PT Symmetry-Enabled Physically Unclonable Functions for Anti-Counterfeiting RF Tags

Yichong Ren, Minye Yang, Hongyi Pan, *Member, IEEE,* Mohamed Farhat, Ahmet Enis Cetin, *Fellow*, *IEEE*, and Pai-Yen Chen, *Senior Member*, *IEEE*

***Abstract*—We present the concept and design of physically unclonable function (PUF)-based cryptographic key generation, which exploits the uniqueness of electromagnetic signatures of radio frequency (RF)-transponder tags derived from random physical variations during manufacturing. When the RF tag is inductively coupled to a designated readout circuitry, forming the higher-order parity-time (*PT*) symmetry, high sensitivity, and high entropy near the system's divergent exceptional point (DEP) can maximize the difference in temporal/spectral responses among tags. Our results show that due to the DEP singularity, PUF keys generated by converting the temporal response into binary sequences can exhibit excellent encryption performance in terms of randomness, uniqueness, encoding capacity, and resilience to machine learning-based modeling attacks. This RF PUF technique may pave the way towards ultra-lightweight, low-cost, and efficient hardware security solutions for wireless identification and authentication in various applications, including but not limited to the security of near-field connectivity and telematic infrastructure, wireless access control, authentication protocols for internet-of-things (IoTs), and anti-counterfeiting labels for goods, foods, and drugs.**

***Index Terms*— Physically unclonable function, electromagnetic signatures, parity-time symmetry, exceptional points, radio-frequency identification, hardware security**

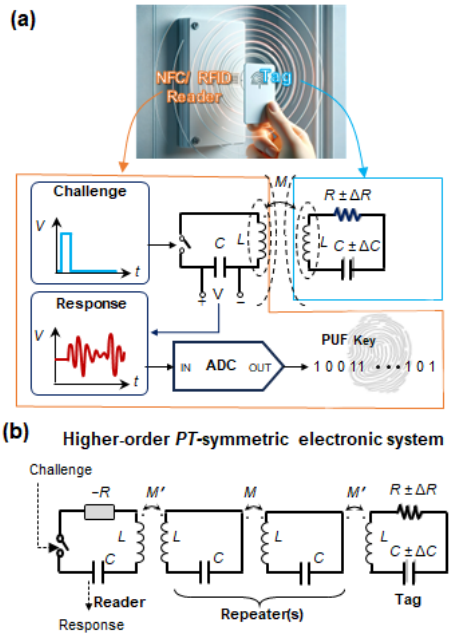


Fig. 1. Schematic diagrams of PUF-based wireless identification implemented using (a) the traditional readout system based on RFID/NFC coils, and (b) the higher-order (fourth-order) *PT*-symmetric electronic system composed of an active reader, a passive tag, and two repeaters.

I. Introduction

Rapid advent in internet-of-things (IoTs) benefiting from near-field communication (NFC) and radio-frequency identification (RFID) platforms has unlocked the digitally-connected universe, of which vast amounts of perceptual devices are wirelessly connected to enable data-driven smart ecosystems, such as smart cities and industry 4.0 [1]. In this regard, there is a high demand for new encryption technologies that can effectively protect sensitive information, such as classified data and privacies, and can be capable of combating adversarial attacks, such as those modeling attacks based on advanced machine- and deep-learning algorithms [2]. Wireless security and anti-counterfeiting solutions are imperative to many fields, such as wireless access control, safety in telematics infrastructure, encrypted wireless communications, and authentication of RFID/NFC tags and merchandise labels (e.g., foods and drugs) [3], to name a few. Nonetheless, wireless devices exploiting currently affordable authentication methods based on digital security keys stored in memory chipsets are usually vulnerable to exhaustive decryptions and device cloning [4]. To make things worse, advances in artificial intelligence (AI)-assisted electromagnetic side-channel attacks have further made traditional digital encryption methods more vulnerable [5].

To mitigate the shortcomings of digital signatures, hardware security alternatives, such as physically unclonable functions (PUFs), have emerged as promising and cost-effective methods for device authentication and cryptographic key generation [6]. Current PUF technologies are largely based on physical

Y. Ren, M. Yang, A. E. Cetin, and P. Y. Chen are affiliated with the Department of Electrical and Computer Engineering, University of Illinois Chicago, Chicago, IL 60607 USA.

Hongyi Pan is affiliated with Feinberg School of Medicine, Northwestern University, Chicago, IL 60611, USA.

M. Farhat is affiliated with Computer, Electrical, and Mathematical Science and Engineering Division, King Abdullah University of Science and Technology, Thuwal 23955, Saudi Arabia.

Corresponding author: P. Y. Chen; e-mail: pychen@uic.edu

P.Y.C. would like to thank National Science Foundation Grant No. ECCS-CCSS 2229659 for supporting this work. A. E. Cetin would like to thank University of Illinois Discovery Partners Institute.

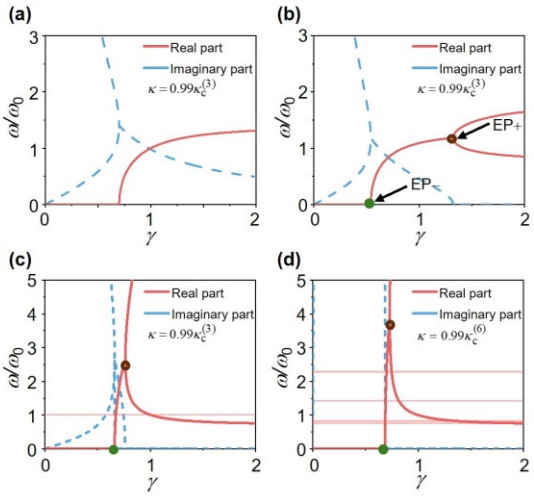


Fig. 2. Complex eigenspectra of (a) the traditional wireless interrogation system and (b)–(d) the *PT*-symmetric electronic systems with the standard (second-order), third-order, and sixth-order configurations. Here, $\kappa = 0.99\times(1/\sqrt{2})$ is used for the traditional wireless interrogation system and the standard/third-order *PT* system, and $\kappa = 0.99\times(1/2)$ is used for the sixth-order *PT* system. The DEP occurs at $\kappa = 1/\sqrt{2}$ in the third-order *PT* system and at $\kappa = 1/2$ and $\kappa' = 1/\sqrt{2}$ in the sixth-order *PT* system.

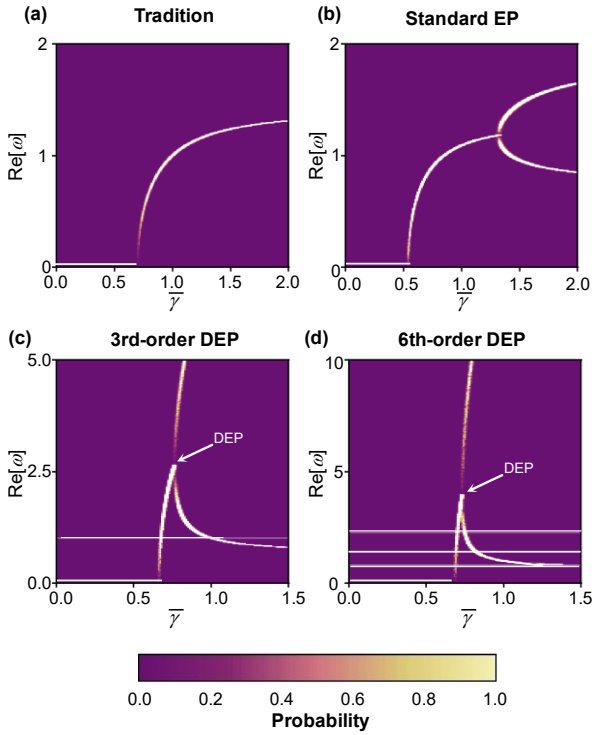


Fig. 3. Probabilities of real parts of eigenfrequencies of (a) the traditional wireless interrogation system and (b)–(d) the *PT*-symmetric electronic system with standard, third-order, and sixth-order configurations. Here, 1000 randomly generated tags are interrogated by the same reader, and their resistance and capacitance distributions follow a Gaussian distribution function with a standard deviation $\sigma = 0.01$. $\bar{\gamma}$ represents the mean value of γ.

property variations that naturally occur in complementary metal-oxide-semiconductor (CMOS) fabrication processes and are implemented in integrated circuits (ICs) or chipsets, including arbiter PUFs [7], static random-access memory (SRAM) PUFs [8], monostable PUFs [9], and voltage divider PUFs [10], among many others. Each PUF device can be regarded as a challenge-response unit, of which a given "input challenge" and its corresponding "output response" form a challenge-response pair (CRP), as shown in Fig. 1(a). In principle, each challenge is associated with a unique response, which must be reproducible over time. However, with the continuous pursuit of high reliability and yield in the semiconductor industry, gross area defects have been minimized and almost eliminated in the mature, well-controlled fabrication lines. This paradoxically makes the generated CRP less unique [11], [12]. As a result, silicon- or CMOS-based PUFs may still be susceptible to machine/deep learning-based modeling attacks [13]. Although beyond-silicon digital PUFs (e.g., graphene ICs [14]) have been recently proposed to improve the uniqueness of CRPs, they still face challenges associated with the implementation cost, system complexity, compatibility with CMOS ICs, and scalability.

To address the aforementioned issues, we herein propose a lightweight, low-cost, and potentially NFC/RFID-compatible PUF based on parity-time (*PT*)-symmetric RF systems, as sketched in Fig. 1(b). The non-Hermitian physical systems with *PT* symmetry have been extensively studied in different spectral ranges due to their anomalous properties, such as exceptional points (EPs) and phase transitions in the eigenspectrum [15]–[22]. In the RF and low-frequency domains, a standard *PT*-symmetric electronic system can be realized with inductively-coupled $-RLC$ and RLC resonators, respectively representing the spatially-distributed gain and loss [21], [23]–[28]. This system has a bifurcating singularity—exceptional point (EP), which marks the boundary between the exact symmetry phase and the broken symmetry phase. At the EP, the *PT* system's eigenfrequencies undergo a bifurcation and complex splitting process, as shown in Fig. 2(b). In addition, the higher-order *PT*-symmetric electronic system can be built with one or multiple LC repeaters, as shown in Fig. 1(b) [25], [26]. It has been theoretically and experimentally demonstrated that in higher-order (third-order and higher) *PT*-symmetric electronic systems, EP and divergent point (DP) may overlap (so-called divergent exceptional point or DEP) such that the eigenfrequency bifurcation effect can be quite drastic [25], [26]. Although in the vicinity of DEP, the system can respond to perturbations in an ultrasensitive manner, it will also inevitably amplify noises and spectral/temporal signal uncertainty by the same factor, since there are random perturbations in the lumped element values due to manufacturing errors. Nonetheless, this shortcoming for sensing applications may be exploited as an excellent source of entropy to generate PUF keys. Recently, we have shown that electromagnetic PUFs and cryptographic random number generators can be implemented by exploiting the exceptional sensitivity existing in the *PT*-symmetric electronic circuit operating near the DEP [27], as well as in the *PT*-symmetric metasurfaces operating at the self-dual spectral singularity associated with the coherent perfect absorber-laser (CPAL) point [29]. Following our seminal discovery, in this paper, we will investigate the possibility of generating high-quality PUF keys using the generalized *PT*-symmetric electronic systems

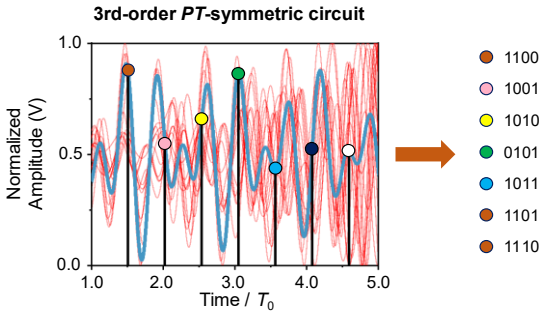


Fig. 4. Simulated (normalized) transient responses of voltage across the capacitor in the reader used to interrogate 15 randomly generate tags, which are interrogated using the third-order *PT* wireless interrogation system in Fig. 2(c). Each colored point in the analog time response is digitalized into a 4-bit binary code, and a total of 64 points are sampled to obtain a sequence of 256 bits.

comprising an active reader and neutral repeater(s) for contactless interrogation of RF-transponder tags. Specifically, the system is designed to operate near an EP or DEP where the highest entropy is obtained. We will exploit the statistical and quantitative indicators, such as randomness, uniqueness, pairwise comparison, and encoding capacity, to evaluate the performance of PUFs. We will gauge the resiliency of the proposed PUF against ML-based modeling attacks.

II. Design of *PT*-Symmetric PUF Systems

A. Generalized PT-Symmetric Electronic Systems

PT-symmetric systems that are invariant under the combined spatial-inversion (P) and time-reversal (T) transformations can be readily realized in the Helmholtz and Maxwellian systems constituted by coupled resonators with spatially distributed and balanced gain and loss [23], [30]. Fig. 1(b) shows the schematic diagram of the Nth-order *PT*-symmetric electronic systems consisting of an active $-RLC$ tank, a passive RLC tank, and lossless LC repeaters. When the system is used for wireless telemetry, these resonators represent the RF reader, tag, and repeaters (which are commonly used to increase the interrogation range). Applying Kirchhoff's laws to the system results in an effective Hamiltonian H_{eff}, which is non-Hermitian and commutes with the combined *PT* operator [23], [30]. The system's eigenfrequencies can be obtained as roots of the polynomial equation $\left|H_{\text{eff}}-\omega\mathbf{I}\right|=0$. The eigenfrequencies of the standard *PT*-symmetric system, which comprises inductively coupled $-RLC$ and RLC tanks, can be derived as [23]:

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

where $\gamma=R^{-1}\sqrt{L/C}$ is the dimensionless gain-loss parameter, $\kappa=M/L$ is the coupling strength between tanks, M is the mutual inductance, L is the self-inductance of the coil, and $\omega_0=1/\sqrt{LC}$. Figs. 2(a) and 2(b) plot the evolution of complex eigenfrequencies of the traditional RFID interrogation system and the standard *PT*-symmetric one. A traditional reader for short-range wireless connectivity comprises a coil antenna and a tuning capacitor, as shown in Fig. 1(a).

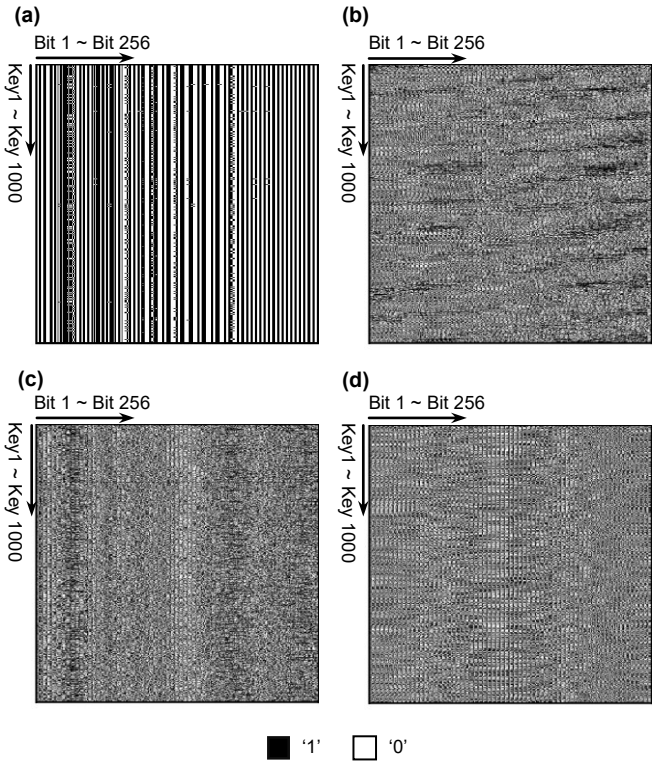


Fig. 5. Binary bitmap obtained with (a) the traditional wireless interrogation method, and (b)–(d) the standard, third-order, and sixth-order *PT*-symmetric interrogation methods; here, only 1000 PUF keys are shown for saving the space.

There are different phases in *PT* systems divided by EPs, given by

$$\gamma_{\text{EP}\pm}^{(2)}=\frac{1}{\kappa}\sqrt{\frac{1\pm\sqrt{1-\kappa^2}}{2}}. \tag{2}$$

When $\gamma\in[\gamma_{\text{EP}+}^{(2)},\infty]$, the two eigenfrequencies are real and, thus, the *PT*-symmetry is exact. When $\gamma\in[0,\gamma_{\text{EP}+}^{(2)}]$, the eigenfrequencies become complex conjugate pairs, signaling a transition to the broken phase. Considering a constant electromotive force at the initial moment (e.g., switching on the pulse generator), in the *PT*-symmetric phase, an oscillatory motion consisting of the superposition of multiple harmonics can be observed in the time domain [26], [30], while in the broken phase, the eigenmodes grow exponentially with time due to the imaginary part of eigenfrequency, resulting in underdamped or overdamped temporal dynamics. On the contrary, the phase transition at the EP is not observed in the conventional wireless interrogation system [Fig. 2(a)].

The eigenfrequencies of the third-order *PT*-symmetric electronic system comprising $-RLC$, LC, and RLC tanks (i.e., gain-neutral-loss) can be derived as [25], [26]:

$$\omega_n^{(3)}=\omega_0,\ \omega_0\sqrt{\frac{2\gamma^2-1\pm\sqrt{1-4\gamma^2+8\gamma^4\kappa^2}}{2\gamma^2(1-2\kappa^2)}}, \tag{3}$$

where the branching point EP is found at:

$$\gamma_{\mathrm{EP}\pm}^{(3)} = \frac{1}{2\kappa}\sqrt{1 \pm \sqrt{1-2\kappa^2}}. \quad (4)$$

Eq. (3) states that a divergent singularity also exists at the critical coupling strength $\kappa = 1/\sqrt{2}$, at which the eigenfrequency bifurcation effect at the EP ($\gamma_{\mathrm{EP}+}^{(3)} = 1/\sqrt{2}$) is elevated to a divergent form, so-called DEP, as shown in Fig. 2(c). We note that a DEP is impossible to be experimentally observed in the standard *PT* system since the emergence of a divergent point requires a perfect magnetic coupling (i.e., $\kappa = 1$).

In the generalized *N*th-order *PT*-symmetric electronic system ($N > 3$), an $-RLC$ oscillator and an RLC oscillator are remotely coupled via $N-2$ neutral repeater(s). By setting the coupling strength between two neutral repeaters as κ, and that between the gain (loss) oscillator and its neighboring repeater as $\kappa' = M'/L = \sqrt{2}\kappa$, the system's eigenfrequencies are found to be roots of a transcendental equation. If N is even, the system's eigenfrequencies are given by [25], [26], [28]:

$$\omega_n^{(N)} = \omega_0\sqrt{\frac{2\gamma^2 - 1 \pm \sqrt{1-4\gamma^2+16\gamma^4\kappa^2}}{2\gamma^2(1-4\kappa^2)}}, \frac{\omega_0}{\sqrt{1 \pm 2\kappa \mathrm{A}_{\alpha\beta}}}, \quad (5)$$

where

$$A_{\alpha\beta} = \sin\left(\frac{\pi}{2}\frac{2\beta+1}{2\alpha+1}\right), \quad (6)$$

$\alpha = (N-2)/2$, and $\beta = 0,1,2,\cdots,\alpha-1$; if N is odd, the system's eigenfrequencies are given by:

$$\omega_n^{(N)} = \omega_0, \omega_0\sqrt{\frac{2\gamma^2 - 1 \pm \sqrt{1-4\gamma^2+16\gamma^4\kappa^2}}{2\gamma^2(1-4\kappa^2)}}, \frac{\omega_0}{\sqrt{1 \pm 2\kappa \mathrm{B}_{\alpha\beta}}}, \quad (7)$$

where

$$B_{\alpha\beta} = \sin\left(\frac{\pi}{2}\frac{\beta+1}{\alpha+1}\right), \quad (8)$$

$\alpha = (N-3)/2$, and $\beta = 0,1,2,\cdots,\alpha-1$. From Eqs. (5) and (7), we observe that there are two eigenfrequencies undergoing the branching process and phase transition at the EP, given by:

$$\gamma_{\mathrm{EP}\pm}^{(N>3)} = \frac{1}{2\sqrt{2}\kappa}\sqrt{1 \pm \sqrt{1-4\kappa^2}}, \quad (9)$$

accompanied with discrete eigenfrequencies that are independent of γ. For both odd and even orders, the critical coupling that results in the divergent bifurcation effect occurs at $\kappa = 1/2$, and the exceptional point $\gamma_{\mathrm{EP}+}^{(N>3)} = 1/\sqrt{2}$. Fig. 2(d) presents the evolution of complex eigenfrequencies for the sixth-order *PT*-symmetric electronic system comprising an $-RLC$ and RLC tanks that are coupled via four LC repeaters. When the coupling strength is close to the critical value, the gigantic bifurcation effect can be obtained near the DEP. Importantly, this infers that even small variations in lumped element value or $\Delta\gamma$ caused by manufacturing process variations could result in significantly different sets of eigenfrequencies, and such high entropy may be beneficial for the PUF application. For instance, when the same reader and repeater(s) are employed to interrogate a group of RF-transponder tags, the device-to-device variations between tags may be amplified when measuring the system's temporal/spectral response near an EP or DEP. As illustrated in Fig. 1, the highly diversified analog output responses can be digitized to produce unique PUF-based secret keys for cryptographic operations.

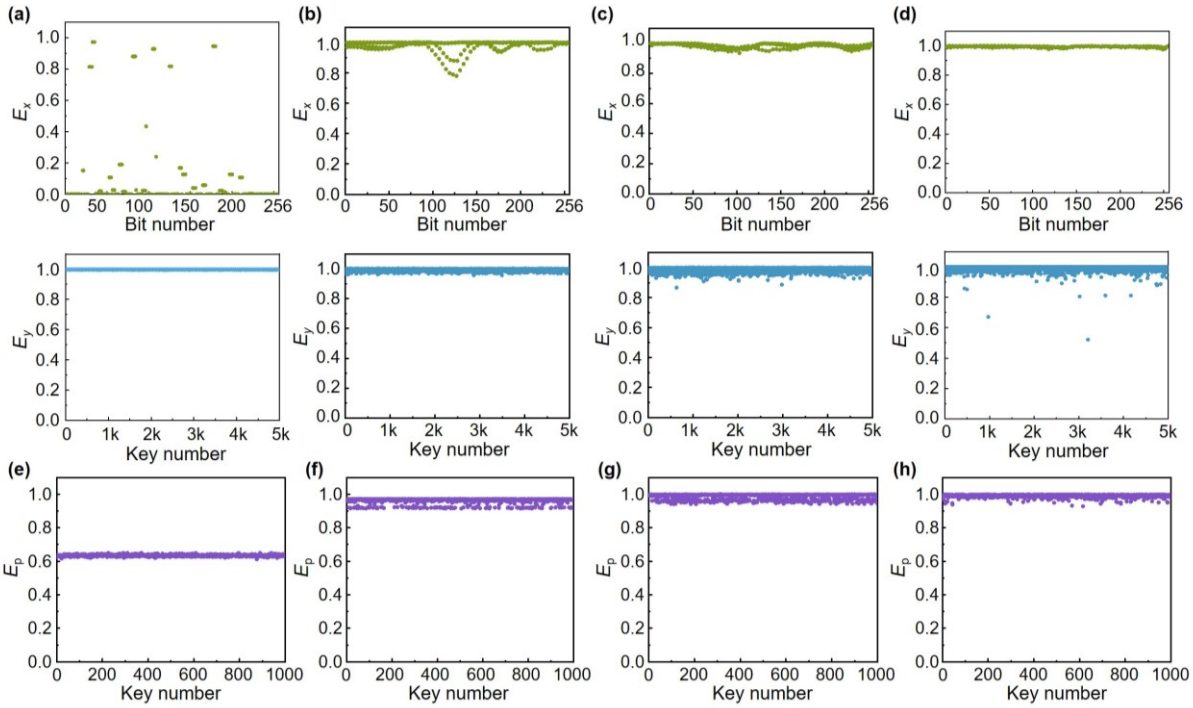
B. PUFs Based on EP- and DEP-Related Singularities

Electronic components generally have $\pm 0.1-5\%$ variations in lumped-element values due to fabrication errors, such as variations in the resistive layer thickness during the metal deposition or misalignment between capacitor metal layers [31]. In our statistical study and simulations, we assume that resistance and capacitance values are described by a Gaussian distribution:

$$P(x) = \frac{1}{\sqrt{2\pi}\sigma}e^{\frac{-(x-\mu)}{2\sigma^2}}, \quad (10)$$

where μ is the mean value of the components and σ is the standard deviation introduced by the fabrication errors; throughout this study, we assume $\sigma = 0.01$. Figs. 3(a)-(d) present the real-part eigenspectrum under the influence of process variations for the conventional short-range wireless connectivity (i.e., an RF tag described by an equivalent *RLC* circuit is interrogated by a coil antenna with self-inductance *L*), and the standard, third-order, and sixth-order *PT*-symmetric electronic systems, respectively; here, $\kappa = 0.99\times(1/\sqrt{2})$ for traditional, standard and third-order *PT* systems, and $0.99\times(1/2)$ for the sixth-order *PT* system; we note that a DEP appears at $\kappa = 1/\sqrt{2}$ and $1/2$ in the third-order and sixth-order *PT* system, respectively. As can be seen in Figs. 3(c) and 3(d), the probability of repeatedly observing eigenfrequencies is very low around the DEP (dark areas), which infers that RF output responses could be highly random. Such high uncertainty is also similarly obtained around the EP, as shown in Fig. 3(b), but with a higher probability of detection (i.e., lower entropy). On the other hand, in the exact symmetry phase, when the operating point is far from the DEP (bright region), there is a high probability of experimentally measuring the same eigenfrequencies. This phenomenon is also found in the traditional wireless interrogation setup that lacks EP or DEP in the eigenspectrum, as shown in Fig. 3(a).

Fig. 1(a) illustrates the proposed RF PUF system that is compatible with the current NFC and RFIC privacy-aware architectures. Passive tags are equivalent to a series RLC circuit and are interrogated by a reader via inductive coupling. In the *PT*-symmetric PUF system, an active $-RLC$ reader and



Figs. 6. (a)–(d) are the corresponding entropies E_x, E_y, and E_p of the bitmap in Figs. 5(a)–(d). The PUF keys obtained with the traditional interrogation method have a biased distribution of 0s and 1s, resulting in low randomness. Randomness can be improved substantially by the *PT*-symmetric interrogation method, particularly when the third- (or higher-) order setup is adopted. Comparing (c) and (d), one may observe that the maximum randomness brought by the singularity is rather independent of the orders of *PT* circuit (i.e., number of repeaters), but relies on the presence of DEP.

$N-2$ LC repeaters (if the higher-order setup is used), together with the passive RLC tag fulfill the *PT*-symmetry condition. The PUF key extraction is detailed below. First, the reader launches a pulse signal as the "input challenge" to activate the tag, and the temporal waveforms recorded on the capacitor in the reader's $-RLC$ tank can be regarded as the "output response." Throughout this study, the output responses are recorded for the period between T_0 and $4T_0$, where $T_0 = 1/f_0 = 2\pi\sqrt{LC}$. $T_0 \approx 156$ ns which is yielded by $|-R| = R = 50\ \Omega$, $L = 1000$ nH, and $C = 615$ pF. Such lumped element values give $\gamma \simeq 0.806$. To conduct a meaningful statistical study, 5000 RF tags were randomly generated, with their lumped element value variations described by Eq. (10) (where μ is equal to the mean values of desired R and C, and $\sigma = 0.01$), and their temporal responses under the pulse excitation were simulated using the Advanced Design System (ADS). For example, Fig. 4 shows the normalized temporal responses of 15 tags (out of 5000), which are interrogated by the same reader designed to implement the third-order *PT*-symmetric electronic system (here $\kappa = 0.99\times(1/\sqrt{2})$). Due to the EP and DEP singularities, output time responses can vary greatly even under small process variations, thanks to the high entropy and uncertainty observed in Fig. 3. Therefore, the hardly repeatable temporal responses can then be exploited to generate cryptographic keys through a proper analog-to-digital conversion (ADC) circuit. The temporal response is first normalized to lie within 0 to 1, as shown in Fig. 4. Then, the normalized analog waveform is partitioned into 64 equidistant data points in the time domain, and each data point is digitized to covert the floating number to a 4-bit binary code, with a possible binary value between 0000 and 1111 [28]. If the normalized value of a data point is below the threshold of 0.0625, it will be automatically assigned a binary value of 0000. Finally, a 256-bit CRP sequence can be generated as an encrypted digital fingerprint, as illustrated in Fig. 1(a). Figs. 5(a)–(d) show the binary bitmaps of 1000 out of 5000 RF tags (i.e., PUF instances) interrogated using the conventional, standard *PT*, third-order *PT*, and sixth-order *PT* wireless interrogation schemes, respectively; the systems' corresponding real eigenspectrums can be seen in Fig. 3. As seen in Fig. 5(a), PUF keys acquired by the traditional wireless reader are poorly differentiated. In contrast, as seen in Fig. 5(b), the PUF keys acquired by the standard *PT* readout circuit with an EP can have good differentiation and uniqueness. Moreover, as seen in Figs. 5(c) and 5(d), PUF keys generated using a higher-order *PT* readout circuit with a DEP exhibit higher uniqueness and unpredictability than the previous two cases. As can be seen in Figs. 5(c) and 5(d), the bitmap contains almost equal numbers of 0's and 1's, indicating that the proposed DEP-based PUF key is not predictable and tamper-resistant. In principle, under the same input challenge, CRPs generated by different PUF instances should be totally random and uniquely different. In the next section, the performance metrics of PUFs, including randomness, uniqueness, and encoding capacity will be fully characterized.

III. Results and Discussions

A. Characterization of Uniformity and Randomness

Uniformity that measures the probability of finding 1s or 0s in the response bit sequence is an important indicator for

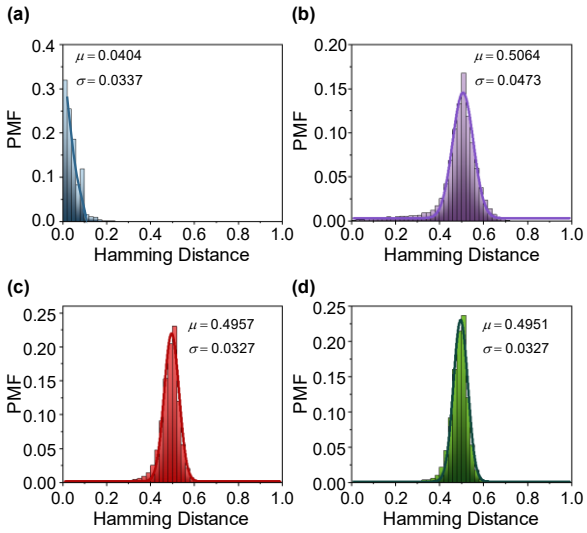


Fig. 7. Histogram of the uniqueness in terms of inter-HDs, which are obtained with (a) the traditional wireless interrogation method and (b)–(d) the standard, third-order, and sixth-order *PT*-symmetric interrogation methods; here, PMF is plotted as a function of inter-HD. The idea mean value (μ) and standard deviations (σ) are: $\mu = 0.5$ and $\sigma = 0$.

evaluating the randomness of PUF keys. Ideally, the uniformity should be 50%, ensuring an equal probability of finding 1s and 0s. The uniformity can be insightfully measured by the Shannon entropy (E_x, E_y):

$$E_x = -[p_x \log_2 p_x + (1-p_x)\log_2(1-p_x)],$$
$$E_y = -[p_y \log_2 p_y + (1-p_y)\log_2(1-p_y)], \quad (11)$$

where p_x and p_y are probabilities of observing "1" along the x- and y-axes of the bitmap, respectively. For a truly random bitmap, the ideal value for E_x and E_y is 1. Figs. 6(a)–(b) report distributions of E_x (top panel) and E_y (middle panel) of the bitmaps in Fig. 5, which correspond to the traditional RF, standard *PT* (EP-based), third-order *PT* (DEP-based), and sixth-order *PT* (DEP-based) PUF systems, respectively. As seen in Fig. 6(a), since the traditional setup has a biased distribution of 0s and 1s [Fig. 5(a)], it gives poor unpredictability and low randomness, with average entropy $(\bar{E}_x, \bar{E}_y) \approx (0.093, 0.997)$. When the readout scheme based on the standard *PT* system is used, due to the EP singularity that enhances the bit uniformity [Fig. 6(b)], the average entropy is improved to $(\bar{E}_x, \bar{E}_y) = (0.981, 0.996)$. The third-order *PT* PUF system with a DEP can further ameliorate the uniformity [Fig. 6(c)], resulting in $(\bar{E}_x, \bar{E}_y) = (0.984, 0.990)$. The sixth-order *PT* PUF system with a DEP and four γ- insensitive eigenfrequencies exhibits good uniformity, with $(\bar{E}_x, \bar{E}_y) = (0.995, 0.991)$ [Fig. 6(d)]; such values are comparable to those of its third-order counterpart. We also evaluated the Shannon entropy for the fourth-, fifth-, and tenth-order *PT* PUF systems, whose entropy values are $(\bar{E}_x, \bar{E}_y) = (0.998, 0.998)$, $(\bar{E}_x, \bar{E}_y) = (0.984, 0.983)$, and $(\bar{E}_x, \bar{E}_y) = (0.986, 0.994)$, respectively; the associated entropy diagrams are not shown here for saving some space. The optimum bit uniformity is attained in the higher-order *PT* systems with DEP singularity.

Permutation entropy is commonly used for analyzing the

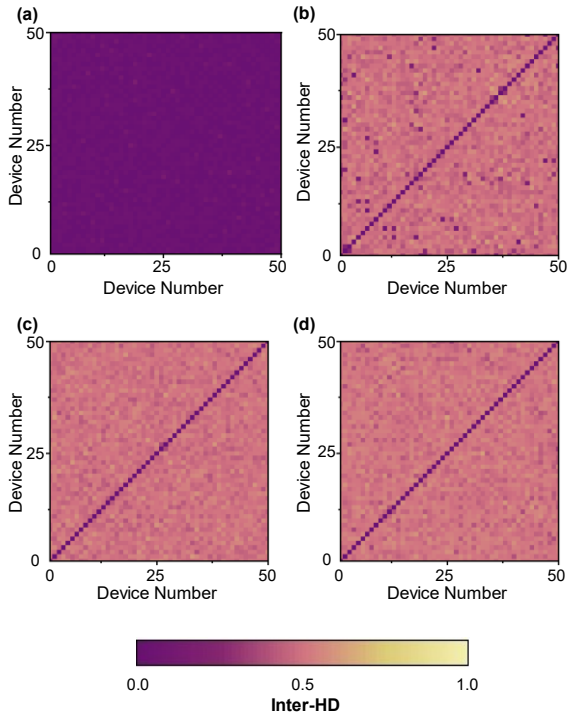


Fig. 8. Pairwise evaluation of PUF keys generated using (a) the traditional wireless interrogation method, and (b)–(d) the standard, third-order, and sixth-order *PT*-symmetric interrogation methods.

complexity of time series encoded in sequential or permutation patterns [32]. The permutation entropy is defined as:

$$H = E_p = -\sum_{j=1}^{n!} p_j \log(p_j), \quad (12)$$

where n is the order chosen to be computed (which is typically greater than 2) and p_j is the frequency of the permutation pattern normalized by the total number of subsequences [32], [33]. Here, we chose 1000 out of 5000 normalized temporal responses and $n = 3$ to compute the permutation entropy. The bottom panels of Figs. 6(a)–(d) report distributions of E_p for the bitmaps in Fig. 5, which correspond to PUF systems based on typical short-range interrogation, standard *PT*, third-order *PT*, and sixth-order *PT* structures. Again, the PUF keys obtained with the traditional interrogation system show moderately low randomness with $\bar{E}_p = 0.635$. Permutation entropy can be enhanced due to the presence of EP and DEP, with $\bar{E}_p = 0.961$ for the standard *PT* system and $\bar{E}_p = 0.985$ for the third-order *PT* system. When the order of the *PT* system $N > 3$, further increasing the order or the number of repeaters has little effect on the permutation entropy. The calculated permutation entropy values for the fourth-, fifth-, sixth-, and tenth-order *PT* PUF systems are $\bar{E}_p = 0.998,\ 0.986,\ 0.990$ and 0.988, respectively. According to the above analysis of Shannon and permutation entropy, it is clearly evident that the optimum bit uniformity obtained with the higher-order *PT* PUF systems can be attributed mainly to the existence of DEP, rather than increasing the order of *PT* system. In fact, when the order of the *PT* circuit $N > 3$, the improvement of E_x, E_y and E_p is nearly imperceptible.

TABLE I
P-VALUES OF PUF KEYS GENERATED USING TRADITIONAL, STANDARD-*PT*, THIRD-ORDER *PT*, AND SIXTH-ORDER *PT* READOUT METHODS.

NIST randomness indicator	Traditional RF PUF		Standard *PT* PUF		Third-order *PT* PUF		Sixth-order *PT* PUF	
	P-values	Pass?	P-values	Pass?	P-values	Pass?	P-values	Pass?
Frequency	0.6171	Yes	0.9303	Yes	0.7737	Yes	0.9701	Yes
FB	0	No	0.5001	Yes	0.4324	Yes	0.5276	Yes
Runs	0	No	0.3826	Yes	0.2897	Yes	0.3829	Yes
LOR	0.1095	Yes	0.1312	Yes	0.1007	Yes	0.1063	Yes
FFT	0.9213	Yes	0.9553	Yes	0.9857	Yes	0.9727	Yes
NOT(m=5)	0.9895	Yes	0.9879	Yes	0.9915	Yes	0.9917	Yes
Serial(m=4)	0	No	0.7133	Yes	0.5116	Yes	0.5225	Yes
AppEn(m=3)	0	No	0.5754	Yes	0.3349	Yes	0.3242	Yes
Cum. Sum.	0	No	0.5084	Yes	0.4427	Yes	0.5292	Yes

While entropy is an effective means of determining randomness, it may not be used to conclusively verify the stochastic properties of the system. Here, we also exploit the National Institute of Standards and Technology (NIST) randomness tests suite [34] to verify the randomness of binary bit sequences generated by the proposed PUFs. The NIST test suite is a statistical package consisting of 15 tests to examine various aspects of randomness in a binary sequence. Table I compares the NIST randomness test results among PUF keys generated by the conventional, standard *PT* (EP-based), and higher-order *PT* (DEP-based) interrogation methods. If the P-values of all NIST tests exceed a threshold of 0.01 [34], the PUF can be classified as a true random number generator (TRNG). From Table I, it is evident that both standard and higher-order *PT* PUFs are qualified as legitimate TRNGs that generate random and unique signatures.

B. Characterization of Uniqueness

Uniqueness represented by the inter-device Hamming distance (inter-HD) measures how each PUF device is uniquely different from another. The ideal average inter-HD is 50%; that is, half of the bits are the same, and the other half are different. The inter-HD can be expressed as:

$$\mathrm{U}=\overline{\mathrm{HD}_{\mathrm{inter}}}=\frac{2}{N(N-1)}\sum_{i=1}^{N-1}\sum_{j=i+1}^{N}\frac{\sum_{l=1}^{L}(K_{i,l}\oplus K_{j,l})}{L}, \qquad (13)$$

where $N=5000$ denotes the number of CRPs, $L=256$ is the length of digitized bitstrings converted from the analog transient response. K_i represents the ith cryptographic key, and $\oplus$ stands for the XOR logic operation. Figs. 7(a)–(b) plot the probability mass function (PMF) as a function of the inter-HDs obtained respectively by the conventional, standard *PT*, third-order *PT*, and sixth-order *PT* readout methods. As seen in Fig. 7(a), the mean inter-HD (μ) and standard deviation (σ) of PUF keys obtained using the conventional readout circuit are 0.0404 and 0.0337, respectively. Such a result indicates that when intrinsic device variation due to fabrication imperfections is small, and, therefore, uniqueness of PUFs sourced from the RF signal fluctuation is low. On the contrary, when a standard *PT* circuit is used to interrogate the tags in contactless ways, as seen in Fig. 7(b), the enhancement of entropy near an EP leads to a sharp Gaussian distribution centered at $\mu=0.5064$, with standard deviation $\sigma=0.0473$. Such a result is close to the ideal values of $\mu=0.5$ and $\sigma=0$. Moreover, the higher-order *PT* circuits can further improve uniqueness by operating near the DEP, as shown in Figs. 7(c) and (d). For the third-order *PT* PUF, a Gaussian fitting is centered at $\mu=0.4957$, with the standard deviations $\sigma=0.0327$, which is smaller than that of the standard *PT* PUF. Although the sixth-order *PT* PUF may have an elongated interrogation distance by using multiple repeaters, its performance ($\mu=0.4951$ and $\sigma=0.0327$) is almost the same as that of its third-order counterpart.

Uniqueness can also be characterized by the uncorrelation between two encrypted keys, which can be visualized by the pairwise comparison map of inter-HD, as shown in Fig. 8 (here, the data is extrapolated from Fig. 4 and 50 CRPs are randomly selected). In the pairwise comparison map, the diagonal line represents the intra-HD values for the same PUF device itself (the ideal value is 0), whereas the off-diagonal points represent the inter-HD values compared with the other PUF instances (the ideal value is 0.5). It can be seen from Fig. 8 that for the higher-order *PT* circuits, the bit uniformity distribution is close to the ideal value of 0.5 at most off-diagonal points, implying that all 50 different PUFs are highly uncorrelated. It can be observed from Fig. 8 that the high-order *PT* readout circuit provides

TABLE II
SIMULATED ENCODING CAPACITY OF PUF KEYS

	Key size	Encoding capacity
Traditional RF PUF	34	1.71×10^{10}
Standard *PT* PUF	112	5.19×10^{33}
Third-order *PT* PUF	234	2.37×10^{70}
Sixth-order *PT* PUF	234	2.36×10^{70}

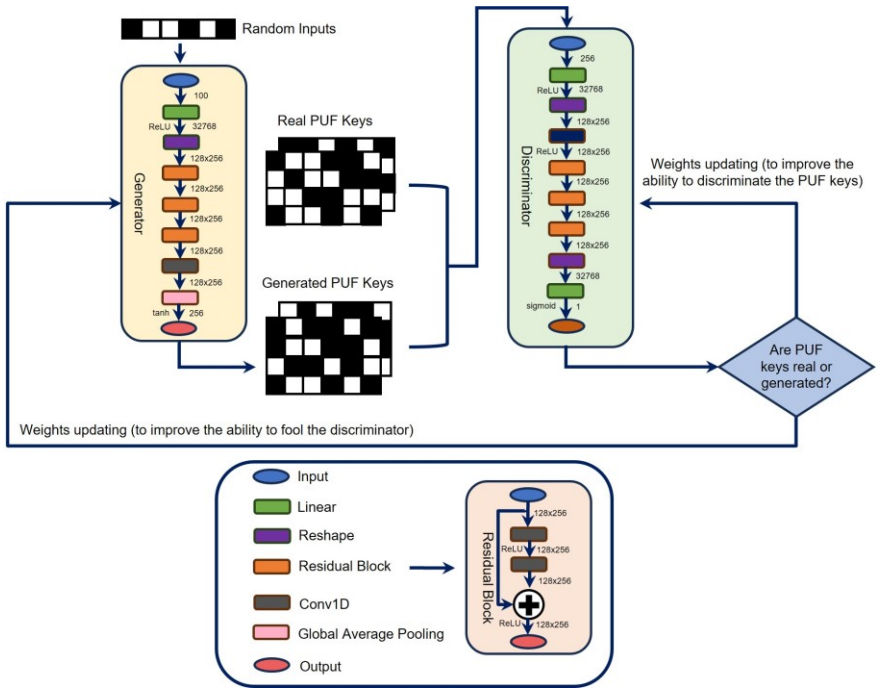


Fig. 9. Schematic of the GAN structure consisting of a generator and a discriminator; here, 5000 randomly generated PUF instances are first simulated to collect their CRPs, of which 4000 CRPs are used for training, while the rest are reserved for testing.

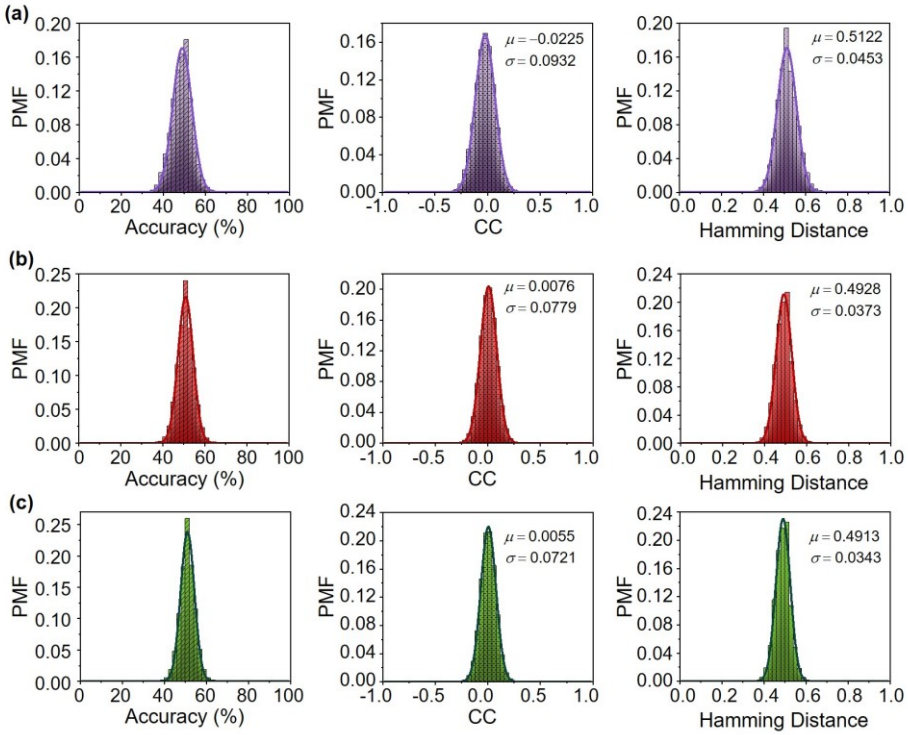


Fig. 10. Simulation results for the ML attack based on the passGAN algorithm. PMFs of the mean ACC, mean CC and mean n-HD for the (a) standard, (b) third-order, and (c) sixth-order *PT* PUFs are shown. The results demonstrate the resilience of higher-order *PT* PUFs against GAN-based attacks.

excellent uniqueness, significantly outperforming the traditional RF readout circuit [Fig. 8(a)].

C. Encryption Quality Evaluation

The encoding capacity denoted by the number of codes that a PUF instance can generate is an imperative metric, as high encoding capacity ensures that cryptographic keys are difficult to duplicate. For binary bit sequences generated by our PUF, the encoding capacity is defined as c^k, where $c = 2$ for binary bits of "0" and "1", the key size $k = \mu(1-\mu)/\sigma^2$, and μ, σ symbolize the mean probability and the standard deviation that can be found in Fig. 7 [35]. Table II summarizes the key size and encoding capacity of different PUF structures in Fig. 7. Apparently, the higher-order *PT* PUFs can have the highest encoding capacity among different designs, and a large

encoding capacity of $2^{234} \approx 2.37\times10^{70}$ can be achieved. Here, we also conducted numerical experiments for the fourth-, fifth-, and tenth-order *PT* PUF systems, which offer an encoding capacity of $2^{231} \approx 4.07\times10^{69}$, $2^{223} \approx 1.35\times10^{67}$, and $2^{244} \approx 3.11\times10^{73}$, respectively; their inter-HD histograms are not shown for brevity. Such results are similar to those obtained in third-order and sixth-order *PT* PUF systems [Table II]. Therefore, from the above randomness and uniqueness analysis, it can be concluded that increasing the number of repeaters in a high-order *PT* PUF system has no obvious advantage in improving encryption quality. In other words, the third-order *PT* PUF system may be the simplest structure that gives the optimum encryption performance.

D. Comparison with State-of-the-Art Methods

Here, we also compare the performance of the proposed PUF with other electromagnetics- and analog-based PUFs in terms of the randomness, uniqueness, complexity/compactness, and cost [36]–[40]. The results are shown in Table III. To the best of the authors' knowledge, the concept of electromagnetic PUF based on RF circuits or non-Hermitian physical systems with EPs has not yet been studied, especially for applications in identification, authentication, and secure wireless communications. As can be seen in Table III, the performance of the proposed RF PUF is better than that of analog/digital circuit-based PUFs, while being comparable to or even superior than those of optical and photonic PUFs. Nevertheless, the proposed systems are more compact and cost-effective when compared to their short-wavelength counterparts, i.e., optical PUF typically requires costly and bulky readout instruments such as optical table and optical microscopy, ultrafast laser [36], or Raman spectroscopy [37]. The proposed low-frequency electromagnetic PUF keys based on lumped components can be ultracompact, low-cost, and can be mass-produced using PCB or integrated circuit technologies. Furthermore, the reader/interrogator composed of an active tank and an analog-to-digital converter can be lightweight, low-cost, and portable, significantly facilitating the practice of electromagnetic PUF.

E. Resilience to Machine Learning (ML) Attacks

In recent years, the emergence of machine learning techniques has offered significant potential for aiding in the domains of image and speech recognition [41]–[43], natural language processing [44], recommendation systems [45], and inverse design within the field of electromagnetics [46]. Particularly noteworthy is its reported efficacy as a potent tool for perpetrating password-guessing attacks and decrypting sensitive information. As per findings from prior works [13], [14], despite some certain conventional PUFs demonstrating commendable attributes regarding randomness and uniqueness, they exhibit vulnerability to attacks leveraging machine and deep learning models, such as generative adversarial networks (GANs) [47].

In this section, we investigate the susceptibility of the proposed *PT* PUFs to the modeling attack employing the PassGAN model. The PassGAN model emerges as a formidable tool for password-guessing endeavors. It contains two parts: a generator network and a discriminator network. The overall architecture of the model is presented in Fig. 9. In detail, the generator network creates fake PUF instances grounded on random inputs. The produced PUF keys are then mixed with real PUF to test the discriminator network. The objective of the generator network is to produce fake PUF keys that are indistinguishable from the real ones. In contrast, the discriminator network has a competing aim to identify if the supplied PUF instances are real or fake. In this work, we generate 5000 simulated CRPs. 1000 of them are designated for testing purposes and the remainder reserved for training the passGAN model. The evaluations of the resilience against attacks based on passGAN model for the standard, third- and sixth-order PUF relied on the utilization of accuracy (ACC), correlation coefficients (CC), and Hamming distance (HD). These metrics evaluate the linear correlation level between two random sequences and the dissimilarity between the predicted and simulated CRPs. For a generated 256-length CRP $\tilde{y}_i$ and a test 256-length y_i, the ACC, CC, and HD are formalized below:

TABLE III
SUMMARY OF PERFORMANCE METRICS BETWEEN DIFFERENT PUFS.

Reference	Technique	Cost & complexity	Uniqueness (inter-HD)	Encoding capacity	NIST randomness test	ML attacks reported
[36]	Silicon photonics	High	μ=0.5	N/A	Not reported	No
[37]	Raman scattering	High	Not reported	3×10^{15051}	Not reported	No
[38]	Optical imaging	Medium	μ=0.4937 σ=0.0556	2.19×10^{24}	Pass	No
[39]	Analog circuit	Low	Not reported	N/A	73.23%	Yes/Not Pass
[40]	Analog circuit	Low	μ=0.492 σ=0.06	7.93×10^{20}	Pass	No
This work	RF circuit	Low	μ=0.4957 σ=0.0327	2.37×10^{70}	Pass	Yes/Pass

$$\begin{aligned} \mathrm{ACC} &= \frac{\#(\tilde{y}_i = y_i)}{256}, \text{ where } i = 1,2,3,\ldots,256, \\ \mathrm{CC} &= \frac{1}{255}\sum_{i=1}^{256}\left(\frac{\tilde{y}_i - \mu_{\tilde{y}}}{\sigma_{\tilde{y}}}\right)\left(\frac{y_i - \mu_y}{\sigma_y}\right), \\ \mathrm{HD} &= \sum_{i=1}^{256}(y_i \oplus \tilde{y}_i), \end{aligned} \tag{14}$$

where $\#(\cdot)$ counts the number of bits fulfilling the specified condition, $\mu_{\tilde{y}}$ (μ_y) and $\sigma_{\tilde{y}}$ (σ_y) denote the mean and the variance of $\tilde{y}$ (y), and $\oplus$ represents the XOR logic operation. The ACC, CC, and HD of the unpredictable CRPs are expected to be close to 50%, 0, and 0.5, respectively. Fig. 10 presents distributions of the ACC, CC, and normalized HD (n-HD) between the GAN-predicted and simulated CRPs for the standard and higher-order *PT* PUFs. To accommodate a large number of sampled CRPs, the PMF is employed. The ACC exhibits a distributed pattern centered around 50% for both standard and higher-order *PT* PUFs. The distributions of ACC, CC, and n-HD are narrower for the third-order and sixth-order *PT* PUFs when compared to standard *PT* PUFs, indicating improved resilience against passGAN-based modeling attacks. The means and standard deviations of CC and HD for PUFs are presented in Table IV. This provides additional evidence in support of the resilience of the proposed higher-order *PT* PUF against machine learning-assisted modeling attacks. The means (μ) and standard deviations (σ) of CC and HD for all conditions are summarized in Table IV, showing that the third-order and sixth-order *PT* PUFs exhibit similar performance and are resilient to ML-based modeling attacks.

TABLE IV
MEANS AND STANDARD DEVIATIONS OF CC AND HD OF PUF KEYS

	CC		HD	
	Mean (μ)	Standard deviation (σ)	Mean (μ)	Standard deviation (σ)
Standard *PT* PUF	-0.0225	0.0932	0.5122	0.0453
Third-order *PT* PUF	0.0076	0.0779	0.4928	0.0373
Sixth-order *PT* PUF	0.0055	0.0721	0.4913	0.0343

IV. CONCLUSION

We have presented the concept and design of a lightweight and secure PUF-based identification and authentication scheme based on sample-specific electromagnetic signatures of RF-transponder tags. We have demonstrated with the *PT*-symmetric circuities that high entropy and signal ambiguity/ uncertainty near the EP and DEP, although detrimental to sensing applications, may be leveraged to produce high-quality PUF encryption keys. We have thoroughly characterized the performance metrics of different PUF-key generation (wireless interrogation) structures, including the traditional wireless readout system and the standard and higher-order (third- and higher-order) *PT*-symmetric readout systems. Our results show that the higher-order *PT* PUF can withstand all scrutiny in terms of randomness, uniqueness, pairwise correlation, and encoding capacity, thanks to the ultrahigh entropy near the DEP singularity. Although the standard *PT* PUF enhanced by an EP exhibits degraded performance metrics compared to higher-order *PT* PUFs, it can still outperform the traditional RF PUF. Moreover, we have found that all higher-order *PT* readout setups show comparable PUF metrics since high entropy mainly stems from the divergent bifurcation effect near the DEP, regardless of the number of repeaters. Therefore, considering the implementation complexity and cost, the third-order *PT* PUF would be preferable. Additionally, we have demonstrated that the proposed PUF can be robust against advanced ML-based modeling attacks and does not require anti-tamper mechanisms to detect invasive attacks. Such results reinforce the potential and applicability of the proposed PUF as a highly-versatile anti-counterfeiting solution, which is in strong demand in many fields, such as radio-frequency identification, wireless access control, authentication of NFC and IoT, and anti-counterfeiting/anti-fraud labels.

Although in this proof-of-concept demonstration, the non-Hermitian open system with an EP/DEP was built upon electronic circuits, this work can be generalized, transformative, and readily extended to other non-Hermitian electromagnetic structures exhibiting exceptional points and branch singularities, such as metamaterials [48], [49] metasurfaces [50]–[52], frequency-selective surfaces, and waveguide/transmission-line networks [21], [53]–[55]. We should also point out that there are other singular electromagnetic behaviors, such as electromagnetically-induced transparency (EIT) [56], Fano resonance [57], and bound states in the continuum (BIC) [58], as well as sensitive topological dynamics, which may be exploited to realize electromagnetic unclonablity, with encryption keys stored in the structure's propagation, scattering, and/or radiation characteristics. Therefore, our discovery of the electromagnetically unclonable functions may light up a new spark in hardware security and cryptographic technologies.

REFERENCES

[1] G. Hancke, B. Silva, and G. Hancke, Jr., "The Role of Advanced Sensing in Smart Cities," *Sensors*, vol. 13, no. 1, pp. 393–425, Dec. 2012.

[2] I. Rosenberg, A. Shabtai, Y. Elovici, and L. Rokach, "Adversarial Machine Learning Attacks and Defense Methods in the Cyber Security Domain," *ACM Comput. Surv.*, vol. 54, no. 5, pp. 1–36, Jun. 2022.

[3] D. Dobrykh, D. Filonov, A. Slobozhanyuk, and P. Ginzburg, "Hardware RFID Security for Preventing Far-Field Attacks," *IEEE Trans. Antennas Propag.*, vol. 70, no. 3, pp. 2199–2204, Mar. 2022.

[4] N. Miloslavskaya and A. Tolstoy, "Internet of Things: information security challenges and solutions," *Clust. Comput.*, vol. 22, no. 1, pp. 103–119, Mar. 2019.

[5] B. Hitaj, P. Gasti, G. Ateniese, and F. Perez-Cruz, "PassGAN: A Deep Learning Approach for Password Guessing," in *Applied Cryptography and Network Security*, vol. 11464, R. H. Deng, V. Gauthier-Umaña, M. Ochoa, and M. Yung, Eds., in Lecture Notes in Computer Science, vol. 11464. , Cham: Springer International Publishing, 2019, pp. 217–237.

[6] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[7] 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.

[8] Y. Shifman, A. Miller, O. Keren, Y. Weizmann, and J. Shor, "A Method to Improve Reliability in a 65-nm SRAM PUF Array," *IEEE Solid-State Circuits Lett.*, vol. 1, no. 6, pp. 138–141, Jun. 2018.

[9] "Static Physically Unclonable Functions for Secure Chip Identification With 1.9–5.8% Native Bit Instability at 0.6–1 V and 15 fJ/bit in 65 nm," *IEEE J. Solid-State Circuits*, vol. 51, no. 3, pp. 763–775, Mar. 2016.

[10] M. Vatalaro, R. De Rose, M. Lanuzza, and F. Crupi, "Static CMOS Physically Unclonable Function Based on 4T Voltage Divider With 0.6%–1.5% Bit Instability at 0.4–1.8 V Operation in 180 nm," *IEEE J. Solid-State Circuits*, vol. 57, no. 8, pp. 2509–2520, Aug. 2022.

[11] B. H. Calhoun *et al.*, "Digital Circuit Design Challenges and Opportunities in the Era of Nanoscale CMOS," *Proc. IEEE*, vol. 96, no. 2, pp. 343–365, Feb. 2008.

[12] J. Tang *et al.*, "Flexible CMOS integrated circuits based on carbon nanotubes with sub-10 ns stage delays," *Nat. Electron.*, vol. 1, no. 3, pp. 191–196, Mar. 2018.

[13] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proceedings of the 17th ACM conference on Computer and communications security*, Chicago Illinois USA: ACM, Oct. 2010, pp. 237–249.

[14] A. Dodda, S. Subbulakshmi 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, May 2021.

[15] C. E. Rüter, K. G. Makris, R. El-Ganainy, D. N. Christodoulides, M. Segev, and D. Kip, "Observation of parity–time symmetry in optics," *Nat. Phys.*, vol. 6, no. 3, pp. 192–195, Mar. 2010.

[16] 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, p. 040101, Oct. 2011.

[17] R. Fleury, D. Sounas, and A. Alù, "An invisible acoustic sensor based on parity-time symmetry," *Nat. Commun.*, vol. 6, no. 1, p. 5905, Jan. 2015.

[18] Y. Ra'di, D. L. Sounas, A. Alù, and S. A. Tretyakov, "Parity-time-symmetric teleportation," *Phys. Rev. B*, vol. 93, no. 23, p. 235427, Jun. 2016.

[19] M. A. K. Othman and F. Capolino, "Theory of Exceptional Points of Degeneracy in Uniform Coupled Waveguides and Balance of Gain and Loss," *IEEE Trans. Antennas Propag.*, vol. 65, no. 10, pp. 5289–5302, Oct. 2017.

[20] M. Sakhdari, M. Hajizadegan, Y. Li, M. M.-C. Cheng, J. C. H. Hung, and P.-Y. Chen, "Ultrasensitive, Parity–Time-Symmetric Wireless Reactive and Resistive Sensors," *IEEE Sens. J.*, vol. 18, no. 23, pp. 9548–9555, Dec. 2018.

[21] A. F. Abdelshafy, M. A. K. Othman, D. Oshmarin, A. T. Almutawa, and F. Capolino, "Exceptional Points of Degeneracy in Periodic Coupled Waveguides and the Interplay of Gain and Radiation Loss: Theoretical and Experimental Demonstration," *IEEE Trans. Antennas Propag.*, vol. 67, no. 11, pp. 6909–6923, Nov. 2019.

[22] P.-Y. Chen and R. El-Ganainy, "Exceptional points enhance wireless readout," *Nat. Electron.*, vol. 2, no. 8, pp. 323–324, Aug. 2019.

[23] P.-Y. Chen *et al.*, "Generalized parity–time symmetry condition for enhanced sensor telemetry," *Nat. Electron.*, vol. 1, no. 5, pp. 297–304, May 2018.

[24] M. Hajizadegan, M. Sakhdari, S. Liao, and P.-Y. Chen, "High-Sensitivity Wireless Displacement Sensing Enabled by PT-Symmetric Telemetry," *IEEE Trans. Antennas Propag.*, vol. 67, no. 5, pp. 3445–3449, May 2019.

[25] 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, p. 193901, Nov. 2019.

[26] 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, p. 013152, Feb. 2020.

[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, Feb. 2023.

[28] 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.

[29] M. Yang, Z. Ye, H. Pan, M. Farhat, A. E. Cetin, and P.-Y. Chen, "Electromagnetically unclonable functions generated by non-Hermitian absorber-emitter," *Sci. Adv.*, vol. 9, no. 36, p. eadg7481, Sep. 2023.

[30] J. Schindler, Z. Lin, J. M. Lee, H. Ramezani, F. M. Ellis, and T. Kottos, "$\mathcal{PT}$-symmetric electronics," *J. Phys. Math. Theor.*, vol. 45, no. 44, p. 444029, Nov. 2012.

[31] Xuan Zhang, Bojiong Ni, I. Mukhopadhyay, and A. B. Apsel, "Improving Absolute Accuracy of Integrated Resistors With Device Diversification," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 59, no. 6, pp. 346–350, Jun. 2012.

[32] C. Bandt and B. Pompe, "Permutation Entropy: A Natural Complexity Measure for Time Series," *Phys. Rev. Lett.*, vol. 88, no. 17, p. 174102, Apr. 2002.

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

[34] A. Rukhin *et al.*, *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, vol. 22. US Department of Commerce, Technology Administration, National Institute of …, 2001.

[35] Z. Hu *et al.*, "Physically unclonable cryptographic primitives using self-assembled carbon nanotubes," *Nat. Nanotechnol.*, vol. 11, no. 6, pp. 559–565, Jun. 2016.

[36] B. C. Grubel *et al.*, "Silicon photonic physical unclonable function," *Opt. Express*, vol. 25, no. 11, p. 12710, May 2017.

[37] Y. Gu, C. He, Y. Zhang, L. Lin, B. D. Thackray, and J. Ye, "Gap-enhanced Raman tags for physically unclonable anticounterfeiting labels," *Nat. Commun.*, vol. 11, no. 1, p. 516, Jan. 2020.

[38] 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.

[39] L. Liu, H. Huang, and S. Hu, "Lorenz Chaotic System-Based Carbon Nanotube Physical Unclonable Functions," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 37, no. 7, pp. 1408–1421, Jul. 2018.

[40] S. Lee, M.-K. Oh, Y. Kang, and D. Choi, "Design of Resistor-Capacitor Physically Unclonable Function for Resource-Constrained IoT Devices," *Sensors*, vol. 20, no. 2, p. 404, Jan. 2020.

[41] L. Deng and X. Li, "Machine Learning Paradigms for Speech Recognition: An Overview," *IEEE Trans. Audio Speech Lang. Process.*, vol. 21, no. 5, pp. 1060–1089, May 2013.

[42] H. Pan, D. Badawi, and A. E. Cetin, "Computationally Efficient Wildfire Detection Method Using a Deep Convolutional Network Pruned via Fourier Analysis," *Sensors*, vol. 20, no. 10, p. 2891, May 2020.

[43] H. Pan, X. Zhu, S. Atici, and A. E. Cetin, "A Hybrid Quantum-Classical Approach based on the Hadamard Transform for the Convolutional Layer," 2023.

[44] A. Le Glaz *et al.*, "Machine Learning and Natural Language Processing in Mental Health: Systematic Review," *J. Med. Internet Res.*, vol. 23, no. 5, p. e15708, May 2021.

[45] I. Portugal, P. Alencar, and D. Cowan, "The use of machine learning algorithms in recommender systems: A systematic review," *Expert Syst. Appl.*, vol. 97, pp. 205–227, May 2018.

[46] M. Li *et al.*, "Machine Learning in Electromagnetics With Applications to Biomedical Imaging: A Review," *IEEE Antennas Propag. Mag.*, vol. 63, no. 3, pp. 39–51, Jun. 2021.

[47] J. Delvaux, "Machine-Learning Attacks on PolyPUFs, OB-PUFs, RPUFs, LHS-PUFs, and PUF–FSMs," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 8, pp. 2043–2058, Aug. 2019.

[48] G. Castaldi, S. Savoia, V. Galdi, A. Alù, and N. Engheta, "P T Metamaterials via Complex-Coordinate Transformation Optics," *Phys. Rev. Lett.*, vol. 110, no. 17, p. 173901, Apr. 2013.

[49] S. Savoia, G. Castaldi, V. Galdi, A. Alù, and N. Engheta, "PT -symmetry-induced wave confinement and guiding in ε -near-zero metamaterials," *Phys. Rev. B*, vol. 91, no. 11, p. 115114, Mar. 2015.

[50] R. Fleury, D. L. Sounas, and A. Alù, "Negative Refraction and Planar Focusing Based on Parity-Time Symmetric Metasurfaces," *Phys. Rev. Lett.*, vol. 113, no. 2, p. 023903, Jul. 2014.

[51] P.-Y. Chen and J. Jung, "P T Symmetry and Singularity-Enhanced Sensing Based on Photoexcited Graphene Metasurfaces," *Phys. Rev. Appl.*, vol. 5, no. 6, p. 064018, Jun. 2016.

[52] M. Sakhdari, M. Farhat, and P.-Y. Chen, "PT-symmetric metasurfaces: wave manipulation and sensing using singular points," *New J. Phys.*, vol. 19, no. 6, p. 065002, Jun. 2017.

[53] G. W. Hanson, A. B. Yakovlev, M. A. K. Othman, and F. Capolino, "Exceptional Points of Degeneracy and Branch Points for Coupled Transmission Lines—Linear-Algebra and Bifurcation Theory Perspectives," *IEEE Trans. Antennas Propag.*, vol. 67, no. 2, pp. 1025–1034, Feb. 2019.

[54] K. Rouhi, H. Kazemi, A. Figotin, and F. Capolino, "Exceptional Points of Degeneracy Directly Induced by Space–Time Modulation of a Single Transmission Line," *IEEE Antennas Wirel. Propag. Lett.*, vol. 19, no. 11, pp. 1906–1910, Nov. 2020.

[55] M. Yang, Z. Ye, M. Farhat, and P.-Y. Chen, "Enhanced Radio-Frequency Sensors Based on a Self-Dual Emitter-Absorber," *Phys. Rev. Appl.*, vol. 15, no. 1, p. 014026, Jan. 2021.

[56] N. Papasimakis, V. A. Fedotov, N. I. Zheludev, and S. L. Prosvirnin, "Metamaterial Analog of Electromagnetically Induced Transparency," *Phys. Rev. Lett.*, vol. 101, no. 25, p. 253903, Dec. 2008.

[57] R. Singh, I. Al-Naib, W. Cao, C. Rockstuhl, M. Koch, and W. Zhang, "The Fano Resonance in Symmetry Broken Terahertz Metamaterials," *IEEE Trans. Terahertz Sci. Technol.*, vol. 3, no. 6, pp. 820–826, Nov. 2013.

[58] C. W. Hsu, B. Zhen, A. D. Stone, J. D. Joannopoulos, and M. Soljačić, "Bound states in the continuum," *Nat. Rev. Mater.*, vol. 1, no. 9, p. 16048, Jul. 2016.