ENGINEERING

Electromagnetically unclonable functions generated by non-Hermitian absorber-emitter

Minye Yang[1]†, Zhilu Ye[1]†, Hongyi Pan[1], Mohamed Farhat[2]*, Ahmet Enis Cetin[1]*, Pai-Yen Chen[1]*

Physically unclonable functions (PUFs) are a class of hardware-specific security primitives based on secret keys extracted from integrated circuits, which can protect important information against cyberattacks and reverse engineering. Here, we put forward an emerging type of PUF in the electromagnetic domain by virtue of the self-dual absorber-emitter singularity that uniquely exists in the non-Hermitian parity-time (*PT*)–symmetric structures. At this self-dual singular point, the reconfigurable emissive and absorptive properties with order-of-magnitude differences in scattered power can respond sensitively to admittance or phase perturbations caused by, for example, manufacturing imperfectness. Consequently, the entropy sourced from inevitable manufacturing variations can be amplified, yielding excellent PUF security metrics in terms of randomness and uniqueness. We show that this electromagnetic PUF can be robust against machine learning–assisted attacks based on the Fourier regression and generative adversarial network. Moreover, the proposed PUF concept is wavelength-scalable in radio frequency, terahertz, infrared, and optical systems, paving a promising avenue toward applications of cryptography and encryption.

INTRODUCTION

Development of cryptographic techniques to ensure data security and privacy is critical and an urgent need in modern society. Nowadays, many cryptographic techniques have been proposed for identification (*1*), authentication (*2*), and anticounterfeiting (*3*, *4*). Among various cryptographic techniques, physically unclonable function (PUF) has been widely regarded as one of the most promising hardware security primitives, which maps input challenges C_n to output responses R_n (so-called challenge-response pairs or CRPs) of a physical system for constructing cryptographic keys (*5*–*7*). Because of unmanipulable variations arising from process variations inherent to manufacturing, CRPs are device specific and prohibitively challenging to replicate, such that they can be used as unique and unclonable encryption keys. Perhaps, silicon-based PUFs, which exploit intrinsic variations in the complementary metal-oxide semiconductor (CMOS) manufacturing process, are by far the most common PUF schemes. Up to date, a variety of silicon-based PUFs have been proposed, including static random-access memory PUFs (*8*, *9*), ring oscillator PUFs (*10*, *11*), phase change memory PUFs (*12*), and memristor PUFs (*13*, *14*). Although these digital circuit–based PUFs benefit from the high throughput and reliability of CMOS technologies, they have been recently reported to be vulnerable to approximation and modeling attacks due to the limited interdevice and intradie variations (*15*). It is therefore imperative to develop lightweight, low-cost PUFs with outstandingly lower predictability and higher resilience against machine learning–assisted attacks, so as to facilitate their practice as hardware security primitives.

Ever since the experimental validation of optical and photonic analogues of parity-time (*PT*)–symmetric non-Hermitian Hamiltonian, across the spectrum, the field of non-Hermitian physics continues to blossom, leading to many promising applications, such as unidirectional invisibility (*16*), nonreciprocal one-way optical devices (*17*), coherent perfect absorber-laser (CPAL) (*18*–*20*), high-performance telemetry for sensing (*21*–*24*), and wireless power transmission (*25*–*28*). *PT* symmetry has been innovating the design paradigms of wave propagation and scattering by expanding the control of waves into the non-Hermitian realm. However, it has been recently reported that, at or close to singular points of the *PT* system where the completeness and continuity of the Hamiltonian's eigenbasis are broken, e.g., exceptional point (EP) or CPAL point, the distribution of complex eigenvalues/eigenstates could be quite turbulent and noisy (*29*). This may cause pronounced sample-to-sample fluctuations that affect the reproducibility and scalability of non-Hermitian physical systems having EPs (*30*–*33*). In a different circumstance, high entropy nearby the EP or the CPAL point may be leveraged to generate high-quality PUF-based encryption keys. At the CPAL point, the output of the system can be switched from the lasing mode to its time-reverse counterpart, coherent perfect absorption (CPA) mode, by adjusting the complex-valued amplitude ratio of incident waves. Notably, because of the self-dual singular nature of the CPAL point, both CPA and lasing modes are narrowband effects, and both modes are susceptible to fluctuations in materials properties of gain and loss elements and their coupling rate (*34*). In this regard, even small but inevitable process variations in manufacturing *PT*-symmetric structures may produce very different output responses from device to device. Although such a property may be seen as a foe for sensing purposes, on the contrary, it may find useful applications in generating high-quality PUF keys. In particular, with the rapid advent of manufacturing technologies in the microelectronics industry, the inherent device variability on an electronic or photonic microchip has been minimized, which poses a challenge to improve the randomness and uniqueness of digital circuit–based PUFs. In this regard, the proposed PUF keys generated from the frequency-domain (analog) electromagnetic responses may

[1]Department of Electrical and Computer Engineering, University of Illinois Chicago, Chicago, IL 60607, USA. [2]Division of Computer, Electrical and Mathematical Sciences and Engineering, King Abdullah University of Science and Technology (KAUST), Thuwal 23955-6900, Saudi Arabia.
*Corresponding author. Email: mohamed.farhat@kaust.edu.sa (M.F.); aecyy@uic.edu (A.C.); pychen@uic.edu (P.-Y.C.)
†These authors contribute equally to this work.

remarkably enhance the entropy inherent in fabrication flaws, in light of the extreme sensitivity at the self-dual singularity—CPAL point, thereby enabling high cryptographic randomness and uniqueness.

Here, we propose an emerging electromagnetic PUF paradigm that exploits stochastic and fluctuating properties among CPAL devices to generate unique encryption keys. For instance, its optical realization is illustrated in Fig. 1A. Figure 1B shows the two-port transmission-line network (TLN) model for the generalized *PT*-symmetric CPAL device consisting of spatially distributed and balanced gain and loss, of which the shunt/surface conductances $-G$ (gain) and G (loss) are separated by a transmission-line segment with an electrical distance $x = kd$, where k is the propagation constant and d is the physical length. This generalized PUF paradigm can be readily translated to any physical system spanning a broad electromagnetic spectrum, including optics, photonics, radio frequency (RF), and microwave electronics. In the infrared and optical regions, the equivalent TLN model in Fig. 1B can be implemented using, for example, a pair of active and passive optical metasurfaces separated by a thin dielectric spacer, as shown in Fig. 1A (*35*–*37*). In the RF and microwave regions, the structure can be implemented using integrated circuit or printed circuit board (PCB) technology, where a negative-resistance converter (NRC) and a shunt resistor are separated by a portion of a transmission line or a T/Π-transformer. In the PUF key retrieval process, the nonlinear and analog output responses of CPAL-based PUF instances (*34*, *38*) can be appropriately discretized and digitized into the bitstring-based authorization codes with excellent unclonability (Fig. 1C). Moreover, the PUF keys retrieved from the output responses of the CPAL-based PUF instances can be reconfigured by adjusting the complex amplitude ratio of incident waves. Such a property may not be possible for most CMOS-based digital PUFs, in which each instance corresponds to one or multiple bits in the response, and, thus, increasing the number of CRPs comes at the cost of increased size, device area, and design complexity.

RESULTS

Concept of CPAL singularity enabling high randomness

The scattering parameters of the two-port TLN model in Fig. 1B can be computed using the transfer matrix method; details can be found in section S1. The CPAL point can be obtained by setting $x = \pi/2$ and $G = \sqrt{2}Y_0$, where Y_0 is the port admittance and the characteristic admittance of the finite transmission-line segment (*34*, *39*). At the CPAL point, the eigenvalues of the system's scattering matrix approach zero and infinity, corresponding to the CPA mode and the lasing mode, respectively. When characterizing the CPAL properties in terms of energy flux, the output is defined as the ratio of total output power to the total input power: $R = (|\psi_o^-|^2 + |\psi_o^+|^2)/(|\psi_i^-|^2 + |\psi_i^+|^2)$, where $\psi_i^{\pm}$ and $\psi_o^{\pm}$ are the incoming and outgoing waves from the left (−) and right (+) sides, as shown in Fig. 1B. With finite inputs, when $\psi_i^-/\psi_i^+ = i(\sqrt{2}-1)$, the CPA mode with complete absorption and zero reflection/transmission (i.e., $R \to 0$) can be obtained, whereas the lasing mode with large scattering coefficients (i.e., $R \to \infty$) can be achieved under the condition: $\psi_i^-/\psi_i^+ \neq i(\sqrt{2}-1)$; throughout this paper, we adopt the notation of $e^{i\omega t}$ and $\psi_i^-/\psi_i^+ = |\sqrt{2}-1|\,e^{i\phi}$. In the optical region, such a complex-valued amplitude ratio of two incident light waves can be achieved with a polarizer and a voltage-controlled liquid crystal phase shifter; a brief discussion on the experimental setup

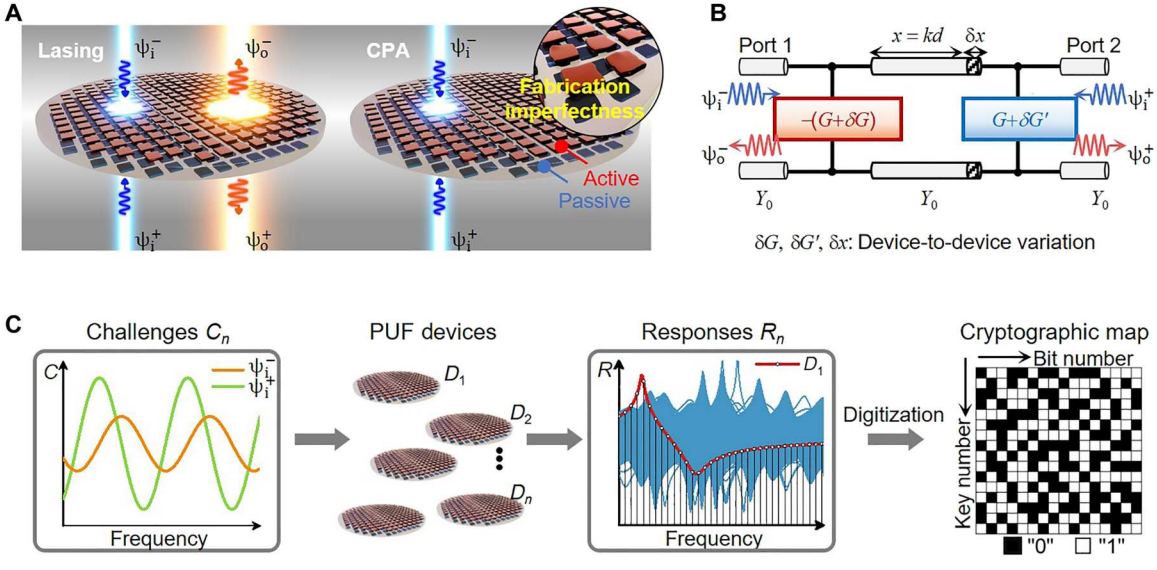

Fig. 1. Coherent perfect absorber-laser (CPAL)–enabled physically unclonable function (PUF) and PUF keys extraction. (**A**) Schematics of the proposed CPAL PUF implemented using the active and passive metasurfaces in the optical region; here, manufacturing variations can cause random fluctuations among unit cells (or meta-atoms), resulting in device-to-device variations. (**B**) Transmission-line network (TLN) model of the CPAL PUF instance in (A), which includes a negative surface/shunt conductance $-G$ (gain) and a positive surface/lumped conductance G (loss) separated by a transmission-line segment with the electrical length of $x = \pi/2$ and the characteristic admittance of Y_0. The manufacturing variations are manifested in both the conductance (δG) and the electrical length of transmission line (δx). (**C**) Cryptographic process of the proposed PUF. Different challenges (C_n) achieved with different complex-valued amplitude ratios of two incoming waves ($\alpha = \psi_i^-/\psi_i^+$) are applied to the PUF devices to generate unique responses (R_n). The responses are then discretized and digitized into binary bit strings, forming digital cryptographic maps for PUF applications. The output responses in (C) are simulation results.

can be found in section S2 (*40*). In the low-frequency range, various analog/digital phase shifters and attenuators can be used to precisely tune the complex amplitude ratio of two input radio signals.

Naturally occurring process variations in dimensions, defects, and material profiles may cause fluctuations in the shunt conductances (see Fig. 1B; here, we simply assume $\delta G = \delta G'$) and electrical distance (here, we assume δx), thus resulting in different output responses for an ensemble of CPAL devices. As an example, if the CPAL device is initially operated at the CPA mode (i.e., challenged by $\phi = \pi/2$), the output response as a function of the normalized conductive perturbation $\nu = \delta G/Y_0$ can be written as (see details in section S1)

$$R_{\mathrm{CPAL}}^{(\mathrm{CPA})} = \frac{(\nu^2+2)(\nu+\sqrt{2})^2 - 4\sec(\delta x)[2+\sqrt{2}\nu - \sec(\delta x)]}{\nu^2(\nu+2\sqrt{2})^2 + 4\tan(\delta x)^2} \quad (1)$$

In the ideal scenario with $(\nu, \delta x) = (0, 0)$, a null output response is obtained. Given that the manufacturing-induced flaws are small, i.e., $\delta x, \nu \ll 1$, applying the Taylor series expansion to Eq. 1 leads to

$$R_{\mathrm{CPAL}}^{(\mathrm{CPA})} \approx \frac{1}{4}(\delta x)^2 + \frac{\nu^2}{(\delta x)^2} + O(\nu^3) \quad (2)$$

Such a result implies that the output is sensitive to ν, with a ν^2 dependence. Further, the sensitivity of output response is enhanced by a factor of $1/(\delta x)^2$. One may envision that because of a small change in $(\nu, \delta x)$, a device could hop from the low-scattering (absorptive) mode to the high-scattering (emissive) mode, resulting in markedly different scattering responses and net outgoing energy flux. We should note that even when the system is initially operated in the lasing mode (i.e., challenged by $\phi \neq \pi/2$), a similar sensitive output response can be obtained (see section S1). Figure 2A presents the theoretical results for the contour of the output response $R_{\mathrm{CPAL}}^{(\mathrm{CPA})}$ as a function of δx and ν, plotted using Eq. 1. The scattered points represent the simulation results; throughout this paper, the simulations are performed using Pathwave Advanced Design Systems (*41*). The 1000 randomly generated CPAL-based PUF instances are initially locked in the CPA mode; here, δx (ν) is assumed to follow a Gaussian distribution with mean $\mu = 10^{-2}$ (10^{-3}) and standard deviation (SD) $\sigma = 10^{-2}$ (10^{-3}) due to device-to-device variations. From Fig. 2A, we find that, unexpectedly, even with subtle fluctuations in conductance and electrical distance, the outputs of a set of devices can differ by ~60 dB. For comparison, Fig. 2B plots the same contours as Fig. 2A but for the Fabry-Perot interferometer (FPI)–based PUF system under the same perturbation levels. The device configuration of FPI is similar to that of the CPAL device but with a pair of surface/shut conductances $G = cY_0$ and a separation distance $x = \pi$, where passive and active FPIs are obtained with $c > 0$ and $c < 0$, respectively. In contrast to the passive FPI that acts as a CPA, the active FPI exhibits only lasing properties. The results shown in Fig. 2B indicate that the output responses of FPI-based PUF systems, regardless of their type, are rather insensitive to small-valued δx and ν, with a theoretical expression approximated by (see details in section S1)

$$R_{\mathrm{FPI}} \approx \begin{cases} \left(\dfrac{c-1}{c+1}\right)^2 + \dfrac{4(c-1)}{(c+1)^3}\nu + O(\nu^2) & \text{if } c > 0 \text{ (passive)} \\ \left(\dfrac{c+1}{c-1}\right)^2 + \dfrac{4(c+1)}{(c-1)^3}\nu + O(\nu^2) & \text{if } c < 0 \text{ (active)} \end{cases} \quad (3)$$

By comparing the simulation results in Fig. 2 (A and B), we find that the CPAL PUF instances exhibit a larger variation in their output responses and, thus, potentially higher entropy than those of their passive/active FPI counterparts, thanks to the self-dual singular nature of the CPAL point. This diversified distribution of output responses caused by the interdevice variation may ensure high randomness and uniqueness for PUF applications. This paper also studies the sensitivity of output responses to ν and δx for the same *PT* system operating at the EP; details can be found in section S3. Our theoretical results show that devices operating near the CPAL point can exhibit greater variations in output responses and thus higher randomness than those operating near the EP.

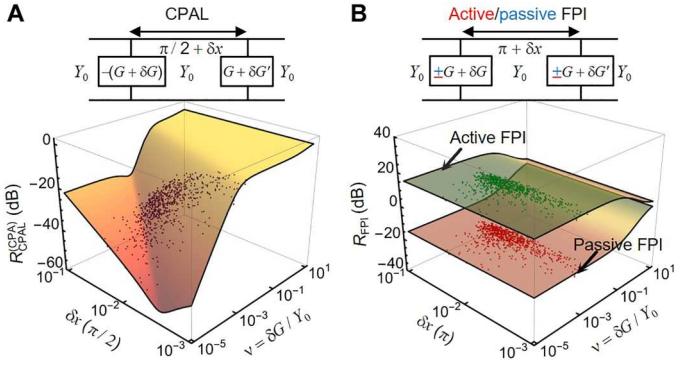

Fig. 2. Comparison of randomness between the coherent perfect absorber-laser (CPAL)–enabled physically unclonable function (PUF) and Fabry-Perot interferometer (FPI)–enabled PUF. Theoretical (contour) and simulated (point) output responses of (**A**) the parity-time (*PT*)–symmetric system operating near the CPAL point (CPA mode) and (**B**) the active FPI operating near the lasing point (top sheet) and the passive FPI operating at the CPA point (bottom sheet), as a function of the phase (δx) and impedance ($\nu = \delta G/Y_0$) perturbations; here, $\delta G = \delta G'$ are assumed, but in experiments, perturbations on both sides, δG and $\delta G'$, are not necessarily the same. For both (A) and (B), the dispersive points are from 1000 simulated PUF devices. In the simulation, δx (ν) follows the Gaussian distribution with a mean equal to 10^{-2} (10^{-3}) and standard deviation (SD) equal to 10^{-2} (10^{-3}), to mimic the realistic device-to-device fluctuations. The inset in the top panel shows the equivalent transmission-line model for each setup.

Experimental validations of the CPAL-based PUF

Here, we experimentally demonstrate the proposed electromagnetic PUF paradigm in the RF region. However, we should note that as long as the equivalent TLN model in Fig. 1B is valid, the proposed concept can be similarly implemented in the fields of optics, photonics, optomechanics, and even acoustics. At low frequencies, the CPAL-based PUF instance shown in Fig. 1B can be implemented with the lumped-element circuitry on the PCB or monolithically integrated circuit chip, as shown in Fig. 3A, where a transmission-line segment can be transformed into a compact, lumped "T" network, and the shunt $-G$ and G can be realized with the NRC and resistor, respectively. Figure 3A also shows the photograph of a prototype of an onboard CPAL PUF instance. In this prototype (Fig. 3A), NRC is based on a single current-feedback operational amplifier (OPA817,

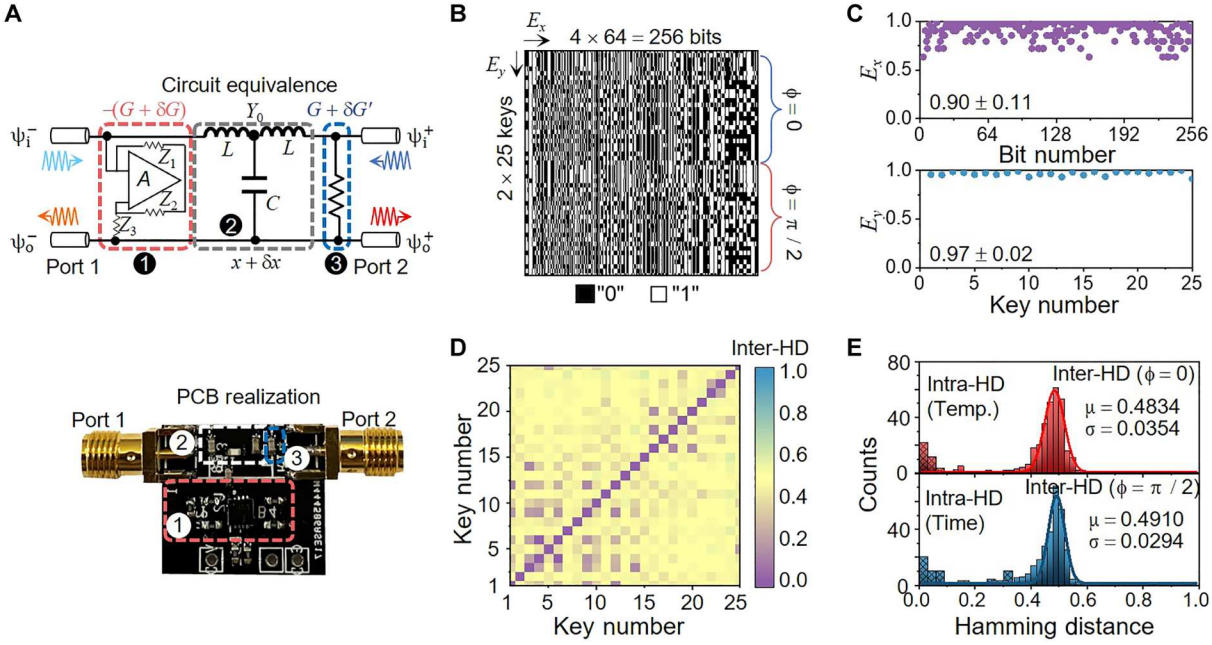

Fig. 3. Experimental results of the coherent perfect absorber-laser (CPAL)–enabled physically unclonable function (PUF). (**A**) Circuit diagram (top) and photograph (bottom) of the CPAL PUF instance realized using the printed circuit board (PCB) technology in the radio frequency (RF) range. (**B**) Bitmap measured over 25 CPAL PUF instances under two challenges (ϕ = 0, π/2). (**C**) Measured entropies E_x and E_y for the bit strings and key strings of the CPAL PUF. (**D**) Pairwise map comparing the interdevice Hamming distances (or inter-HDs) between two arbitrary PUF devices, showing that the fabricated PUF keys are almost uncorrelated. (C) and (D) were obtained by applying only the CPA challenge (ϕ = π/2). (**E**) Measured inter-HDs (solid) and intradevice HDs (intra-HDs) (meshed) of the proposed PUF by applying lasing (red) and CPA (blue) challenges and their Gaussian-fitting results. For the lasing challenge, inter-HDs fitted by a Gaussian distribution are centered at μ = 0.4834 with σ = 0.0354. For the CPA challenge, the fitted values are μ = 0.4910 and σ = 0.0294. The intra-HD histogram for temperature stability (meshed red) is centered at μ = 0.0469 with σ = 0.0513; here, four PUF devices were measured from −20° to 80°C, with an interval of 10°C. The intra-HD histogram (meshed blue) for temporal stability is centered at μ = 0.1444 with σ = 0.1534, showing great robustness; here, six PUF instances were measured every 30 s (for a total of 3 min). The intra-HDs of these challenge-response pairs (CRPs) show that the CPAL PUF can have good temperature and temporal robustness.

Texas Instruments Inc.), and types of lumped elements and integration can be found in Materials and Methods. To effectively evaluate the PUF performance, 25 PUF instances were built and tested. Because of the manufacturing process tolerance, NRCs have an averaged negative conductance of $-\overline{G_{\mathrm{NRC}}} \approx -0.0284 + i0.0001$ S at the CPAL frequency of 16.7 MHz and the averaged shunt conductance $\overline{G} = 0.0284$ S. The fabricated "T" networks also have phase variation (δx) of ±3°, alongside other parasitics from the board and package (see details in fig. S5 and section S4). It is already known that if the system is initially designed to work at the CPAL point, any small perturbation in lumped element values may cause the output response to differ substantially (see details in fig. S6 and section S4). This makes possible the generation of PUF keys. In the synthesis of PUF keys (Fig. 1C), each CPAL device as a PUF instance translates various input challenges C_n (i.e., different sets of ψ_i^-/ψ_i^+) to unique output responses R_n. In our experiment, the output response was measured over a frequency range of 16.7 ± 0.1 MHz. The output response spectrum was first normalized in the range of (0, 1) and then discretized into 64 points. Subsequently, the 64 points were digitized into a 4-bit binary code to form a 256 (4 × 64)–bit CRP as the device-specific unique identifier. For example, points with values smaller than 0.0625 will be given the binary code "0000" (details are schematically shown in Fig. 1C and explained in table S1 and section S5). We note that by changing the complex amplitude ratio $\psi_i^-/\psi_i^+ = |\sqrt{2} - 1|e^{i\phi}$ where $0 \le \phi \le \pi$, it may be possible to produce a large number of CRPs from a single PUF instance by adjusting the phase shift ϕ, which, in turn, creates other input challenges. Figure 3B plots the extracted 50 × 256 cryptographic bitmap for two challenges with ϕ = π/2 and ϕ = 0 (corresponding to the CPA and lasing modes, respectively).

The quality of PUF keys, by and large, is determined by three main metrics, namely, randomness, uniqueness, and reliability (*5*, *42*, *43*). Different PUF instances should have random and unique responses when interrogated by the same challenge, while reliability represents the consistency of the response of the same PUF instance at different environmental conditions. We first evaluate the randomness of the proposed CPAL-based PUF, i.e., the entropy of the cryptographic map associated with the uniformity, given by

$$E_{x,y} = -[p_{x,y}\log_2 p_{x,y} + (1 - p_{x,y})\log_2(1 - p_{x,y})] \quad (4)$$

where the uniformity p_x (p_y) is defined as the distribution of 0s and 1s in the bit strings (binary CRPs). Ideally, the number of 0s and 1s in the cryptographic map should occur with equal probability, which, in turn, results in $p_{x,y} = 0.5$ and $E_{x,y} = 1$. Figure 3C shows the entropies E_x and E_y extracted from the bitmap in Fig. 3B. We find that E_y (0.97 ± 0.02) exhibits a nearly perfect distribution and E_x (0.90 ± 0.11) deviates only slightly from unity, indicating excellent randomness in the generated PUF keys. The entropy quality is a direct measure but may not be sufficient to describe the randomness of a PUF. The National Institute of Standards and

Technology randomness test suite (*44*) may be used to fully assess the randomness of the CPAL-based PUF (see details in table S2 and section S6). Our results show that the CPAL-based PUF can pass all nine National Institute of Standards and Technology randomness tests (the rest six require a bit length greater than 10^6) with P values larger than 0.01. Therefore, the proposed PUF can be regarded as a true random number generator.

The uniqueness of PUF, as another important performance metric, can be assessed by the interdevice Hamming distance (or inter-HD) between the (digitized) response bit strings of all PUF instances under the same challenge. An ideal inter-HD should be 0.5, which means that, on average, half the response bits are not repeated, thus ensuring the best quality of encryption from the statistical perspective. The mean inter-HD can be expressed as

$$\overline{\mathrm{HD}_{\mathrm{inter}}} = \frac{2}{N_{\mathrm{PUF}}(N_{\mathrm{PUF}}-1)} \sum_{i=1}^{N_{\mathrm{PUF}}-1} \sum_{j=i+1}^{N_{\mathrm{PUF}}} \frac{\mathrm{HD}(\mathrm{Key}_i, \mathrm{Key}_j)}{l} \quad (5)$$

where N_{PUF} represents the number of PUF keys, l refers to the bit length, and $\mathrm{Key}_i(\mathrm{Key}_j)$ is the ith (jth) PUF key in the cryptographic map generated from the ith (jth) PUF instance under the same challenge. Figure 3D shows the pairwise comparisons of inter-HDs among 25 PUF keys. It is seen that inter-HDs in the off-diagonal areas only fluctuate slightly around the mean value of 0.46. The result suggests that all PUF keys have great uniqueness; that is, each key is unique, highly uncorrelated, and unpredictable from history. It is worth mentioning that PUF can be divided into strong and weak categories, which are classified according to the number of CRPs. A PUF is considered strong (weak) if the number of CRPs scales exponentially (linear or polynomial) with its size. Weak PUFs with a limited number of CRPs are often used for cryptographic key generation in identification applications (*45*), whereas strong PUFs capable of generating a large number of CRPs are used for authentication and secure communication applications (*46*). Since the output response of the CPAL device is very sensitive to input challenges (i.e., ψ_i^-/ψ_i^+), it may be possible to create a large CRP space by adjusting both the amplitude and/or phase offset between two incident waves. Here, we illustrate this idea by applying two challenges to the CPAL-based PUF instances: lasing ($\phi = 0$) and CPA ($\phi = \pi/2$); here, the absolute value of amplitude ratio is fixed to $\sqrt{2}-1$, while the phase shift is varied. Figure 3E plots the histogram of average inter-HDs measured over 25 PUF instances under the two challenges. The CRPs on the top (bottom) panel of Fig. 3E are obtained by applying the lasing (CPA) challenge. The inter-HDs of the lasing challenge have a near-ideal distribution where $\mu = 0.4834$ and $\sigma = 0.0354$, while that of the CPA challenge performs even better ($\mu = 0.4910$ and $\sigma = 0.0294$). The inter-HD histogram fitted by a Gaussian distribution is centered around the ideal value of 0.5. The binary encoding capacity of a PUF related to information density can be expressed as c^n, where $c = 2$ and $n = \mu(1-\mu)/\sigma^2$ (*47*, *48*). The statistical results in Fig. 3E demonstrate a high encoding dimensionality of $c^n = 2^{289}$, which may enable the development of high-capacity encryption systems. We note that the number of CRPs can be further increased by introducing more challenges in terms of phase shifts. We should also point out that the average electrical length extracted from all "T" networks is $\overline{x} \approx 17\pi/40$, which is slightly away from the CPAL point. The PUF metrics may be further improved using advanced fabrication techniques that minimize the board parasitics, allowing the devices to operate in close proximity to the CPAL point.

For comparison, we also built 25 PUF instances based on the conventional passive and active FPI structures (Fig. 4A). The lumped elements used to build these FPIs and input challenges remain the same as those used in CPAL devices. The measured output responses of passive and active FPI-based PUF instances are nearly identical, implying poor randomness and uniqueness (see details in fig. S9 and section S7). Figure 4B plots the bitmap obtained from the 25 passive FPI-based CPAs (with the challenges $\phi = 0$ and $\phi = \pi$ applied), clearly showing a deteriorated uniformity compared to the results in Fig. 3B. The entropy contents of the active (hollow circle) and passive (solid dot) FPI-based PUFs are plotted in Fig. 4C. Under the same manufacturing tolerance, the entropies of both the passive FPI-based PUF keys ($E_x = 0.54 \pm 0.41$, $E_y = 0.86 \pm 0.04$) and active FPI-based PUF keys ($E_x = 0.35 \pm 0.35$, $E_y = 0.15 \pm 0.10$) are much lower than those of the CPAL-based PUF keys. Figure 4D reports the pairwise map of inter-HDs for the passive FPI CPA-based PUF. From Fig. 4D, we find that most FPI CPA instances are highly correlated, namely, the extracted PUF keys could be vulnerable to attacks. Figure 4E is similar to Fig. 3E but obtained with active and passive FPI-based PUF instances. From these histograms, we find that the mean inter-HD value for the passive (active) FPI-based PUFs is only 0.31 (0.12). Although the passive (active) FPI-based PUF instances are also initially locked at the CPA (lasing) mode, the resulting uniqueness or randomness is much worse than that of their CPAL counterparts. The results in Fig. 4E are in sharp contrast to Fig. 3E obtained with the CPAL-based PUF. Therefore, the presence of the self-dual CPAL singularity in PT non-Hermitian systems plays a key role in amplifying the output response deviation caused by the interdevice variation, thus providing unique and unclonable encryption keys.

From the perspective of practical application, reliability refers to the consistency of CRPs under environmental variations (e.g., ambient temperature) is essential. In PUF applications, reliability can be described by intradevice HD (intra-HD), defined as the bit error rate between responses generated by the same PUF instance at different operating conditions for a given challenge

$$\overline{\mathrm{HD}_{\mathrm{intra}}} = \frac{1}{N_{\mathrm{con}}} \sum_{m=1}^{N_{\mathrm{con}}} \frac{\mathrm{HD}(\mathrm{Key}_i, \mathrm{Key}_{i,m})}{l} \quad (4)$$

where N_{con} signifies the number of operating conditions, Key_i is the original response key taken as a reference, $\mathrm{Key}_{i,m}$ is the response key at the mth operating condition, and l is the size of PUF keys. A reliable PUF should have a near-zero intra-HD. To assess the reliability of the fabricated CPAL PUF circuits, each instance was measured at 11 different temperatures (from −20° to 80°C with an interval of 10°C). The measured intra-HD histogram of the proposed PUF is shown in the top panel of Fig. 3E (meshed), which is normally distributed with a mean of 0.05 and an SD of 0.05. These values are sufficiently low to ensure good robustness against environmental variations. In addition to the temperature stability, "dynamic" noises, such as phase/flicker noises and thermal noises introduced by the agitation of electrical charges, may also generate temporal fluctuations in a system's responses. We also studied the time dependence of reliability by measuring the output responses of six CPAL PUF instances every 30 s (for a total of 3 min) and calculating the intra-HDs of the generated CRPs. The intra-HD histogram

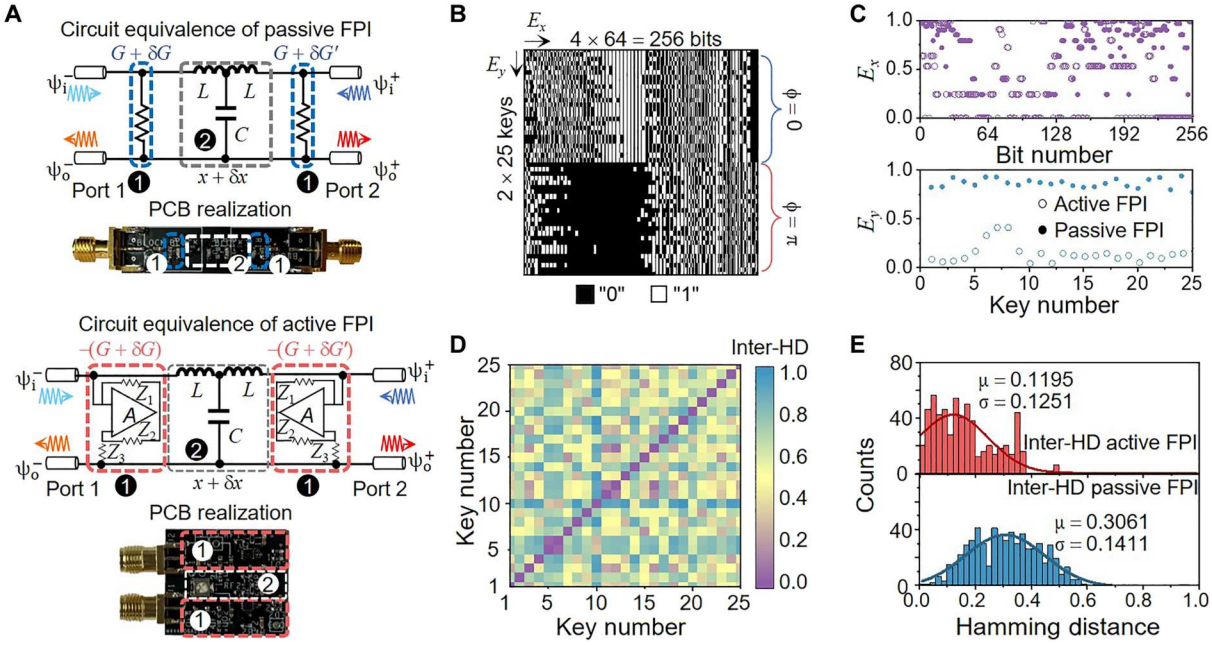

Fig. 4. Experimental results of the Fabry-Perot interferometer (FPI)–enabled physically unclonable function (PUF). (**A**) Circuit diagram of passive (top) and active (bottom) FPIs and their onboard realizations in the radio frequency (RF) region. (**B**) Bitmap measured over 25 passive FPI-based PUF instances. (**C**) Measured entropy contents of passive FPI (solid dot) and active FPI (hollow circle) PUF instances. (**D**) Pairwise map of the 25 passive FPI PUF instances. There exists a strong correlation between arbitrary PUF instances. (**E**) The interdevice Hamming distances (or inter-HDs) of the active (red) and passive (blue) FPI-based PUF instances. In both cases, the mean of the inter-HD distribution severely deviates from 0.5 (μ = 0.1195 and σ = 0.1251 for the active FPI PUF instance, and μ = 0.3061 and σ = 0.1411 for the passive FPI PUF instances).

associated with the temporal stability is plotted in the bottom panel of Fig. 3E (meshed), which shows a near-zero mean, implying that the CPAL PUF can be robust against dynamic noises. Previous studies on the CPAL systems have shown that thermal noises as the dominant noise source contributes negligibly to the signal-to-noise ratio (*49*). Last, we note that since the encryption keys of the CPAL PUF exist in an analog form (before digitization), the bit length can be arbitrarily long depending on how discretization and digitization are performed. These intriguing properties may make the proposed PUF outperform the traditional digital PUFs, such as the multiple-valued logic PUF (*50*), monostable PUF (*51*), and voltage divider PUF (*52*), of which the bit length can only be increased by introducing considerably increasing the number of cells/bits. In addition, various input challenges and, thus, a potentially large number of CRPs may be created by adjusting the complex-valued amplitude ratio of two input waves. As a result, considering all these merits, a single CPAL PUF instance may create a large CRP space, far exceeding the aforementioned digital PUFs.

The resilience of CPAL PUF to machine learning–assisted attacks

Machine/deep learning has emerged in recent years, which may provide strong assistance in pattern recognition, signal processing, and inverse design in electromagnetics (*53*–*56*). In particular, it is also reported to be a powerful tool for password-guessing attacks and decrypting (*57*, *58*). Some recent works pointed out that some PUFs with relatively low randomness and uniqueness may also be vulnerable to attacks based on machine learning models, such as the Fourier regression (FR) model and generative adversarial network (GAN) (*59*, *60*). Here, we also perform the FR- and GAN-based modeling attacks on the CPAL-based PUF. FR-based modeling attacks do not require a large training database and are, therefore, commonly used in attacking PUFs. Figure 5A shows the model expression $F(x_i)$, in which a_{0i}, a_{ni}, and b_{ni} (n = 1,2, ⋯, N) are Fourier coefficients determined by the least-squares fitting (the order of regression), and x_i is the random input in the range (0, 1); here, the 8/16/32-order regressions were performed, and only the results of 16-order are presented because it gives the optimum performance (details of FR model can be found in section S8). The FR model extracts the features of randomness from the training dataset (estimator CRPs) to predict PUF responses. In the attack-defense experiment, we divide 50 256-bit measured CRPs, which are obtained from 25 devices with two challenges, into the training dataset (40 estimator CRPs) and the test dataset (10 CRPs). After completing the training, the FR model was used to generate 10 CRPs to be compared with the test dataset. The performance of PUF could be understood from the prediction accuracy (ACC), namely, the number of correctly predicted bits as a percentage of the total number of predictions. Here, we used the correlation coefficients (CCs), defined as the linear correlation level between two random sequences and HDs between the predicted and measured CRPs, to evaluate the resilience of our CPAL PUF against attacks (details of definition of ACC and CC can be found in section S8). In an ideal scenario, the ACC, CC, and HD are expected to be sufficiently close to 50%, 0, and 0.5, respectively. Figure 5 (B to D) reports the results of the FR modeling attack. The mean values of ACC, CC, and HD are 54%, 0.03, and 0.46, respectively. Compared

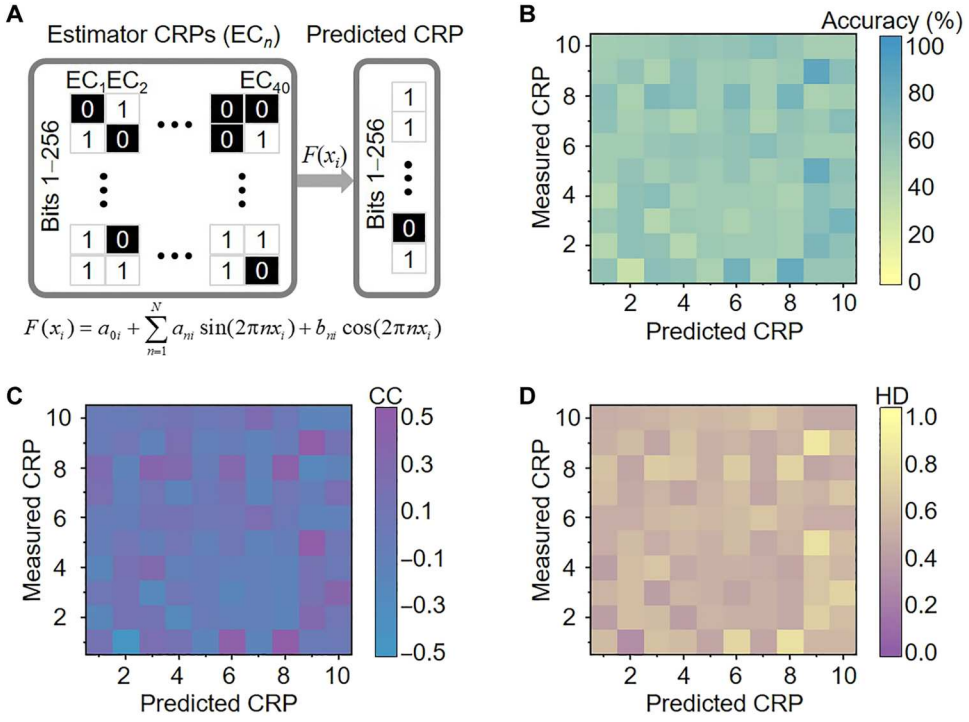

Fig. 5. Resilience of coherent perfect absorber-laser (CPAL)–enabled physically unclonable function (PUF) against Fourier regression (FR) model-assisted attacks. (**A**) Schematics of FR model with the model expression. Forty challenge-response pairs (CRPs) of the 50 measured CRPs are used for training, and the rest are used for testing. The FR model will predict 10 CRPs to compare with the testing CRPs. The colored maps of prediction accuracies (ACCs), correlation coefficients (CCs), and Hamming distances (HDs) between predicted 10 CRPs and 10 measured CRPs in (**B**), (**C**), and (**D**), respectively. The mean ACC, CC, and HD are calculated as 54%, 0.03, and 0.46, respectively, showing that our PUF may have a remarkable resilience to the attacks based on the FR model.

with the ACC in traditional silicon-based PUFs (typically larger than 90%) (*49*, *50*), these results show excellent robustness to the FR-based modeling attack.

The GAN-based modeling attack, comprising two deep neural networks, a generator and a discriminator, is another strong password-guessing tool (Fig. 6A). The discriminator is a binary classifier used to distinguish whether an input CRP belongs to the training dataset or is produced by the generator. The generator, on the flip side, strives to generate fake CRPs that resemble the training data to fool the discriminator. In many applications, such as image synthesis, the well-trained GAN can generate additional data instances that resemble the training data (details of the GAN model can be found in section S8). The GAN structure adopted in this study, as shown in Fig. 6A, consists of a generator network with four layers and a discriminator network with three layers; here, we adopted 4/3 linear layers because too many hidden layers could lead to convergence failure, which reduces the ACC of the model. Since the GAN structure requires a large amount of training data, we simulated 1000 PUF instances with the fabrication tolerance extracted from experimental results and applied 10 input challenges (10 phase differences between two input signals) to generate 10,000 CRPs, where 2000 CRPs were used for testing and the rest were kept for training. The GAN was trained with 3000 epochs. Without the loss of generality, all 0s of the CRPs for training the GAN were replaced with −1s. The distributions of ACC, CC, and HD between the GAN-predicted and -simulated CRPs are shown in Fig. 6 (B to D), respectively; here, the probability mass function of a normal distribution is adopted. It can be clearly seen that the ACC is narrowly distributed and centered at 50%, implying that the CPAL-based PUF is resilient to the GAN-based modeling attacks. The maximum (minimum) ACC is 73% (35%), corresponding to a success possibility of only 0.0001 (0.0003). These results suggest that the GAN may fail to generate CRPs resembling the ones extracted from PUF instances. The mean CC and HDs are 0.07 and 0.46, which further confirms that proposed PUF is resilient to machine learning–assisted attacks.

DISCUSSION

In summary, we have proposed a robust, high-quality PUF primitive based on the CPAL effect enabled by *PT*-symmetric non-Hermitian electromagnetic structures. We have theoretically demonstrated that the self-dual singularity may make output responses of CPAL-based PUF instances highly sensitive to inevitable device-to-device variations. Besides, we have conducted experimental studies for the CPAL-based PUF keys implemented using the RF circuits and have shown that the performance metrics, including randomness, uniqueness, correlation level, encoding capacity, and thermal/temporal stability, can outperform PUF instances based on traditional passive and active FPIs. Furthermore, the CPAL-based PUF is highly robust against state-of-the-art machine learning-assisted attacks, such as FR and GAN modeling attacks. We foresee that the proposed PUF technique may pave a promising avenue toward next-generation identification, authentication, encryption, and security systems, which may find widespread applications in modern society. The proposed hardware security paradigm may

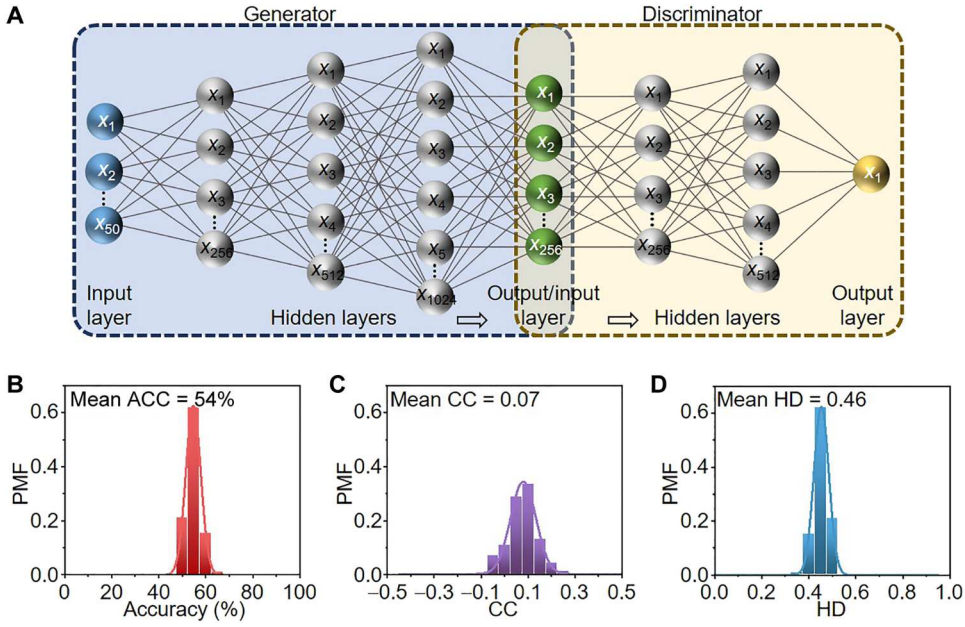

Fig. 6. Resilience of coherent perfect absorber-laser (CPAL)–enabled physically unclonable function (PUF) against generative adversarial network (GAN)–assisted attacks. (**A**) Schematics of GAN structure consists of a generator and a discriminator. In this modeling attack, we have generated 10,000 challenge-response pairs (CRPs) from our PUF by simulations, and 8000 of them are used for training, while the rest are used for testing. The probability mass functions of (**B**) prediction accuracies (ACCs), (**C**) correlation coefficients (CCs), and (**D**) Hamming distances (HDs) between the predicted CRPs by GAN and the simulated CRPs by proposed PUF. The mean ACC, CC, and HD are 54%, 0.07, and 0.46, respectively. PMF, probability mass function.

also be extended to other wave systems, such as photonics, acoustics, elastics, and optomechanics.

MATERIALS AND METHODS

Design of CPAL devices

We designed an NRC that serves as the gain element in the RF region. The effective negative resistance was also tuned to achieve the CPAL effect. The NRC circuit has a typical negative feedback-based structure, as depicted in fig. S5A. The operational amplifier used in the NRC is OPA817, fabricated by Texas Instruments Inc. By properly tuning the resistances in the feedback loop of the NRC, where $Z_2 = Z_3 = 500$ ohms was selected and Z_1 was given by a potential trimmer with a maximum resistance of 100 ohms. The distribution of negative impedances of 25 NRCs can be found in fig. S5C, of which the average negative impedance is $-\overline{Z_{\mathrm{NRC}}} \approx -35.2 - i0.2$ ohms at $f_0 = 16.7$ MHz.

Supplementary Materials

This PDF file includes:

Supplementary text sections S1 to S8
Figs. S1 to S9
Tables S1 and S2
References

REFERENCES AND NOTES

1. L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, I. Verbauwhede, Public-key cryptography for RFID-tags, *Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07)*, White Plains, NY, USA, 19 to 23 March 2007.
2. W. Diffie, M. E. Hellman, Privacy and authentication: An introduction to cryptography. *Proc. IEEE* **67**, 397–427 (1979).
3. D. Bansal, S. Malla, K. Gudala, P. Tiwari, Anti-counterfeit technologies: A pharmaceutical industry perspective. *Sci. Pharm.* **81**, 1–13 (2013).
4. A. K. Deisingh, Pharmaceutical counterfeiting. *Analyst* **130**, 271–279 (2005).
5. Y. Gao, S. F. Al-Sarawi, D. Abbott, Physical unclonable functions. *Nat. Electron.* **3**, 81–91 (2020).
6. T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, R. J. Young, A PUF taxonomy. *Appl. Phys. Rev.* **6**, 011303 (2019).
7. T. Idriss, H. Idriss, M. Bayoumi, A PUF-based paradigm for IoT security, *Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, Reston, VA, USA, 12 to 14 December 2016.
8. K. Xiao, M. T. Rahman, D. Forte, Y. Huang, M. Su, M. Tehranipoor, Bit selection algorithm suitable for high-volume production of SRAM-PUF, *Proceedings of the 2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, Arlington, VA, USA, 6 to 7 May 2014.
9. A. Garg, T. T. Kim, Design of SRAM PUF with improved uniformity and reliability utilizing device aging effect, *Proceedings of the 2014 IEEE International Symposium on Circuits and Systems (ISCAS)*, Melbourne, VIC, Australia, 1 to 5 June 2014.
10. L. Bossuet, X. T. Ngo, Z. Cherif, V. Fischer, A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon. *IEEE Trans. Emerg. Top. Comput.* **2**, 30–36 (2013).
11. M. T. Rahman, D. Forte, J. Fahrny, M. Tehranipoor, ARO-PUF: An aging-resistant ring oscillator PUF design, *Proceedings of the 2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Dresden, Germany, 24 to 28 March 2014.
12. L. Zhang, Z. H. Kong, C.-H. Chang, A. Cabrini, G. Torelli, Exploiting process variations and programming sensitivity of phase change memory for reconfigurable physical unclonable functions. *IEEE Trans. Inf. Forensics Secur.* **9**, 921–932 (2014).
13. G. S. Rose, N. McDonald, L.-K. Yan, B. Wysocki, K. Xu, Foundations of memristor based PUF architectures, *Proceedings of the 2013 IEEE/ACM International Symposium on Nanoscale Architectures (NANOARCH)*, Brooklyn, NY, USA, 15 to 17 July 2013.
14. P. Koeberl, Ü. Kocabaş, A.-R. Sadeghi, Memristor PUFs: A new generation of memory-based physically unclonable functions, *Proceedings of the 2013 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Grenoble, France, 18 to 22 March 2013.
15. H. Nili, G. C. Adam, B. Hoskins, M. Prezioso, J. Kim, M. R. Mahmoodi, F. M. Bayat, O. Kavehei, D. B. Strukov, Hardware-intrinsic security primitives enabled by analogue state and nonlinear conductance variations in integrated memristors. *Nat. Electron.* **1**, 197–202 (2018).

16. Z. Lin, H. Ramezani, T. Eichelkraut, T. Kottos, H. Cao, D. N. Christodoulides, Unidirectional invisibility induced by PT-symmetric periodic structures. *Phys. Rev. Lett.* **106**, 213901 (2011).
17. C. E. Rüter, K. G. Makris, R. El-Ganainy, D. N. Christodoulides, M. Segev, D. Kip, Observation of parity–time symmetry in optics. *Nat. Phys.* **6**, 192–195 (2010).
18. S. Longhi, PT-symmetric laser absorber. *Phys. Rev. A* **82**, 031801 (2010).
19. H.-Y. Wu, F. Vollmer, Enhanced chiroptical responses through coherent perfect absorption in a parity-time symmetric system. *Commun. Phys.* **5**, 78 (2022).
20. D. G. Baranov, A. Krasnok, T. Shegai, A. Alù, Y. Chong, Coherent perfect absorbers: Linear control of light with light. *Nat. Rev. Mater.* **2**, 17064 (2017).
21. P.-Y. Chen, M. Sakhdari, M. Hajizadegan, Q. Cui, M. M.-C. Cheng, R. El-Ganainy, A. Alù, Generalized parity–time symmetry condition for enhanced sensor telemetry. *Nat. Electron.* **1**, 297–304 (2018).
22. M. Sakhdari, M. Hajizadegan, Q. Zhong, D. N. Christodoulides, R. El-Ganainy, P.-Y. Chen, Experimental observation of PT symmetry breaking near divergent exceptional points. *Phys. Rev. Lett.* **123**, 193901 (2019).
23. R. Fleury, D. Sounas, A. Alù, An invisible acoustic sensor based on parity-time symmetry. *Nat. Commun.* **6**, 5905 (2015).
24. Z.-P. Liu, J. Zhang, Ş. K. Özdemir, B. Peng, H. Jing, X.-Y. Lü, C.-W. Li, L. Yang, F. Nori, Y. Liu, Metrology with PT-symmetric cavities: Enhanced sensitivity near the PT-phase transition. *Phys. Rev. Lett.* **117**, 110802 (2016).
25. M. Song, P. Jayathurathnage, E. Zanganeh, M. Krasikova, P. Smirnov, P. Belov, P. Kapitanova, C. Simovski, S. Tretyakov, A. Krasnok, Wireless power transfer based on novel physical concepts. *Nat. Electron.* **4**, 707–716 (2021).
26. S. Assawaworrarit, S. Fan, Robust and efficient wireless power transfer using a switch-mode implementation of a nonlinear parity–time symmetric circuit. *Nat. Electron.* **3**, 273–279 (2020).
27. M. Sakhdari, M. Hajizadegan, P.-Y. Chen, Robust extended-range wireless power transfer using a higher-order PT-symmetric platform. *Phys. Rev. Res.* **2**, 013152 (2020).
28. X. Hao, K. Yin, J. Zou, R. Wang, Y. Huang, X. Ma, T. Dong, Frequency-stable robust wireless power transfer based on high-order pseudo-Hermitian physics. *Phys. Rev. Lett.* **130**, 077202 (2023).
29. N. A. Mortensen, P. A. D. Gonçalves, M. Khajavikhan, D. N. Christodoulides, C. Tserkezis, C. Wolff, Fluctuations and noise-limited sensing near the exceptional point of parity-time-symmetric resonator systems. *Optica* **5**, 1342 (2018).
30. R. El-Ganainy, K. G. Makris, M. Khajavikhan, Z. H. Musslimani, S. Rotter, D. N. Christodoulides, Non-Hermitian physics and PT symmetry. *Nat. Phys.* **14**, 11–19 (2018).
31. P.-Y. Chen, R. El-Ganainy, Exceptional points enhance wireless readout. *Nat Electron.* **2**, 323–324 (2019).
32. C. Hahn, Y. Choi, J. W. Yoon, S. H. Song, C. H. Oh, P. Berini, Observation of exceptional points in reconfigurable non-Hermitian vector-field holographic lattices. *Nat. Commun.* **7**, 1–6 (2016).
33. M. Yang, L. Zhu, Q. Zhong, R. El-Ganainy, P.-Y. Chen, Spectral sensitivity near exceptional points as a resource for hardware encryption. *Nat. Commun.* **14**, 1145 (2023).
34. M. Farhat, M. Yang, Z. Ye, P.-Y. Chen, PT-symmetric absorber-laser enables electromagnetic sensors with unprecedented sensitivity. *ACS Photonics* **7**, 2080–2088 (2020).
35. R. Fleury, D. L. Sounas, A. Alù, Negative refraction and planar focusing based on parity-time symmetric metasurfaces. *Phys. Rev. Lett.* **113**, 023903 (2014).
36. P.-Y. Chen, J. Jung, PT symmetry and singularity-enhanced sensing based on photoexcited graphene metasurfaces. *Phys. Rev. Appl.* **5**, 064018 (2016).
37. M. Lawrence, N. Xu, X. Zhang, L. Cong, J. Han, W. Zhang, S. Zhang, Manifestation of PT symmetry breaking in polarization space with terahertz metasurfaces. *Phys. Rev. Lett.* **113**, 093901 (2014).
38. R. Pappu, Physical one-way functions. *Science* **297**, 2026–2030 (2002).
39. M. Sakhdari, M. Farhat, P.-Y. Chen, PT-symmetric metasurfaces: Wave manipulation and sensing using singular points. *New J. Phys.* **19**, 065002 (2017).
40. C.-S. Yang, T.-T. Tang, P.-H. Chen, R.-P. Pan, P. Yu, C.-L. Pan, Voltage-controlled liquid-crystal terahertz phase shifter with indium–tin–oxide nanowhiskers as transparent electrodes. *Opt. Lett.* **39**, 2511–2513 (2014).
41. Keysight, *Pathwave Advanced Design System (ADS)*;www.keysight.com/us/en/products/software/pathwave-design-software/pathwave-advanced-design-system.html.
42. R. Arppe, T. J. Sørensen, Physical unclonable functions generated through chemical methods for anti-counterfeiting. *Nat. Rev. Chem.* **1**, 0031 (2017).
43. R. Maes, I. Verbauwhede, Physically unclonable functions: A study on the state of the art and future research directions, in *Towards Hardware-Intrinsic Security* (Springer Science & Business Media, 2010).
44. L. E. Bassham III, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, *Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* (National Institute of Standards & Technology, 2010).
45. C. Herder, M.-D. Yu, F. Koushanfar, S. Devadas, Physical unclonable functions and applications: A tutorial. *Proc. IEEE* **102**, 1126–1141 (2014).
46. Y. Gao, H. Ma, D. Abbott, S. F. Al-Sarawi, PUF sensor: Exploiting PUF unreliability for secure wireless sensing. *IEEE Trans. Circuits Syst. I Regul. Pap.* **64**, 2532–2543 (2017).
47. J. W. Leem, M. S. Kim, S. H. Choi, S.-R. Kim, S.-W. Kim, Y. M. Song, R. J. Young, Y. L. Kim, Edible unclonable functions. *Nat. Commun.* **11**, 328 (2020).
48. M. R. Carro-Temboury, R. Arppe, T. Vosch, T. J. Sørensen, An optical authentication system based on imaging of excitation-selected lanthanide luminescence. *Sci. Adv.* **4**, e1701384 (2018).
49. M. Yang, Z. Ye, M. Farhat, P.-Y. Chen, Enhanced radio-frequency sensors based on a self-dual emitter-absorber. *Phys. Rev. Appl.* **15**, 014026 (2021).
50. Y. Zhang, Z. Pan, P. Wang, D. Ding, Q. Yu, A 0.1-pJ/b and ACF <0.04 multiple-valued PUF for chip identification using bit-line sharing strategy in 65-nm CMOS. *IEEE Trans. VLSI Syst.* **27**, 1043–1052 (2019).
51. G. Li, P. Wang, X. Ma, Y. Shi, B. Chen, Y. Zhang, A multimode configurable physically unclonable function with bit-instability-screening and power-gating strategies. *IEEE Trans. VLSI Syst.* **29**, 100–111 (2021).
52. M. Vatalaro, R. De Rose, M. Lanuzza, 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.* **57**, 2509–2520 (2022).
53. C. M. Bishop, N. M. Nasrabadi, *Pattern Recognition and Machine Learning* (Springer, 2006).
54. N. D. Sidiropoulos, L. De Lathauwer, X. Fu, K. Huang, E. E. Papalexakis, C. Faloutsos, Tensor decomposition for signal processing and machine learning. *IEEE Trans. Signal Process* **65**, 3551–3582 (2017).
55. W. W. Ahmed, M. Farhat, X. Zhang, Y. Wu, Deterministic and probabilistic deep learning models for inverse design of broadband acoustic cloak. *Phys. Rev. Res.* **3**, 013142 (2021).
56. W. W. Ahmed, M. Farhat, P.-Y. Chen, X. Zhang, Y. Wu, A generative deep learning approach for shape recognition of arbitrary objects from phaseless acoustic scattering data. arXiv:2207.05433 [cs.SD] (2022).
57. B. Hitaj, P. Gasti, G. Ateniese, F. Perez-Cruz, PassGAN: A deep learning approach for password guessing, *Proceedings of the 17th International Conference on Applied Cryptography and Network Security,* Bogota, Colombia, 5 to 7 June 2019.
58. Y. Ding, P. Horster, Undetectable on-line password guessing attacks. *Oper. Syst. Rev.* **29**, 77–86 (1995).
59. A. Dodda, S. Subbulakshmi Radhakrishnan, T. F. Schranghamer, D. Buzzell, P. Sengupta, S. Das, Graphene-based physically unclonable functions that are reconfigurable and resilient to machine learning attacks. *Nat. Electron.* **4**, 364–374 (2021).
60. J. Lu, T. Morehouse, J. Yuan, R. Zhou, Machine-learning PUF-based detection of RF anomalies in a cluttered RF environment, *Proceedings of the 2021 IEEE International Symposium on Technologies for Homeland Security (HST)*, Boston, MA, USA, 8 to 9 November 2021.
61. Z. Ye, M. Yang, L. Zhu, P.-Y. Chen, PTX-symmetric metasurfaces for sensing applications. *Front. Optoelectron.* **14**, 211–220 (2021).
62. I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, Y. Bengio, Generative adversarial networks. *Commun. ACM* **63**, 139–144 (2020).
63. R. Rojas, The backpropagation algorithm, in *Neural networks* (Springer, 1996), pp. 149–182.
64. D. P. Kingma, J. Ba, Adam: A method for stochastic optimization. arXiv:1412.6980 [cs.LG] (2014).

Acknowledgments
Funding: A.E.C. acknowledges the financial support from Discovery Partners Institute, University of Illinois System. A.E.C. and P.-Y.C. would like to thank NSF ECCS-2229659 Grant for supporting this work. **Author contributions:** P.-Y.C., M.Y., M.F., and A.E.C. conceived the project. M.Y. and Z.Y. performed the simulations and conducted the experiments. Z.Y., M.Y., and P.-Y.C. developed the theoretical basis. H.P. and A.E.C. provided the support of machine learning experiments. All authors analyzed the data and contributed to the manuscript writing. M.Y. and Z.Y. contributed equally to this work. **Competing interests:** The authors declare that they have no competing interests. **Data and materials availability:** All data needed to evaluate the conclusions in the paper are present in the paper and/or the Supplementary Materials.

Submitted 18 January 2023
Accepted 9 August 2023
Published 8 September 2023
10.1126/sciadv.adg7481