposed PUF can achieve lightweight wireless authentication compatible with communication protocols.

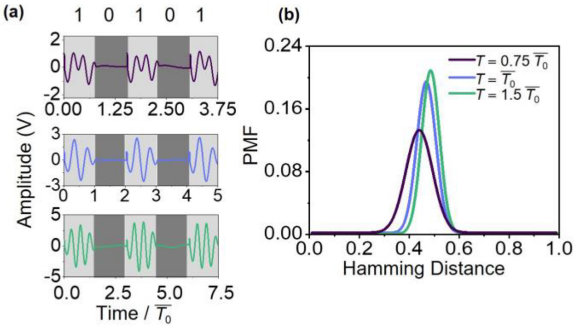

Fig. 7. (a) Simulation results of binary amplitude modulation at different modulation speeds (from top to bottom: bit period = $0.75\overline{T}_0$, $\overline{T}_0$ and $1.5\overline{T}_0$). PUF-based encryption keys are extracted from the BASK-modulated temporal voltage response. (b) Distributions of inter-HDs of PUF keys are extracted from the BASK-modulated signal.

V. CONCLUSION

In summary, we have proposed and numerically studied a lightweight and reconfigurable PUF-based anti-counterfeiting label consisting of a micro-coil antenna loaded with a graphene quantum capacitor. Given the random fluctuations in residue charge density and Fermi energy in graphene, there exists randomness and stochasticity between these labels formed by graphene oscillators. We have exploited the PT-symmetric wireless readout platform to interrogate the proposed anti-counterfeiting labels. Our results show that the encryption keys extracted from each PUF instance exhibit excellent randomness and uniqueness and, more interestingly, are robustly reconfigurable through chemical doping and/or electrostatic gating. Table III provides a detailed comparison between the proposed PUF system and the state-of-the-arts [30], [31], [32], [33]. Compared to other emerging PUFs, the proposed PUF technique exhibits excellent uniformity and reconfigurability

TABLE III
SUMMARY OF PERFORMANCE METRIC AMONG DIFFERENT PUFS

Ref.	Technique	Randomness (entropy)	Uniqueness (inter-HD)	Reconfigurability
[31]	Silicon photonics	High	μ=0.5	Not reported
[32]	Optical imaging	Ultra-High	μ=0.4937 σ=0.0556	High
[30]	GFET-based integrated circuits	High	μ=0.47	High
[33]	Carbon nanotube network	High	μ=0.5	Not reported
This work	Graphene quantum capacitor-based RFID system	Ultra-High	μ=0.4956 σ=0.0319	High

with reduced physical size and cost compared to the optical and photonic PUFs, which require bulky readout instruments such as ultrafast laser and optical microscopy. The proposed PUF system may also outperform other nanomaterial-based PUF architectures in terms of performance, cost, and design and fabrication complexity.

In addition, we have also demonstrated the possibility of integrating the proposed PUF instance with a digital modulator (e.g., BASK modulation scheme) for secure wireless communication. The proposed PUF technique sheds light on lightweight, low-cost hardware security solutions for many applications that have strong demands for wireless identification and cryptographic authentication, such as RFID, NFC, anti-counterfeiting/anti-fraud labels, wireless access control, and IoT devices and networks.

REFERENCES

[1] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[2] D. P. Sahoo, D. Mukhopadhyay, R. S. Chakraborty, and P. H. Nguyen, "A multiplexer-based arbiter PUF composition with enhanced reliability and security," *IEEE Trans. Comput.*, vol. 67, no. 3, pp. 403–417, Mar. 2018.

[3] X. Xin, J.-P. Kaps, and K. Gaj, "A configurable ring-oscillator-based PUF for Xilinx FPGAs," in *Proc. 14th Euromicro Conf. Digit. Syst. Design*, Aug. 2011, pp. 651–657.

[4] L. Bossuet, X. T. Ngo, Z. Cherif, and V. Fischer, "A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon," *IEEE Trans. Emerg. Topics Comput.*, vol. 2, no. 1, pp. 30–36, Mar. 2014.

[5] H.-L. Jiang, J. Pan, W. Zhou, H.-M. Li, and S. Liu, "Fabrication and application of arrays related to two-dimensional materials," *Rare Metals*, vol. 41, pp. 262–286, Jan. 2022.

[6] P.-Y. Chen and A. Alù, "Atomically thin surface cloak using graphene monolayers," *ACS Nano*, vol. 5, no. 7, pp. 5855–5863, 2011.

[7] T. Heine, "Transition metal chalcogenides: Ultrathin inorganic materials with tunable electronic properties," *Acc. Chem. Res.*, vol. 48, no. 1, pp. 65–72, 2015.

[8] H. Huang et al., "Chemical-sensitive graphene modulator with a memory effect for Internet-of-Things applications," *Microsyst. Nanoeng.*, vol. 2, no. 1, 2016, Art. no. 16018.

[9] S. Peng et al., "The sheet resistance of graphene under contact and its effect on the derived specific contact resistivity," *Carbon*, vol. 82, pp. 500–505, Feb. 2015.

[10] D. A. Deen, E. J. Olson, M. A. Ebrish, and S. J. Koester, "Graphene-based quantum capacitance wireless vapor sensors," *IEEE Sensors J.*, vol. 14, no. 5, pp. 1459–1466, May 2014.

[11] A. H. Pourasl, S. H. S. Ariffin, M. T. Ahmadi, N. Gharaei, R. A. Rashid, and R. Ismail, "Quantum capacitance model for graphene FET-based gas sensor," *IEEE Sensors J.*, vol. 19, no. 10, pp. 3726–3732, May 2019.

[12] Q.-A. Huang, L. Dong, and L.-F. Wang, "LC passive wireless sensors toward a wireless sensing platform: Status, prospects, and challenges," *J. Microelectromech. Syst.*, vol. 25, no. 5, pp. 822–841, Oct. 2016.

[13] S. Kim, K. Lee, M.-H. Oh, J.-H. Lee, B.-G. Park, and D. Kwon, "Physical unclonable functions using ferroelectric tunnel junctions," *IEEE Electron Device Lett.*, vol. 42, no. 6, pp. 816–819, Jun. 2021.

[14] C. Erdogan, I. Myderrizi, and S. Minaei, "FPGA implementation of BASK-BFSK-BPSK digital modulators [testing ourselves]," *IEEE Antennas Propag. Mag.*, vol. 54, no. 2, pp. 262–269, Apr. 2012.

[15] J. Xia, F. Chen, J. Li, and N. Tao, "Measurement of the quantum capacitance of graphene," *Nat. Nanotechnol.*, vol. 4, no. 8, pp. 505–509, 2009.

[16] J. B. Park, W. S. Lim, B. J. Park, I. H. Park, Y. W. Kim, and G. Y. Yeom, "Atomic layer etching of ultra-thin HfO$_2$ film for gate oxide in MOSFET devices," *J. Phys. D, Appl. Phys.*, vol. 42, no. 5, 2009, Art. no. 55202.

[17] J.-H. Chen, C. Jang, S. Adam, M. S. Fuhrer, E. D. Williams, and M. Ishigami, "Charged-impurity scattering in graphene," *Nat. Phys.*, vol. 4, no. 5, pp. 377–381, 2008.

[18] S. Kim et al., "Realization of a high mobility dual-gated graphene field-effect transistor with Al$_2$O$_3$ dielectric," *Appl. Phys. Lett.*, vol. 94, no. 6, 2009, Art. no. 62107.

[19] B. Kaczer et al., "A brief overview of gate oxide defect properties and their relation to MOSFET instabilities and device and circuit time-dependent variability," *Microelectron. Reliab.*, vol. 81, pp. 186–194, Feb. 2018.

[20] C. M. Bender and S. Boettcher, "Real spectra in non-hermitian hamiltonians having P T symmetry," *Phys. Rev. Lett.*, vol. 80, no. 24, pp. 5243–5246, 1998.

[21] J. Schindler, Z. Lin, J. M. Lee, H. Ramezani, F. M. Ellis, and T. Kottos, "*PT*-symmetric electronics," *J. Phys. A, Math. Theor.*, vol. 45, no. 44, 2012, Art. no. 444029.

[22] Y. Ren, M. Yang, H. Pan, M. Farhat, A. E. Cetin, and P.-Y. Chen, "PT symmetry-enabled physically unclonable functions for anti-counterfeiting RF tags," *IEEE Trans. Antennas Propag.*, vol. 72, no. 6, pp. 5129–5140, Jun. 2024.

[23] J. Schindler, A. Li, M. C. Zheng, F. M. Ellis, and T. Kottos, "Experimental study of active LRC circuits with *PT* symmetries," *Phys. Rev. A*, vol. 84, no. 4, 2011, Art. no. 40101.

[24] M. Sakhdari, M. Hajizadegan, Q. Zhong, D. N. Christodoulides, R. El-Ganainy, and P.-Y. Chen, "Experimental observation of P T symmetry breaking near divergent exceptional points," *Phys. Rev. Lett.*, vol. 123, no. 19, 2019, Art. no. 193901.

[25] M. Sakhdari, M. Hajizadegan, and P.-Y. Chen, "Robust extended-range wireless power transfer using a higher-order PT-symmetric platform," *Phys. Rev. Res.*, vol. 2, no. 1, 2020, Art. no. 13152.

[26] M. Sakhdari, Z. Ye, M. Farhat, and P.-Y. Chen, "Generalized theory of PT-symmetric radio-frequency systems with divergent exceptional points," *IEEE Trans. Antennas Propag.*, vol. 70, no. 10, pp. 9396–9405, Oct. 2022.

[27] M. Yang, L. Zhu, Q. Zhong, R. El-Ganainy, and P.-Y. Chen, "Spectral sensitivity near exceptional points as a resource for hardware encryption," *Nat. Commun.*, vol. 14, no. 1, p. 1145, 2023.

[28] M. Riedl, A. Müller, and N. Wessel, "Practical considerations of permutation entropy: A tutorial review," *Eur. Phys. J. Spec. Topics*, vol. 222, no. 2, pp. 249–262, 2013.

[29] A. Rukhin et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," U.S. Dept. Commerce, Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep. 800-22, 2001.

[30] A. Dodda, S. S. Radhakrishnan, T. F. Schranghamer, D. Buzzell, P. Sengupta, and S. Das, "Graphene-based physically unclonable functions that are reconfigurable and resilient to machine learning attacks," *Nat. Electron.*, vol. 4, no. 5, pp. 364–374, 2021.

[31] B. C. Grubel et al., "Silicon photonic physical unclonable function," *Opt. Express*, vol. 25, no. 11, pp. 12710–12721, 2017.

[32] H. Zuo, Q. Li, H. Zheng, Y. Yang, and X. Zhao, "An optically-reconfigurable PUF based on logarithmic photoreceptor of CMOS dynamic vision sensors," *IEEE Trans. Electron Devices*, vol. 69, no. 9, pp. 5395–5398, Sep. 2022.

[33] J.-S. Jeong, G. S. Lee, T.-E. Park, K.-Y. Lee, and H. Ju, "Bio-inspired electronic fingerprint PUF device with single-walled carbon nanotube network surface mediated by M13 bacteriophage template," *Sci. Rep.*, vol. 12, no. 1, 2022, Art. no. 20096.

Yichong Ren (Graduate Student Member, IEEE) received the B.S. degree in electronic information science and technology from Northwest University, Xi'an, China, in 2022. He is currently pursuing the Ph.D. degree with the University of Illinois Chicago, USA.

His research interests include electromagnetics, RF microwave circuits and sensors, and wireless communications.

Chia-Heng Sun received the M.S. degree in physics from National Central University, Taoyuan, Taiwan, in 2015. He is currently pursuing the Ph.D. degree in electrical and computer engineering with the University of Illinois Chicago, Chicago, IL, USA. His research interests include measurement and fabrication of 2-D materials and nanodevices.

Chien-Hao Liu (Member, IEEE) received the B.S. and M.S. degrees in mechanical engineering from National Taiwan University, Taipei, Taiwan, in 2005 and 2007, respectively, and the M.S. and Ph.D. degrees in electrical engineering from the University of Wisconsin–Madison (UW-Madison), Madison, WI, USA, in 2013 and 2014, respectively, where he was a Research Assistant with the Electrical and Computer Engineering Department from 2011 to 2014. From 2014 to 2015, he was a Research Associate with the Electrical and Computer Engineering Department, UW-Madison. He is currently an Associate Professor with the Mechanical Engineering Department, National Taiwan University. His research interests include piezoelectric antennas, frequency selective surfaces, and acoustic metamaterials.

Chung-Tse Michael Wu (Senior Member, IEEE) received the B.S. degree in electrical engineering from National Taiwan University (NTU), Taipei, Taiwan, in 2006, and the M.S. and Ph.D. degrees in electrical engineering from the University of California at Los Angeles, (UCLA) Los Angeles, CA, USA, in 2009 and 2014, respectively.

From September 2008 to June 2014, he was a Graduate Student Researcher with the Microwave Electronics Laboratory, UCLA. In 2009, he served as a Summer Intern at Bell Labs, Murray Hill, NJ, USA. In 2012, he was a Special Joint Researcher with the Japan Aerospace Exploration Agency, Sagamihara, Japan. From 2014 to 2017, he was an Assistant Professor with the Department of Electrical and Computer Engineering, Wayne State University, Detroit, MI, USA. In 2017, he joined Rutgers University, New Brunswick, NJ, USA, as an Assistant Professor and was promoted to Tenured Associate Professor in 2022. Since 2024, he has been an Associate Professor at NTU. His research interests include applied electromagnetics, antennas, passive/active microwave and millimeter-wave components, RF systems, and metamaterials. He has received several awards, including the National Science Foundation Faculty Early Career Development Award, the WSU College of Engineering Faculty Research Excellence Award in 2016, the Defense Advanced Research Projects Agency (DARPA) Young Faculty Award in 2019, and the DARPA Director's Fellowship Award in 2021. In 2022, he was also a recipient of the Board of Trustees Research Fellowship for Scholarly Excellence at Rutgers University. He is currently serves as an Associate Editor for IEEE MICROWAVE AND WIRELESS TECHNOLOGY LETTERS, IEEE JOURNAL OF ELECTROMAGNETICS, RF AND MICROWAVES IN MEDICINE AND BIOLOGY, and IEEE ACCESS. He is a member of the Technical Committees for IEEE MTT-28 and MTT-4.

Pai-Yen Chen (Fellow, IEEE) received the B.S. and M.S. degrees from National Chiao Tung University, Hsinchu, Taiwan, in 2004 and 2006, respectively, and the Ph.D. degree from The University of Texas at Austin, Austin, TX, USA, in 2013. He was an Assistant Researcher with Taiwan Semiconductor Research Institute, Hsinchu, Taiwan, from 2006 to 2009. He was a Research Scientist with the Intellectual Ventures' Metamaterial Commercialization Center, Bellevue, WA, USA, from 2013 to 2014. He is a Professor with the Department of Electrical and Computer Engineering, University of Illinois Chicago (UIC), Chicago, IL, USA. He has been involved in multidisciplinary research on applied electromagnetics, RF and microwave antennas and circuits, wireless sensors and systems, nanoelectronics, nanophotonics, plasmonics, metamaterials, and metasurfaces. He has received quite a few prestigious awards, including the IEEE Sensors Distinguished Lecturer from 2024 to 2026, the National Science Foundation CAREER Award, the IEEE Sensors Council Young Professional Award, the IEEE Sensors Council Technical Achievement Award, the IEEE AP-S Raj Mittra Travel Grant, the IEEE Chicago Distinguished Senior Research and Development Award, the SPIE Rising Researcher Award, ACES Early Career Award, the PIERS Young Scientist Award, the Young Scientist Awards from URSI General Assembly and URSI Commission B: Electromagnetics, IOP Emerging Leader in Measurement Science and Technology, Air Force Research Laboratory Faculty Fellowship, the University Scholar of University of Illinois, university of Illinois Scholar (awarded to 10 among all UI professors each year), UIC Researcher of the Year, UIC College of Engineering Faculty Research Award, College of Engineering Faculty Research Excellence Award, the Donald Harrington Fellowship, the Taiwan Ministry of Education Study Abroad Award, the Honorary Member of the Phi Tau Phi Scholastic Honor Society of Taiwan, the United Microelectronics Corporation Scholarship, the best student paper awards/finalists from the IEEE Antennas and Propagation Symposium in 2011, 2013, 2016, and 2021, respectively, the IEEE International Microwave Symposium in 2015, the IEEE Sensors Conference in 2016, the IEEE Wireless Power Transfer Conference in 2021, the USNC-URSI Ernest K. Smith Student Paper Award in 2012, and the Second Prize of the Student Design Contest from the IEEE Antennas and Propagation Symposium in 2022. He currently serves as an Associate Editor for IEEE SENSORS JOURNAL, the IEEE TRANSACTIONS ON ANTENNAS AND PROPAGATION, and IEEE ANTENNAS AND WIRELESS PROPAGATION LETTERS, and a Senior Editor for IEEE JOURNAL OF SELECTED AREAS IN SENSORS. He was a Former Associate Editor of *Applied Electromagnetics*, IEEE JOURNAL OF RADIO FREQUENCY IDENTIFICATION, and IEEE JOURNAL OF ELECTROMAGNETICS, RF AND MICROWAVES IN MEDICINE AND BIOLOGY, a Former Lead Guest Editor of IEEE JOURNAL OF SELECTED AREAS IN SENSORS and a Former Guest Editor of the IEEE TRANSACTIONS ON ANTENNAS AND PROPAGATION. He currently serves as the IEEE APS/MTTS Chicago Chapter Chair and the IEEE CRFID Associate Vice President. He was the IEEE Sensors Chicago Chapter Chair/Founder from 2019 to 2021, and the ACES Board of Directors from 2021 to 2023.