ACS NANO

www.acsnano.org

ARTICLE

Reconfigurable Electromagnetically Unclonable Functions Based on Graphene Radio-Frequency Modulators

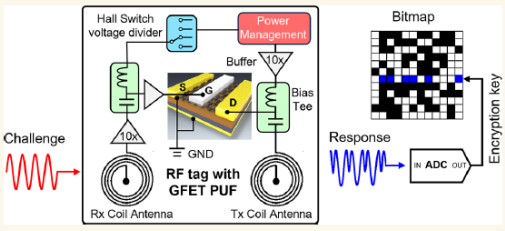
Yichong Ren, Chia-Heng Sun, Mohan De Silva, Hongyi Pan, Xuecong Nie, Emadeldeen Hamdan, Zhixian Zhou, Ahmet Enis Cetin,* and Pai-Yen Chen*

Cite This: *ACS Nano* 2026, 20, 421−431

Read Online

ACCESS | Metrics & More | Article Recommendations | Supporting Information

ABSTRACT: Modern society, revolutionized by the Internet of Things (IoTs), is witnessing exponential growth in the number of connected devices and the volume of data being generated and shared, raising significant concerns about safeguarding classified information against various cyber threats. Here, we introduce a lightweight, robust hardware security primitive based on the electromagnetic physical unclonable function (PUF) for cryptographic identification and authentication of wireless devices. Unlike traditional digital-based PUFs, the proposed electromagnetic PUF keys are generated using graphene-based harmonic transponders, of which the inherent variations in electronic properties of ambipolar graphene field-effect transistors (GFETs) result in highly stochastic, mixed modulations of radio frequency (RF) signals (i.e., unique electromagnetic fingerprints). Our experimental results demonstrate that this electromagnetic PUF exhibits excellent PUF performance metrics in terms of randomness, uniqueness, reliability, and resistance to machine learning-based modeling attacks. Moreover, the PUF keys can be reconfigured by altering the RF excitation frequency or through the electrostatic gating effect, further strengthening the security and resilience against modeling attacks. The proposed electromagnetic PUF may be well-suited for a variety of wireless authentication, encryption, and anticounterfeiting applications, and supports cryptographic key generation.



KEYWORDS: *low-dimensional nanomaterials, graphene field-effect transistors (GFET), radio frequency (RF) oscillator, physical unclonable function (PUF), hardware security*

INTRODUCTION

The advancement of 5G and beyond-5G (B5G) technologies has given birth to the Internet-of-things (IoTs) and machine-to-machine (M2M) networks, creating massive flows of data amid numerous wireless sensors, edge gateways, and infrastructures. As IoT devices gain popularity across various sectors, there are increasing concerns about how to protect these devices against more frequent and sophisticated cyberattacks that leverage artificial intelligence (AI) algorithms to automate or accelerate the malicious process.[1] This has raised an urgent demand for more robust security measures to authenticate and safeguard wireless devices, ensuring the trustworthiness and dependability of IoT ecosystems. In today's software-based encryption mechanisms, cryptographic keys, derived from passwords stored in digital memories, provide users with accessibility to the encrypted data underlying the locks. However, this key-and-lock form has been proven vulnerable against adversarial attacks powered by machine and deep learning algorithms.[2] To address such challenges, tremendous research efforts have been devoted to hardware-enabled cryptographic alternatives over the past decade.[3,4] Yet, existing hardware-based physical layer security solutions, such as low-cost chipless radio frequency identification (RFID),[5] remain vulnerable to exhaustive mining attacks due to the limited key space or lack of signal unpredictability. Recently, physically unclonable functions (PUFs) have emerged as a promising new class of hardware-based security primitives, which leverage physical variations occurring naturally during chip manufacturing (i.e., low-cost

Received: August 2, 2025
Revised: December 11, 2025
Accepted: December 12, 2025
Published: December 20, 2025

https://doi.org/10.1021/acsnano.5c13119
ACS Nano 2026, 20, 421−431

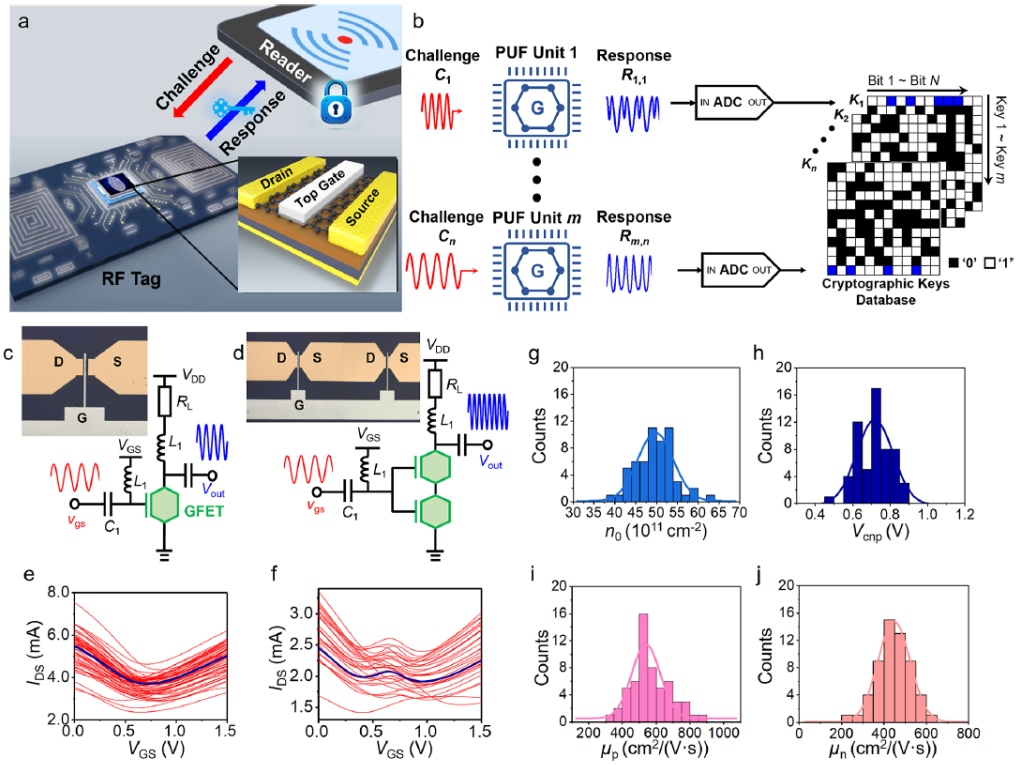


Figure 1. GFET-based RF PUF for cost-effective, low-latency, and reliable wireless identification and authentication. (a) Schematic of the RF PUF primitive based on a GFET harmonic transponder. (b) Cryptographic process of the proposed RF PUF: n-th challenge (C_n), achieved with different interrogating signals and electrostatic gating conditions, are applied to the m-th PUF devices to generate unique responses ($R_{m,n}$). The responses are then discretized and digitized into binary bit strings, forming digital cryptographic maps for PUF applications. Schematics of (c) single-GFET (d) and dual-GFET RF signal modulators. (e) Measured drain current-gate voltage characteristics (I_{DS}−V_{GS}) of 60 single-channel GFETs with their device structure depicted in (c). (f) Is similar to (e), but for dual-channel GFETs depicted in (d). Statistical results for (g) residue density n_0, (h) charge neutrality point V_{cnp}, (i) hole mobility μ_p, and (j) electron mobility μ_n of 60 single-channel GFETs.

entropy source) to produce highly unpredictable and device-specific encryption keys. A PUF instance can translate input challenges to unique output responses so as to build a database of challenge−response pairs (CRPs) for authentication.[6,7] In this regard, each CRP produced by a specific hardware instance must be unique and unclonable, which can be characterized by predefined randomness, uniqueness, and unclonability functions.[7] By far, the majority of PUFs are based on complementary metal-oxide-semiconductor (CMOS) integrated circuits (ICs) due to their low cost, high integrability, and digital compatibility. For instance, the static random-access memory (SRAM)-based PUF, as one of the most common types, exploits the unique startup values of SRAM cells, which are rather random between devices, to create a unique pattern of 0s and 1s for each SRAM cell.[8] Similarly, the arbiter PUF measures the difference in delay between two identical but physically slightly varied logic paths within a circuit to generate a 1 bit PUF response.[9] Although these digital PUFs benefit from the mature CMOS fabrication technologies, on the flip side, they also suffer from the relatively low device-to-device variation, as improving the manufacturing yield is prioritized in the semiconductor industry. To make things worse, due to this paradox, some recent studies have reported that conventional CMOS-based PUFs may still be susceptible to machine learning-based modeling attacks.[10] In addition, CMOS-based PUFs, which rely on threshold voltage or delay variations across cells in an array, often encounter limitations in scalability, cost, and power consumption. Due to their restricted number of CRPs, these digital PUFs are typically classified as weak PUFs.[7] By contrast, a strong PUF capable of generating enormous CRPs is always desirable to better secure wireless identification and communication in dynamic environments.[11]

In recent years, many efforts have been dedicated to exploring new materials, devices, and system architectures to enhance the reliability and unpredictability of PUFs. Very recently, digital PUFs realized with electronic devices based on graphene and low-dimensional materials have been proposed.[12,13] Graphene field-effect transistors (GFETs) have been enormously studied in the past decade for their unique ambipolar transport properties and shiftable charge neutrality point V_{cnp} (via the electrostatic or chemical doping[14,15]). Although graphene's exotic monatomic structure makes the characteristics of GFET very sensitive to nanomanufacturing

https://doi.org/10.1021/acsnano.5c13119
ACS Nano 2026, 20, 421−431

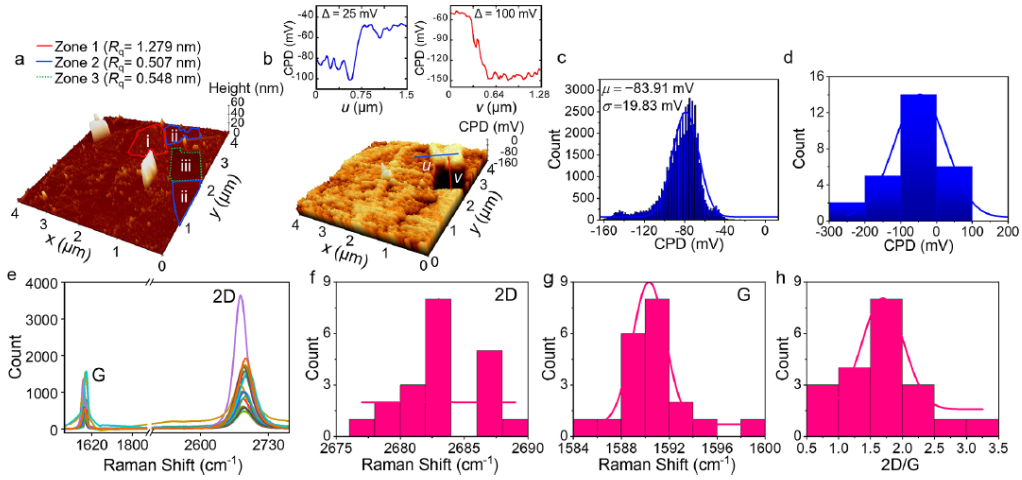


Figure 2. Surface roughness, electrostatic potential, and Raman characterization of CVD-grown graphene channels. (a) AFM and (b) KPFM images of a graphene channel, comprising the regions of graphene covered by resist residues (Zone 1), clean graphene (Zone 2), and exposed bare SiO_2 substrate (Zone 3). The top-left and top-right insets in (b) highlight the CPD differences between zone 1 and zone 2, and between zone 2 and zone 3, respectively. (c) Histogram of CPDs measured by the KPFM across the entire sample area for a representative graphene channel. (d) Distribution of the mean CPD values over the graphene channels of 20 GFETs. (e) Raman spectra of 20 graphene channels, with the corresponding distributions of the obtained 2D- and G-band peaks displayed in (f) and (g), respectively. (h) Distribution of the 2D/G intensity ratio.

imperfections (e.g., variations in graphene's number of layers, strains, and defects) and random dopant fluctuation, such properties may be ideal for implementing the tamper-resilient PUF instances.[16,17] So far, several GFET-based digital PUFs, such as resistive random access memory (RRAM) PUFs[18] and straintronic PUFs,[19] have been proposed and demonstrated to be robust against cloning and tampering. Here, we conceptually introduce a lightweight and robust PUF primitive based on a single-GFET or dual-GFET, as depicted in Figure 1a, which can be seamlessly integrated with RF front-end components in wireless identification and communication systems. A single GFET, which exhibits the "V-shape" transfer characteristics (drain current I_{DS} v.s. gate voltage V_{GS}), can be regarded as a lightweight multifunctional signal modulator (Figure 1c). When it is operated at the V_{cnp}, it can act as a simple, yet effective frequency doubler in RF and mixed-signal circuits.[20,21] On the other hand, when the same device is operated in the linear I_{DS}−V_{GS} regions aside from V_{cnp}, it can act as an amplitude or phase modulator.[22] Furthermore, a dual-GFET circuit with the "W-shape" I_{DS}−V_{GS} curve has been proposed to build a frequency tippler (Figure 1d).[23]

The unclonable, device-specific electronic properties arising from stochastic material characteristics are evident in the transfer characteristics of GFETs shown in Figure 1e−j. The Dirac point shift, asymmetricity, and nonlinearity, appearing in the ambipolar transport characteristics of GFETs (Figure 1e,f) result in the complex mixed (frequency/amplitude/phase) modulation of RF signal,[24,25] producing unique yet reconfigurable (i.e., via the gating effect) electromagnetic fingerprints that can be converted into PUF-based cryptographic keys for wireless identification and authentication applications, as illustrated in Figure 1b. When compared to those digital PUFs based on arrayed nanomaterial transistors and memory cells,[13,26] the proposed RF PUF offers several advantages, such as scalability, energy efficiency, low latency, and compatibility with wireless systems. For instance, in wireless authentication applications (see Figure 1a,b), an identification (ID) tag comprising the GFET-based PUF core can backscatter a unique, unpredictable, and repeatable RF signal when interrogated by a wireless reader via an inductive or radiative link. Once the backscattered RF response is validated by the reader connected to the database in IoT gateways or edge devices, the ID tag's access request is authorized. As illustrated in Figure 1b, the reader launches a monotonic RF signal as the challenge C_n to the m-th PUF instance; a unique mixed-modulation product will be obtained as the response $R_{m,n}$. On the reader, responses can be discretized and digitized into binary encryption keys through a proper analog-to-digital conversion (ADC) process, and they are ultimately stored in the cryptographic bitmap K_n. Moreover, PUF keys, derived from the modulated RF signals, can be reconfigured by varying the carrier frequency of RF excitation or be self-reconfigurable by altering the GFET's gate bias, resulting in a large CRP space formed by multiple bitmaps. When the RF PUF is used for secure wireless communications, the GFET-based PUF core is placed on the transceiver side and integrated with, for example, an amplitude-shift keying (ASK) modulator. In this case, the PUF signal embedded in the on-state of the on-off keying signal is first certificated by the receiver with the predefined authentication. After verification, the encrypted information stored in the receiver is authorized to be transmitted to the transceiver, thereby avoiding privacy leakage and guaranteeing secure communications. The integration of this PUF technique with wireless identification and communication systems is discussed in Supporting Information S1. In this work, we experimentally study RF PUFs based on the single-GFET and dual-GFET modulators sketched in Figure 1c,d, and report their PUF performance metrics in terms of randomness, uniqueness, reliability, and resilience to machine learning

https://doi.org/10.1021/acsnano.5c13119
ACS Nano 2026, 20, 421−431

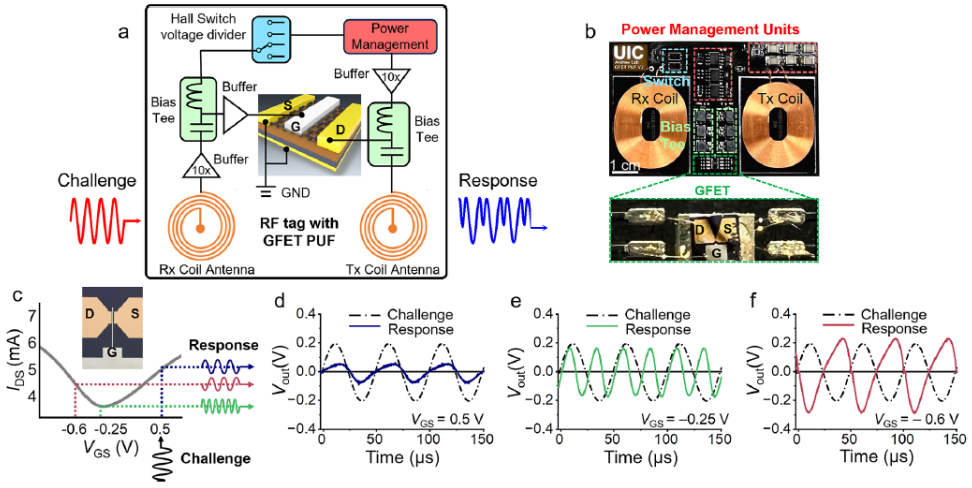


Figure 3. Reconfigurable RF PUF primitive based on a GFET signal modulator. (a) Circuit diagram and (b) photograph of a compact RF tag equipped with a GFET-based PUF core for wireless identification and anticounterfeiting applications. (c) Drain current-gate voltage characteristics of a single-GFET modulator and its RF output responses under various modulation schemes: (d) amplitude modulation at the gate bias voltage V_{GS} = 0.5 V, (e) frequency modulation at V_{GS} = − 0.25 V, and (f) phase modulation at V_{GS} = − 0.6 V.

assisted attacks using generative adversarial neural network (GAN) model.

RESULT/DISCUSSION

Atomic Force Microscopy, Kelvin Probe Force Spectroscopy, and Raman Spectroscopy Characterization of Graphene Channels. The electronic properties of atomically thin 2D materials such as graphene are known to be highly sensitive to manufacturing variations during the material growth and device fabrication processes.[27,28] Possible factors that can cause variations in electronic properties include grain boundaries, wrinkles, edge roughness, charge puddles, strain fluctuations, and substrate/oxide-induced traps,[27−29] among others. Here, Kelvin probe force microscopy (KPFM; Park Systems XE 70) was utilized to elucidate the origins of the Dirac point shift, asymmetry, and nonlinearity in the ambipolar transport of GFETs under ambient conditions. Figure 2 presents the structural and surface characteristics of the chemical vapor deposition (CVD)-grown graphene channel. As a representative example, Figure 2a,b shows the nanoscale surface morphology and local potential difference of a graphene channel. The three-dimensional (3D) atomic force microscopy (AFM) topography in Figure 2a resolves regions of graphene covered by resist residues (Zone 1), clean graphene (Zone 2), and the exposed SiO_2 substrate (Zone 3), which are outlined in red, blue, and green, respectively. The residue-covered graphene exhibits the largest root-mean-square roughness (R_q = 1.279 nm), while the clean graphene and bare substrate show significantly lower roughness values (R_q = 0.507 nm and 0.548 nm, respectively). The surface roughness correlates with fluctuations in local contact potential difference (CPD) between the clean graphene and the residue-covered graphene, as illustrated in the KPFM images in the insets of Figure 2b. Figure 2c reports the histograms that quantify the distributions of CPD for the graphene channel in Figure 2a,b, across the entire sample area. Figure 2d reports the histogram of the mean CPD values for the graphene channels of 20 GFETs, revealing pronounced device-to-device variations that contribute to the randomness observed in ambipolar transport characteristics of GFETs; detailed CPD histograms for all 20 GFETs' channels are provided in S1 of the Supporting Information. The CPD measurement results can be used to extract variations in work function on the graphene surface. The results indicate a Fermi-level shift of approximately 0.30 eV away from the Dirac point,[30] corresponding to a carrier density of approximately 6.5 × 10^{12} cm^{-2}. The same analysis reveals that photoresist residues contribute only an additional ∼30 meV work function shift relative to clean graphene, indicating that the dominant Fermi-level modulation originates from substrate-induced charge inhomogeneity, with possible contributions from local strain and nonuniform graphene layer thickness (see S1 of the Supporting Information for a more detailed analysis). Furthermore, the 532 nm Raman spectroscopy was employed to analyze variations in the structural and electronic properties of the CVD-grown graphene. For each device, the Raman measurement was conducted at the center of the graphene channel to ensure a fair comparison across all samples. Figure 2e reports the Raman spectra from 20 graphene channels, showing that all of them exhibit the characteristic G (∼1580 cm^{-1}) and 2D (∼2680 cm^{-1}) bands with minimal D-band intensity, which infers a low defect density.[31] Despite identical manufacturing processing, the extracted 2D- and G-band peaks display clear statistical spreads, as shown in Figure 2f,g, respectively. Such fluctuations may originate from nanoscale variations commonly observed in CVD-grown graphene transferred onto SiO_2 substrates such as local strain, charge-doping fluctuations, and transfer-related chemical residues.[32−34] The distribution of the 2D/G ratio (Figure 2h) further indicates the presence of nonuniform graphene layer thickness, where higher values correspond to monolayer regions and lower values to multilayer domains.[35] These Raman results highlight the inherent material variability of CVD graphene, which contributes to the variant electronic

https://doi.org/10.1021/acsnano.5c13119
ACS Nano 2026, 20, 421−431

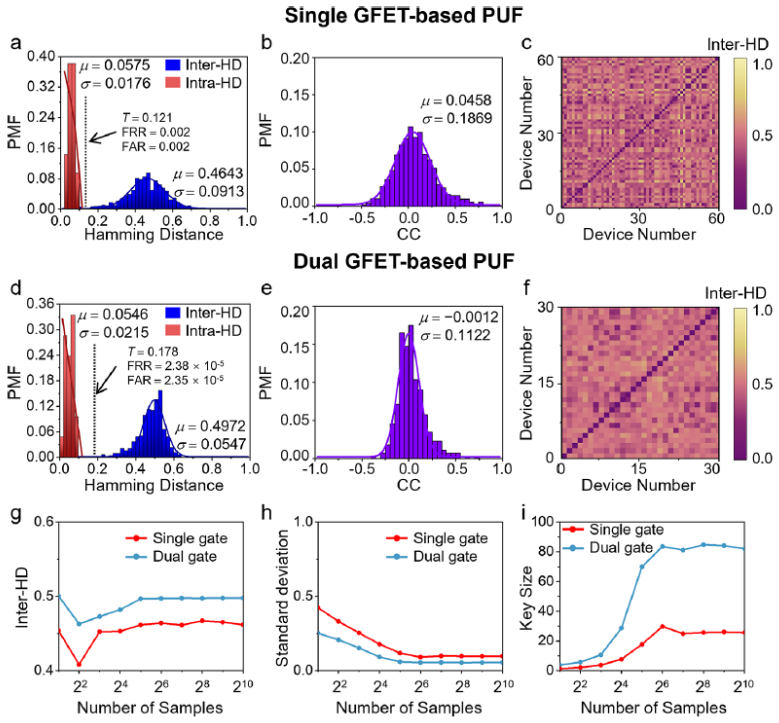


Figure 4. Measured performance metrics of GFET-based PUF instances. Measurement results for single-GFET PUF instances: (a) inter-HD, intra-HD, FRR and FAR, (b) Pearson correlation coefficient analysis, and (c) pairwise response evaluations. (d–f) are similar to (a–c), but for dual-GFET PUF instances. (g) Mean of inter-HDs, (h) standard deviation of inter-HDs, and (i) key size as a function of the sampling rate (the number of samples taken per 0.5 ms window) that is proportional to the number of bits; here, V_{GS} = 0 V and f_0 = 10 kHz.

responses that serve as the entropy source of our graphene-based PUF.

Characteristics of Graphene-Based RF Modulators. The proposed RF PUF is based on a harmonic transponder comprising the single or dual top-gated GFETs. A native oxide layer (Al_2O_3) adherent to the aluminum surface is used as the gate dielectric between the aluminum top gate and the graphene channel. Since native oxide exhibits random doping and gating effects (e.g., trapped charges induced by surface defects), the electronic properties of GFETs follow a Gaussian distribution. Figure 1e reports the measured transfer characteristics of 60 fabricated top-gated GFETs. It can be observed that each device possesses a unique transfer characteristic. Figure 1g–j reports the distributions of charge residue density n_0, charge neutrality point V_{cnp}, hole mobility μ_p, and electron mobility μ_n extracted from the transfer characteristics of top-gated GFETs, respectively; see Supporting Information S1 for details. It is evident that all these physical quantities follow the Gaussian distribution. Figure 1f is similar to Figure 1e, but for the static characteristics of dual-GFET modulators in Figure 1d. A dual-GFET modulator is formed by a pair of series connected GFETs that share one gate electrode. Due to the random dopant and gate oxide variations, the two channels in the dual-GFET modulator generally have dissimilar V_{cnp}, leading to the "W-shaped" transfer characteristic and thus generation of third and higher harmonics.[23] Since dual-GFET modulators typically generate more complex RF output responses (i.e., a mix of multiple harmonics), they are expected to provide improved PUF's randomness and unpredictability compared to their single-GFET counterparts.

Here, we have built a single-GFET harmonic transponder to illustrate the mixed modulation of RF signals. Figure 3a,b presents the circuit schematic and photograph of a PUF-based anticounterfeiting prototype, of which the GFET-based RF modulator is connected to a power management unit and receiving (R_x) and transmitting (T_x) coil antennas. This setup is compatible with near-field communication (NFC) and RFID technologies, and the overall size is comparable to that of a credit card. The challenge and response correspond to the RF monotone received by R_x antenna and the modulated signal transmitted through the T_x antenna. Notably, different types of modulation, including phase modulation, amplitude modulation, frequency modulation or a combination of these, can be achieved by applying different gate voltages (V_{GS}), as illustrated in Figure 3c; here, the drain bias voltage V_{DS} = 4 V, and the amplitude and carrier frequency of the input RF signal are v_{GS} = ± 0.5 V and f_0 = 20 kHz. Figure 3d–f presents the wireless measurement results for the amplitude modulation (V_{GS} = 0.5 V), frequency modulation (V_{GS} = −0.25 V), and phase modulation (V_{GS} = −0.6 V). We note that although V_{GS} is carefully chosen to achieve the optimum modulation characteristics, the output signal is more or less mixed with residual harmonics or experiences unwanted amplitude and/or phase modulations. In general, the GFET-based modulator provides a mixed modulation. The experimental results presented here show that the gate-tuned ambipolar electrical

https://doi.org/10.1021/acsnano.5c13119
ACS Nano 2026, 20, 421–431

characteristics of GFETs may unleash their potential to produce dynamically reconfigurable PUF keys and thus a large CRP space.

Encryption Quality of RF PUFs. In the following, we will evaluate the PUF performance and reconfigurability of single-GFET and dual-GFET modulators that act as the core component for the cryptographic key generation. The output RF signals shown in Figure 3 of the GFET modulators are digitized into 192 bit binary strings, following the analog-to-digital conversion process described in Supporting Information S2. Measured output signals from fabricated GFET modulators and the corresponding bitmaps are reported in Supporting Information S3. The PUF performance is typically evaluated through uniqueness, randomness, and reliability.[26] Uniqueness measures the degree of difference between responses generated by different PUF instances when queried by the same challenge. Randomness or uniformity indicates the degree of balance between occurrences of 1 bit or 0 bit states in the binary response of PUF, for which 1s and 0s must be equally distributed. Reliability refers to the consistency and stability of the response for a given challenge under different environmental conditions (e.g., temperature and humidity) and can also be verified by repeatedly measuring the response under identical conditions and confirming minimal variation among each measurement. Uniqueness is usually evaluated by the average inter-device Hamming distance (inter-HD) calculated between the response bitstrings of different PUF instances:[36]

$$\overline{\mathrm{HD}_{\mathrm{inter}}} = \frac{2}{N(N-1)} \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} \frac{\mathrm{HD}(R_i, R_j)}{L}, \tag{1}$$

where N stands for the total number of CRPs, L represents the length of the bit string, R_i and R_j refer to the i-th and j-th PUF key in the bitmap for a specific challenge. The ideal average inter-HD value should be 0.5. Figure 4a,b plots the histogram of average inter-HDs and the Pearson correlation coefficient (PCC) for the single-GFET modulators under the challenge V_{GS} = 0 V and f_0 = 10 kHz.[37] By fitting the histogram to a Gaussian distribution, we observed a peak centered at μ = 0.4643 with a standard deviation σ = 0.0913. The mean PCC value μ = 0.0458 ± 0.1869 also suggests that there is a very weak correlation between the different PUF responses. The uniqueness of the PUF system can also be illustrated by a pairwise HD map, which compares the response bit strings of all devices. Each entry on the map shows the inter-HD between two PUF instances, and all diagonal elements on the pairwise map (i.e., self-HD) are zero. Figure 4c presents the pairwise comparison of inter-HDs across 60 PUF devices, showing that the off-diagonal elements are close to 0.5. Figure 4d–f is similar to a–c, but for PUF keys generated by dual-GFET modulators. As seen in Figure 4d, PUF keys generated by dual-GFET modulators exhibit improved uniqueness (μ = 0.4972 ± 0.0547), compared to those obtained from single-GFET modulators. Additionally, the mean PCC value extracted from Figure 4e is only μ = −0.0012 ± 0.1122, revealing that there is almost no correlation between the output responses of dual-GFET modulators. Overall, our results show that RF PUFs based on GFET modulators can exhibit outstanding uniqueness. Moreover, dual-GFET modulators can produce more sophisticated and unpredictable RF responses than single-GFET counterparts, thereby showing further improvement in all uniqueness measurements. Figure 4g–i presents the evolution of the mean value and standard deviation of inter-HDs and the key size χ as a function of the sampling rate (the number of samples taken per 0.5 ms), which is associated with the number of extracted from the RF temporal characteristic.[38] The bit depth, which is the number of bits used to represent the amplitude of each data point in the temporal response, is fixed to 3 bits. The total key size is the product of bit depth and the sampling rate. Here, the sampling rate is varied until the mean value of the inter-HDs converges, in order to analyze the maximum key size (encoding capacity) and its uniqueness. The encoding capacity is given by c^{χ}, where c = 2 denoting "0" and "1", $\chi = \mu(1\text{-}\mu)/(\sigma^2)$ standing for the key size,[39,40] and μ and σ represent the mean and standard deviation of inter-HD, respectively. In this case, the encoding capacity converges at approximately 2^{83}, which may be further enhanced by increasing the number of GFET per modulator.[41]

Reliability, which measures how consistently the responses can be generated against varying operating conditions for a given challenge, can be evaluated by the average intra-HD:[36]

$$\overline{\mathrm{HD}_{\mathrm{intra}}} = \frac{1}{M} \sum_{p=1}^{M} \frac{\mathrm{HD}(R_i, R_{i,p})}{L}, \tag{2}$$

where M stands for the number of repeated measurements under the same environmental situations. In our work, one measurement is designated as the reference, and each additional repeated measurement (9 additional measurements in total) is compared against this reference outcome to produce one intra-HD value per repetition. The measured stacked transient responses under the same challenges imposed are shown in Supporting Information S4. Our intra-HD measurement results presented in Figure 4a,d demonstrate that both single- and dual-GFET PUF instances can display outstanding reliability, with the mean and standard deviation of intra-HDs close to the ideal value of zero (μ = 0.0575 ± 0.0176 for single-GFET PUF instances and μ = 0.0546 ± 0.0215 for dual-GFET counterparts).

Uniqueness and reliability are additionally characterized by false rejection rate (FRR) and false acceptance rate (FAR). FRR is defined as the probability that the verifier erroneously denies the authorized PUF instance, while FAR is defined as the probability that the verifier incorrectly accepts an unauthorized device (any PUF instance other than the selected one). FRR and FAR can be calculated as the fraction of intra-device comparisons with Hamming distances above the threshold (T) and as the fraction of inter-device comparisons whose Hamming distances fall below or equal to T, respectively. The two critical parameters can be expressed as[42]: FRR = $\Pr(\mathrm{HD}_{\mathrm{intra}} > T)$, FAR = $\Pr(\mathrm{HD}_{\mathrm{inter}} \leq T)$. The probability of cloning P_{clone} under Q independent attempts is given by[43,44] $P_{\mathrm{clone}} = 1 - (1 - \mathrm{FAR})^Q$; here, T = 0.121 and 0.178 are respectively used for the single-GFET and dual-GFET PUF instances to balance the usability and security (see S5 of Supporting Information for the zoomed-in view of inter- and intra-HDs). For the dual GFET-based PUF, FRR = 2.38×10^{-5}, FAR = 2.35×10^{-5}, equal error rate EER = 2.366×10^{-5}, and $P_{\mathrm{clone}} \approx 2.35 \times 10^{-3}$ under Q = 100 are obtained.[44] Such remarkably low FAR, FRR, and cloning probability observed in comparison to current PUF techniques,[42,45] further validating the high security and applicability of our RF PUF-based authentication approach.

We should emphasize that the proposed RF PUF can be reconfigurable, as PUF keys generated from the same instance

https://doi.org/10.1021/acsnano.5c13119
ACS Nano 2026, 20, 421–431

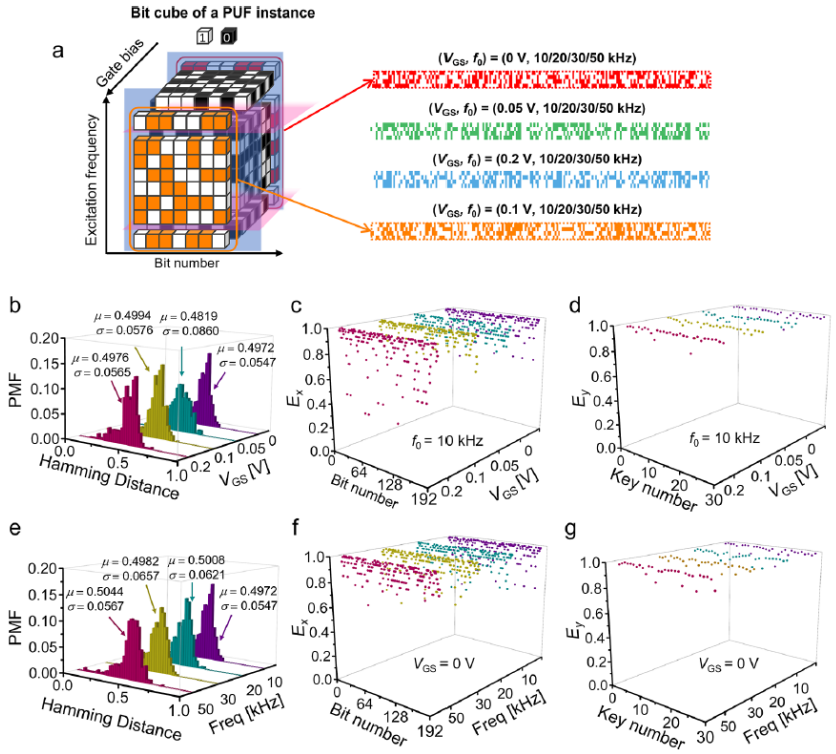


Figure 5. PUF reconfigurability and 3D bit cube. (a) 3D data structure (PUF cube) composed of binary encryption keys from a dual-GFET PUF instance, which can be reconfigured via gate bias voltages and the frequency of the interrogating RF signal. Evolution of (b) inter-HD histogram, (c) entropy E_x, and (d) entropy E_y of the two-dimensional bitmap at V_{GS} varies (here f_0 = 10 kHz). (e–g) are similar to (b–d), but for evaluations as a function of f_0 (here V_{GS} = 0 V) in (f) and (g), respectively.

can be dynamically refreshed by altering the carrier frequency of the input signal or the gate voltages. As illustrated in Figure 5a, each dual-GFET modulator can produce a 3-D "bit cube" formed by CRPs generated using different sets of (f_0, V_{GS}); here, V_{GS} is varied from 0 to 0.2 V, and f_0 is varied from 10 kHz to 50 kHz. Each row in the bit cube signifies a unique 192 bit PUF key that differs between horizontal and vertical cross sections, as can be seen in Figure 5a. Next, we will analyze the uniqueness and randomness of this reconfigurable PUF. Figure 5b plots histograms of the fractional inter-HDs for the dual-GFET RF PUFs operating at different gate voltages (V_{GS} = 0, 0.05, 0.1, and 0.2 V) and a fixed operating frequency (f_0 = 10 kHz); see Supporting Information S3 for the reconfigurable bitmaps corresponding to different operating states. We observe that in all cases, peaks of inter-HDs are centered at 0.5, with a ~5% standard deviation, demonstrating the excellent uniqueness of these reconfigurable PUF keys. Notably, the mean value μ = 0.494 ± 0.0637 can be obtained from inter-HDs of a bitmap that combines seven bitmaps obtained under different conditions (f_0, V_{GS}). Here, we also examine the randomness of the proposed RF PUF, which can be characterized by the Shannon entropy defined as follows:[36]

$$E_x = -[p_x \log_2 p_x + (1 - p_x)\log_2(1 - p_x)],$$
$$E_y = -[p_y \log_2 p_y + (1 - p_y)\log_2(1 - p_y)], \quad (3)$$

where p_x and p_y are probabilities of identifying "1" on the x-axis and y-axis of a bitmap, respectively. Figure 5c,d presents the distributions of E_x and E_y at f_0 = 10 kHz under different gate-bias conditions. It can be seen that when the PUF is reconfigured, E_x and E_y remain close to the ideal value of unity, showing great randomness and reconfigurability. Remarkably, the average entropy is found to $(\overline{E_x}, \overline{E_y})$ = (0.9398, 0.9826) Figure 5e plots histograms of inter-HDs for the dual-GFET RF PUFs at V_{GS} = 0 V and different operating frequencies f_0 = 10, 20, 30, 50 kHz. Our results indicate that, regardless of operating frequency, the average inter-Hamming distance remains near 0.5. The mean value of inter-HDs for the merged bitmap (which consists of bitmaps at different reconfigurable states) is μ = 0.497 ± 0.0628, indicating the excellent unpredictability, stability, and reconfigurability of the proposed RF PUF. Figure 5f,g shows the evaluation of E_x and E_y as f_0 increases from 10 kHz to 50 kHz, showing that near-unity entropy can be achieved with average entropy $(\overline{E_x}, \overline{E_y})$ = (0.9406, 0.9855). The randomness can also be further evaluated using the National Institute of Standards and Technology (NIST) randomness test suite. The reconfigurable dual-GFET RF PUF can pass all the statistical tests in the NIST test suite, and all NIST subtests are satisfied by both pass-rate and p-value uniformity criteria; the detailed analysis and results for the NIST randomness test can be found in Supporting Information S6. Our randomness test results

https://doi.org/10.1021/acsnano.5c13119
ACS Nano 2026, 20, 421–431

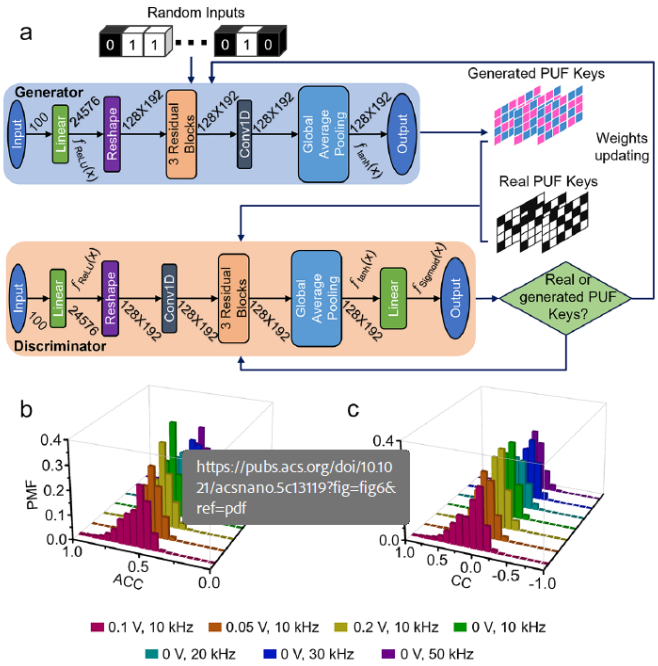


Figure 6. Resilience of PUF against machine learning-based modeling attacks. (a) Schematic of the GAN, comprising a generator and a discriminator. For the modeling attacks, 5000 CRPs were generated through simulation, of which 4000 were used for training and the remaining 1000 were used for testing. Due to the large number of CRPs, probability mass functions (PMFs) are employed to better illustrate the results. Evolution of (b) ACC histograms and (c) CC histograms as PUF keys are reconfigured, demonstrating the system's strong resilience against machine learning-based modeling attacks.

indicate that the GFET-based RF PUF can exhibit high unpredictability and reconfigurability, thus ensuring strong cryptographic strength in wireless identification and authentication.

Resilience Evaluation of GFET-Based RF PUF against Adversarial Attacks. The rapid advancement of artificial intelligence and machine learning has significantly enhanced the ability to break large encryption keys, including those generated by digital PUF instances. Machine learning-aided password-guessing tools have demonstrated a clear advantage over traditional methods, underscoring the need for alternative hardware-based security solutions.[46] Particularly, most silicon-based PUFs with insufficient randomness and uniqueness have been found to be vulnerable to those modeling attacks based on logistic regression algorithms and GAN models.[46] To evaluate the robustness of the proposed PUFs against machine learning-based modeling attacks, we have conducted simulation experiments exploiting PassGAN model attacks on the GFET-based RF PUFs, as shown in Figure 6a.[47,48] The detailed architecture of the PassGAN model is presented in Supporting Information S7. The general structure of PassGAN, as illustrated in Figure S9, consists of a generator and discriminator network, both utilizing residual blocks. The generator, composed of four linear layers with hyperbolic tangent activation functions, attempts to generate fake PUF keys that resemble real ones, while the three-layer discriminator network distinguishes between real and generated keys. Training occurs over 1000 epochs using the AdamW optimizer, with the discriminator and generator trained at learning rates of 0.001 and 0.0001, respectively. Input vectors of length 100 are fed into the generator, producing CRPs, which are then binarized based on their sign bits. In our simulation experiments, 5000 dual-GFET CRPs were randomly generated, with their V_{cnp}, carrier mobilities, and impurity concentrations following the Gaussian distributions depicted in Figure 1. The physics-based compact model was integrated with the circuit simulation to compute the output RF responses under different input challenges (See Supporting Information S1 for details of the physics-based compact model for GFETs).[26] For training, 4000 out of the 5000 PUF keys were used to train PassGAN, while the remaining 1000 were reserved for testing its attack efficacy. Figure 6b,c presents the PassGAN-based modeling attack results. Instead of conventional silicon based PUFs attacked by GANs, which typically have a mean accuracy (ACC) of over 90%,[49,50] our PUFs with various V_{GS} and f_0 values (V_{GS} = 0 V, f_0 = 10 kHz; V_{GS} = 0.05 V, f_0 = 10 kHz; V_{GS} = 0.1 V, f_0 = 10 kHz; V_{GS} = 0.2 V, f_0 = 10 kHz; V_{GS} = 0 V, f_0 = 20 kHz; V_{GS} = 0 V, f_0 = 30 kHz; V_{GS} = 0 V, f_0 = 50 kHz) achieved a mean ACC close to 50% and a correlation coefficient (CC) near 0. The significantly reduced ACC and CC values clearly demonstrate the improved robustness of the proposed PUF against PassGAN. Detailed results of means and standard deviations for different reconfigurable states are summarized in Supporting Information S7. The strong resistance of our dual-GFET RF PUF against the modeling attack highlights the effectiveness of our approach in mitigating AI-driven security threats. Despite these optimizations, the reconfigurable dual-GFET RF PUF

https://doi.org/10.1021/acsnano.5c13119
ACS Nano 2026, 20, 421−431

maintained high resiliency against the modeling attacks, demonstrating that the reconfigurable RF PUF can effectively withstand AI-aided/based adversarial attacks.

In short, we have compared the performance of our GFET-based RF PUF with other PUF techniques in terms of randomness, uniqueness, encoding capacity, reconfigurability, and resilience to AI-assisted attacks (See S8 of Supporting Information for the detailed comparison). Conventional silicon-based PUF techniques (e.g., SRAM PUF and RO PUF[45,51]) offer good uniqueness and reconfigurability, but suffer from low encoding capacity and lack reported ML-attack evaluations. Optical PUFs based on 2D nanomaterials, such as graphene Raman PUF and MoS_2 Raman PUF, although exhibiting large encoding capacity, require bulky and costly experimental setups and lack reconfigurability.[52,53] The proposed GFET PUF offers on-device and on-demand reconfigurability tuned via carrier frequency and gate bias, along with low-latency generation of RF PUFs via a mixed modulation, resulting in a compact and lightweight design compatible with RF front ends. Such advantages are not found in graphene-based straintronic PUFs and memory PUFs.[19,26] Moreover, the proposed RF PUFs also exhibit robustness against advanced ML attacks (PassGan model), further demonstrating their applicability to wireless identification and authentication. In short, the proposed GFET-based PUF simultaneously offers high encoding capacity, reconfigurability, resilience against AI-aided attacks, compactness, cost-effectiveness, and compatibility with front-end RF circuits and wireless systems. On the other hand, conventional PUFs usually fail in one or more of these PUF specifications.

CONCLUSIONS

We have proposed a new class of RF PUF that utilizes the virtue of the GFET modulators to generate unpredictable and unclonable mixed modulations with exceptional reconfigurability. We have experimentally demonstrated that this PUF can possess remarkable encryption quality in terms of uniqueness, randomness, and reliability when reconfigured to different operating states. Moreover, the PUF performance metrics can be enhanced by the dual-GFET device architecture, which inherently outputs more complicated and randomized signal waveforms. We have conducted simulation experiments to demonstrate that this PUF exhibits excellent resilience against machine learning-based modeling attacks based on generative adversarial networks. We should emphasize that the proposed RF PUF can be readily implemented and compatible with current wireless identification and communication systems since the input challenges and output responses are encoded primarily in radio signals. Our results may open a new avenue toward reliable and scalable physical security primitives that address emerging security challenges in wireless systems and networks.

METHODS

Fabrication of GFETs. The graphene layer was grown on the copper foil via CVD. A thin layer of poly(methyl methacrylate) (PMMA) was first coated on the graphene/Cu foil and then baked on a hot plate at 60 °C for 10 min. This PMMA layer served as a support layer to prevent graphene from curling up and breaking up during the Cu etching process. $FeCl_3$ was used as an etchant to etch out Cu foil underneath the graphene monolayer. After the Cu foil was fully etched, the PMMA/graphene film was rinsed using the deionized (DI) water to remove the residue of $FeCl_3$. Subsequently, the PMMA/graphene film was scooped up by the target substrate and baked on a hot plate at 50 °C for 30 min. Finally, the sample was soaked in the MICROPOSIT Remover 1165 for 6 h to remove the PMMA. The p-doped silicon (Si) substrates have a 90 nm thermal oxide layer as the dielectric insulator between doped Si and graphene. Maskless photolithography was conducted by the MLA150 Maskless Aligner to pattern graphene and electrodes. First, a layer of S1813 resist was coated on the graphene/Si substrate. After the exposure of the designed pattern and development of resist, the unwanted area of graphene was exposed to the environment and was then etched with oxygen plasma. The resist was removed by soaking the graphene/Si substrate in the MICROPOSIT Remover 1165, leaving only the patterned graphene on the Si substrate. Both source and drain electrodes are made of gold (Au) with a thickness of 50 nm. Maskless photolithography was implemented to define the geometry of source and drain electrodes, following the metal deposition and lift-off processes. The same lithographic patterning procedures were applied to make the aluminum (Al) gate electrode with a thickness of 10 nm. Both Au and Al films were deposited using the e-beam evaporation at a deposition rate of 1 Å/s. Following the deposition and lift-off of the Al gate, the devices are exposed to ambient conditions for 10 days, which allows for the natural formation of native oxide (i.e., gate dielectric) between the Al gate and the graphene surface.

Design of NFC Tag Equipped with the GFET-Based RF PUF. The diagram of the NFC tag shown in Figure 3a consists of three buffer stages and two bias networks. The receiving and transmitting coils are WE-WPCC wireless power transfer coils from Würth Electronics. The proposed system is powered up by 8 solid-state batteries from TDK, and the Power management circuit handles the necessary power distribution and battery protection. Then a stable reference voltage is generated by the REF5020 voltage reference from Texas Instrument. The reference voltage signal is later fed to the resistive voltage divider, which is controlled by two solid-state relays driven by two TMAG5231 hall effect switches. By switching between the on and off states of the two solid-state relays, four different gate bias voltages are generated by controlling the Hall effect switch-driven relays through a magnetic field applied by the reader. At the same time, the drain bias voltage is generated through a resistor divider following a voltage buffer, which is achieved by the LME49720 operational amplifier from Texas Instrument. The Input signal is also buffered with 10 V/V gain with LME49720, which enhances the system sensibility. The gate and drain bias circuitries are based on the "bias-Tee" network formed by passive lumped elements. The gate bias provides a DC offset to the input AC signal ($v_{GS} = \pm 0.5$ V), and the drain bias ($V_{DS} = 4$ V) ensures proper voltage or current under certain operating conditions.

ASSOCIATED CONTENT

Supporting Information

The Supporting Information is available free of charge at https://pubs.acs.org/doi/10.1021/acsnano.5c13119.

Transfer characteristics of top-gated GFETs; AFM/KPFM analyses with CPD/work function statistics; empirical transport model and parameter extraction; schematics of GFET PUF system level application; time-domain responses and bitmap generation mapping with reconfigurable bitmaps for 30 devices across gate biases and carrier frequencies; reliability (intra-HD) measurements; evaluation of FRR/FAR and EER; NIST randomness test, including the analysis of p-values, pass rates, confidence intervals, and *p*-value uniformity; PassGAN attack model and ACC/CC results; comparison table with other state-of-the-art PUFs; wireless readout setup of the GFET PUF keys (PDF)

https://doi.org/10.1021/acsnano.5c13119
ACS Nano 2026, 20, 421−431

AUTHOR INFORMATION

Corresponding Authors

Ahmet Enis Cetin − *Department of Electrical and Computer Engineering, University of Illinois Chicago, Chicago, Illinois 60607, United States*; Email: aecyy@uic.edu

Pai-Yen Chen − *Department of Electrical and Computer Engineering, University of Illinois Chicago, Chicago, Illinois 60607, United States*; orcid.org/0000-0002-8112-8457; Email: pychen@uic.edu

Authors

Yichong Ren − *Department of Electrical and Computer Engineering, University of Illinois Chicago, Chicago, Illinois 60607, United States*; orcid.org/0009-0005-1662-3952

Chia-Heng Sun − *Department of Electrical and Computer Engineering, University of Illinois Chicago, Chicago, Illinois 60607, United States*

Mohan De Silva − *Department of Physics and Astronomy, Wayne State University, Detroit, Michigan 48201, United States*

Hongyi Pan − *Feinberg School of Medicine, Northwestern University, Chicago, Illinois 60611, United States*

Xuecong Nie − *Department of Electrical and Computer Engineering, University of Illinois Chicago, Chicago, Illinois 60607, United States*

Emadeldeen Hamdan − *Department of Electrical and Computer Engineering, University of Illinois Chicago, Chicago, Illinois 60607, United States*

Zhixian Zhou − *Department of Physics and Astronomy, Wayne State University, Detroit, Michigan 48201, United States*; orcid.org/0000-0002-9228-4260

Complete contact information is available at: https://pubs.acs.org/10.1021/acsnano.5c13119

Author Contributions

Y.Ren, C.H.Sun, M. De Silva, X. Nie, and Z. Zhou designed, manufactured, and characterized graphene field-effect transistors and PUF instances. H.Pan and E. Hamdan performed the machine learning-based modeling attacks. Y.Ren, C.H.Sun, X. Nie, and P.Y.Chen conceived the concept and the experiment. P.Y.Chen, and A.E.Cetin developed the concept and planned and directed the research. Y.Ren, P.Y.Chen, and A.E.Cetin wrote the manuscript.

Funding

A.E.Cetin acknowledges the financial support from NSF under Grant 2229659 and in part from DOE under Grant DE-SC0023715. P.Y.Chen would like to thank National Science Foundation under Grant ECCS-CCSS 2229659. M.D.S. and Z.Z. acknowledge the support of NSF under Grant ECCS-2210861.

Notes

The authors declare no competing financial interest.

ACKNOWLEDGMENTS

This work has been supported by the Device fabrication and measurement was carried out at the Nanotechnology Core Facility at the University of Illinois at Chicago and at the Nano Fabrication Service Core (nFab) at the Wayne State University.

REFERENCES

(1) Miloslavskaya, N.; Tolstoy, A. Internet of Things: Information Security Challenges and Solutions. *Cluster Comput* **2019**, *22* (1), 103−119.

(2) Hu, W.; Chang, C.-H.; Sengupta, A.; Bhunia, S.; Kastner, R.; Li, H. An Overview of Hardware Security and Trust: Threats, Countermeasures, and Design Tools. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2021**, *40* (6), 1010−1038.

(3) Nagata, M.; Miki, T.; Miura, N. Physical Attack Protection Techniques for IC Chip Level Hardware Security. *IEEE Trans. VLSI Syst.* **2022**, *30* (1), 5−14.

(4) Akter, S.; Khalil, K.; Bayoumi, M. A Survey on Hardware Security: Current Trends and Challenges. *IEEE Access* **2023**, *11*, 77543−77565.

(5) Khadka, G.; Ray, B.; Karmakar, N. C.; Choi, J. Physical-Layer Detection and Security of Printed Chipless RFID Tag for Internet of Things Applications. *IEEE Internet Things J.* **2022**, *9* (17), 15714−15724.

(6) Pappu, R.; Recht, B.; Taylor, J.; Gershenfeld, N. Physical One-Way Functions. *Science* **2002**, *297* (5589), 2026−2030.

(7) Gao, Y.; Al-Sarawi, S. F.; Abbott, D. Physical Unclonable Functions. *Nat. Electron* **2020**, *3* (2), 81−91.

(8) Holcomb, D. E.; Burleson, W. P.; Fu, K. Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers. *IEEE Trans. Comput.* **2009**, *58* (9), 1198−1210.

(9) Shifman, Y.; Miller, A.; Keren, O.; Weizmann, Y.; Shor, J. A Method to Improve Reliability in a 65-Nm SRAM PUF Array. *IEEE Solid-State Circuits Lett.* **2018**, *1* (6), 138−141.

(10) Wali, A.; Das, S. Hardware and Information Security Primitives Based on 2D Materials and Devices. *Adv. Mater.* **2023**, *35* (18), 2205365.

(11) Chatterjee, U.; Chakraborty, R. S.; Mukhopadhyay, D. A PUF-Based Secure Communication Protocol for IoT. *ACM Trans. Embed. Comput. Syst.* **2017**, *16* (3), 1−25.

(12) Kang, M.; Kim, J.; Jang, B.; Chae, Y.; Kim, J.-H.; Ahn, J.-H. Graphene-Based Three-Dimensional Capacitive Touch Sensor for Wearable Electronics. *ACS Nano* **2017**, *11* (8), 7950−7957.

(13) Zhong, D.; Liu, J.; Xiao, M.; Xie, Y.; Shi, H.; Liu, L.; Zhao, C.; Ding, L.; Peng, L.-M.; Zhang, Z. Twin Physically Unclonable Functions Based on Aligned Carbon Nanotube Arrays. *Nat. Electron* **2022**, *5* (7), 424−432.

(14) Wang, H.; Wu, Y.; Cong, C.; Shang, J.; Yu, T. Hysteresis of Electronic Transport in Graphene Transistors. *ACS Nano* **2010**, *4* (12), 7221−7228.

(15) Van Geest, E. P.; Shakouri, K.; Fu, W.; Robert, V.; Tudor, V.; Bonnet, S.; Schneider, G. F. Contactless Spin Switch Sensing by Chemo-Electric Gating of Graphene. *Adv. Mater.* **2020**, *32* (10), 1903575.

(16) Li, Z.-F.; Zhang, H.; Liu, Q.; Sun, L.; Stanciu, L.; Xie, J. Fabrication of High-Surface-Area Graphene/Polyaniline Nanocomposites and Their Application in Supercapacitors. *ACS Appl. Mater. Interfaces* **2013**, *5* (7), 2685−2691.

(17) Long, H.; Harley-Trochimczyk, A.; Pham, T.; Tang, Z.; Shi, T.; Zettl, A.; Carraro, C.; Worsley, M. A.; Maboudian, R. High Surface Area MoS_2/Graphene Hybrid Aerogel for Ultrasensitive NO_2 Detection. *Adv. Funct Materials* **2016**, *26* (28), 5158−5165.

(18) Xiang, H.; Chien, Y.-C.; Shi, Y.; Ang, K.-W. Application of 2D Materials in Hardware Security for Internet-of-Things: Progress and Perspective. *Small Structures* **2022**, *3* (8), 2200060.

(19) Ghosh, S.; Zheng, Y.; Radhakrishnan, S. S.; Schranghamer, T. F.; Das, S. A Graphene-Based Straintronic Physically Unclonable Function. *Nano Lett.* **2023**, *23* (11), 5171−5179.

(20) Wang, H.; Hsu, A.; Wu, J.; Kong, J.; Palacios, T. Graphene-Based Ambipolar RF Mixers. *IEEE Electron Device Lett.* **2010**, *31* (9), 906−908.

(21) Liao, L.; Duan, X. Graphene for Radio Frequency Electronics. *Mater. Today* **2012**, *15* (7−8), 328−338.

(22) Lee, S.; Lee, K.; Liu, C.-H.; Kulkarni, G. S.; Zhong, Z. Flexible and Transparent All-Graphene Circuits for Quaternary Digital Modulations. *Nat. Commun.* **2012**, *3* (1), 1018.
(23) Chen, H.-Y.; Appenzeller, J. Graphene-Based Frequency Tripler. *Nano Lett.* **2012**, *12* (4), 2067−2070.
(24) Huang, H.; Tao, L.; Liu, F.; Ji, L.; Hu, Y.; Cheng, M. M.-C.; Chen, P.-Y.; Akinwande, D. Chemical-Sensitive Graphene Modulator with a Memory Effect for Internet-of-Things Applications. *Microsyst Nanoeng* **2016**, *2* (1), 16018.
(25) Hajizadegan, M.; Sakhdari, M.; Zhu, L.; Cui, Q.; Huang, H.; Cheng, M. M. C.; Hung, J. C. H.; Chen, P.-Y. Graphene Sensing Modulator: Toward Low-Noise, Self-Powered Wireless Microsensors. *IEEE Sensors J.* **2017**, *17* (22), 7239−7247.
(26) Dodda, A.; Subbulakshmi Radhakrishnan, S.; Schranghamer, T. F.; Buzzell, D.; Sengupta, P.; Das, S. Graphene-Based Physically Unclonable Functions That Are Reconfigurable and Resilient to Machine Learning Attacks. *Nat. Electron* **2021**, *4* (5), 364−374.
(27) Adam, S.; Hwang, E. H.; Galitski, V. M.; Das Sarma, S. A Self-Consistent Theory for Graphene Transport. *Proc. Natl. Acad. Sci. U.S.A.* **2007**, *104* (47), 18392−18397.
(28) Xia, J.; Chen, F.; Li, J.; Tao, N. Measurement of the Quantum Capacitance of Graphene. *Nat. Nanotechnol.* **2009**, *4* (8), 505−509.
(29) Lee, T.; Mas'ud, F. A.; Kim, M. J.; Rho, H. Spatially Resolved Raman Spectroscopy of Defects, Strains, and Strain Fluctuations in Domain Structures of Monolayer Graphene. *Sci. Rep.* **2017**, *7* (1), 16681.
(30) Sul, O.; Kim, K.; Choi, E.; Kil, J.; Park, W.; Lee, S.-B. Reduction of Hole Doping of Chemical Vapor Deposition Grown Graphene by Photoresist Selection and Thermal Treatment. *Nanotechnology* **2016**, *27* (50), 505205.
(31) Schmoldt, A.; Benthe, H. F.; Haberland, G. Digitoxin Metabolism by Rat Liver Microsomes. *Biochem. Pharmacol.* **1975**, *24* (17), 1639−1641.
(32) Das, A.; Pisana, S.; Chakraborty, B.; Piscanec, S.; Saha, S. K.; Waghmare, U. V.; Novoselov, K. S.; Krishnamurthy, H. R.; Geim, A. K.; Ferrari, A. C.; Sood, A. K. Monitoring Dopants by Raman Scattering in an Electrochemically Top-Gated Graphene Transistor. *Nat. Nanotechnol.* **2008**, *3* (4), 210−215.
(33) Beams, R.; Cançado, L. G.; Jorio, A.; Vamivakas, A. N.; Novotny, L. Tip-Enhanced Raman Mapping of Local Strain in Graphene. *Nanotechnology* **2015**, *26* (17), 175702.
(34) Merino, J. P.; Brosel-Oliu, S.; Rius, G.; Illa, X.; Sulleiro, M. V.; Del Corro, E.; Masvidal-Codina, E.; Bonaccini Calia, A.; Garrido, J. A.; Villa, R.; Guimerà-Brunet, A.; Prato, M.; Criado, A.; Prats-Alfonso, E. Ethanol Solvation of Polymer Residues in Graphene Solution-Gated Field Effect Transistors. *ACS Sustainable Chem. Eng.* **2024**, *12* (24), 9133−9143.
(35) No, Y.-S.; Choi, H. K.; Kim, J.-S.; Kim, H.; Yu, Y.-J.; Choi, C.-G.; Choi, J. S. Layer Number Identification of CVD-Grown Multilayer Graphene Using Si Peak Analysis. *Sci. Rep.* **2018**, *8* (1), 571.
(36) Yang, M.; Zhu, L.; Zhong, Q.; El-Ganainy, R.; Chen, P.-Y. Spectral Sensitivity near Exceptional Points as a Resource for Hardware Encryption. *Nat. Commun.* **2023**, *14* (1), 1145.
(37) Benesty, J.; Chen, J.; Huang, Y.; Cohen, I. *Pearson Correlation Coefficient*; Springer Topics in Signal Processing; Springer: Berlin, Heidelberg, 2009; Vol. *2*, pp 1−4.
(38) Leem, J. W.; Kim, M. S.; Choi, S. H.; Kim, S.-R.; Kim, S.-W.; Song, Y. M.; Young, R. J.; Kim, Y. L. Edible Unclonable Functions. *Nat. Commun.* **2020**, *11* (1), 328.
(39) Hu, Z.; Comeras, J. M. M. L.; Park, H.; Tang, J.; Afzali, A.; Tulevski, G. S.; Hannon, J. B.; Liehr, M.; Han, S.-J. Physically Unclonable Cryptographic Primitives Using Self-Assembled Carbon Nanotubes. *Nat. Nanotechnol.* **2016**, *11* (6), 559−565.
(40) Ren, Y.; Yang, M.; Pan, H.; Farhat, M.; Enis Cetin, A.; Chen, P.-Y. *PT* Symmetry-Enabled Physically Unclonable Functions for Anti-Counterfeiting RF Tags. *IEEE Trans. Antennas Propagat.* **2024**, *72* (6), 5129−5140.
(41) Hajizadegan, M.; Sakhdari, M.; Abbasi, S.; Chen, P.-Y. Machine Learning Assisted Multi-Functional Graphene-Based Harmonic Sensors. *IEEE Sensors J.* **2021**, *21* (6), 8333−8340.
(42) Gao, Y.; Ma, H.; Abbott, D.; Al-Sarawi, S. F. PUF Sensor: Exploiting PUF Unreliability for Secure Wireless Sensing. *IEEE Trans. Circuits Syst. I* **2017**, *64* (9), 2532−2543.
(43) Quinn, G. W.; Grother, P.; Matey, J. *IREX IX Part One, Performance of Iris Recognition Algorithms; NIST IR 8207*; National Institute of Standards and Technology: Gaithersburg, MD, 2018; p NIST IR 8207.
(44) Daugman, J. How Iris Recognition Works. In *The Essential Guide to Image Processing*; Elsevier, 2009; pp 715−739.
(45) Pham, V. K.; Ngo, C. T.; Nam, J.-W.; Hong, J.-P. A Reconfigurable SRAM CRP PUF with High Reliability and Randomness. *Electronics* **2024**, *13* (2), 309.
(46) Delvaux, J. Machine-Learning Attacks on PolyPUFs, OB-PUFs, RPUFs, LHS-PUFs, and PUF−FSMs. *IEEE Trans.Inform.Forensic Secur.* **2019**, *14* (8), 2043−2058.
(47) Hitaj, B.; Gasti, P.; Ateniese, G.; Perez-Cruz, F. PassGAN: A Deep Learning Approach for Password Guessing. In *Applied Cryptography and Network Security*; Deng, R. H., Gauthier-Umaña, V., Ochoa, M., Yung, M., Eds.; Springer International Publishing: Cham, 2019; Vol. *11464*, pp 217−237.
(48) Fauzi, M. A.; Yang, B.; Martiri, E. PassGAN Based Honeywords System for Machine-Generated Passwords Database. *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*; IEEE, Baltimore, MD, USA 2020, 214−220.
(49) Rührmair, U.; Sehnke, F.; Sölter, J.; Dror, G.; Devadas, S.; Schmidhuber, J. Modeling Attacks on Physical Unclonable Functions. *Proceedings of the 17th ACM conference on Computer and communications security*; ACM, Chicago Illinois USA 2010, 237−249.
(50) Ruhrmair, U.; Solter, J.; Sehnke, F.; Xu, X.; Mahmoud, A.; Stoyanova, V.; Dror, G.; Schmidhuber, J.; Burleson, W.; Devadas, S. PUF Modeling Attacks on Simulated and Silicon Data. *IEEE Trans.Inform.Forensic Secur* **2013**, *8* (11), 1876−1891.
(51) Della Sala, R.; Bellizia, D.; Scotti, G. Unveiling the True Power of the Latched Ring Oscillator for a Unified PUF and TRNG Architecture. *IEEE Trans. VLSI Syst.* **2024**, *32* (12), 2403−2407.
(52) Alharbi, A.; Armstrong, D.; Alharbi, S.; Shahrjerdi, D. Physically Unclonable Cryptographic Primitives by Chemical Vapor Deposition of Layered MoS_2. *ACS Nano* **2017**, *11* (12), 12772−12779.
(53) Lee, S.; Pekdemir, S.; Kayaci, N.; Kalay, M.; Onses, M. S.; Ye, J. Graphene-Based Physically Unclonable Functions with Dual Source of Randomness. *ACS Appl. Mater. Interfaces* **2023**, *15* (28), 33878−33889.

https://doi.org/10.1021/acsnano.5c13119
ACS Nano 2026, 20, 421−431