NANO LETTERS

pubs.acs.org/NanoLett

Letter

A Graphene-Based Straintronic Physically Unclonable Function

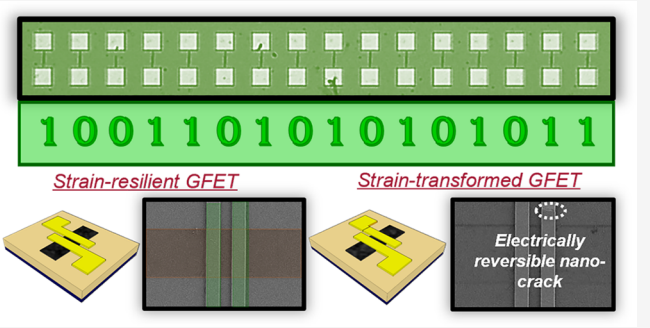
Subir Ghosh, Yikai Zheng, Shiva Subbulakshmi Radhakrishnan, Thomas F Schranghamer, and Saptarshi Das*

Cite This: *Nano Lett.* 2023, 23, 5171−5179

Read Online

ACCESS | Metrics & More | Article Recommendations | Supporting Information

ABSTRACT: Physically unclonable functions (PUFs) are an integral part of modern-day hardware security. Various types of PUFs already exist, including optical, electronic, and magnetic PUFs. Here, we introduce a novel straintronic PUF (SPUF) by exploiting strain-induced reversible cracking in the contact microstructures of graphene field-effect transistors (GFETs). We found that strain cycling in GFETs with a piezoelectric gate stack and high-tensile-strength metal contacts can lead to an abrupt transition in some GFET transfer characteristics, whereas other GFETs remain resilient to strain cycling. Strain sensitive GFETs show colossal ON/OFF current ratios >10^7, whereas strain-resilient GFETs show ON/OFF current ratios <10. We fabricated a total of 25 SPUFs, each comprising 16 GFETs, and found near-ideal performance. SPUFs also demonstrated resilience to regression-based machine learning (ML) attacks in addition to supply voltage and temporal stability. Our findings highlight the opportunities for emerging straintronic devices in addressing some of the critical needs of the microelectronics industry.



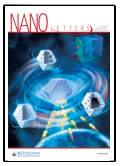
KEYWORDS: *PUF, Straintronics, Graphene, PZT*

Hardware security is a pressing need for Internet of Things (IoT) edge devices,[1−6] and physically unclonable functions (PUFs) are relatively low-cost, low-power, and low-overhead hardware security solutions. PUFs exploit manufacturing process variation in devices and their interactions with external stimuli to generate unique and unpredictable digital signatures, which can be used for hardware authentication.[1,7−10] While silicon PUFs are the most prevalent in the semiconductor industry, their low entropy resulting from poor device-to-device variation and high power consumption owing to their need for complex error correcting peripheral circuits have led to the investigation of alternative PUF formats,[9,11] including nanowire PUFs,[12] memristive PUFs,[13,14] graphene PUFs,[15] CNT PUFs,[16] polymer PUFs,[17] and even optical[18] and biological PUFs.[19,20]

Put simply, a PUF is a one-way hardware function, i.e., it is easy to generate a response from a PUF by applying an external stimulus, known as the challenge, but it is difficult to predict the physical microstructure that generates the response. The challenge can be current, voltage, illumination, temperature, strain, vibration, etc., and the response can be voltage, current, power, image, etc. Each PUF must be associated with one or more unique challenge-response pairs (CRPs); these must differ among different PUFs but must repeat every time the same stimulus is applied to the same PUF. All silicon-based PUFs and most emerging nanomaterial-based PUFs rely on device-to-device variation in response to current/voltage stimuli to generate CRPs. However, such device-to-device variations are often insufficient for direct translation of CRPs into digital keys, necessitating the use of peripheral circuits such as analog-to-digital converters to obtain a digital signature. This naturally leads to significant area and energy overhead.

Here, we introduce a straintronic PUF (SPUF) by exploiting the random formation of nanocracks at metal electrodes in graphene field-effect transistors (GFETs) fabricated on a piezoelectric gate stack with high-tensile-strength source/drain metal contacts. We have found that, when GFETs are subjected to strain cycling by sweeping the back-gate voltage, electrically reversible nanocracks can form at the metal electrodes in some GFETs whereas other GFETs remain resilient to the same process. The GFETs that undergo strain-induced transition show colossal ON/OFF current ratios greater than 10^7 while strain-resilient GFETs continue to show ON/OFF current ratios <10. The crack formation occurs randomly in some of the metal contacts due to nonuniform strain distribution across the piezoelectric domains. Indeed, the formation of nanocracks is not directly caused by graphene;

Received: March 25, 2023
Revised: May 11, 2023
Published: May 22, 2023



https://doi.org/10.1021/acs.nanolett.3c01145
Nano Lett. 2023, 23, 5171−5179

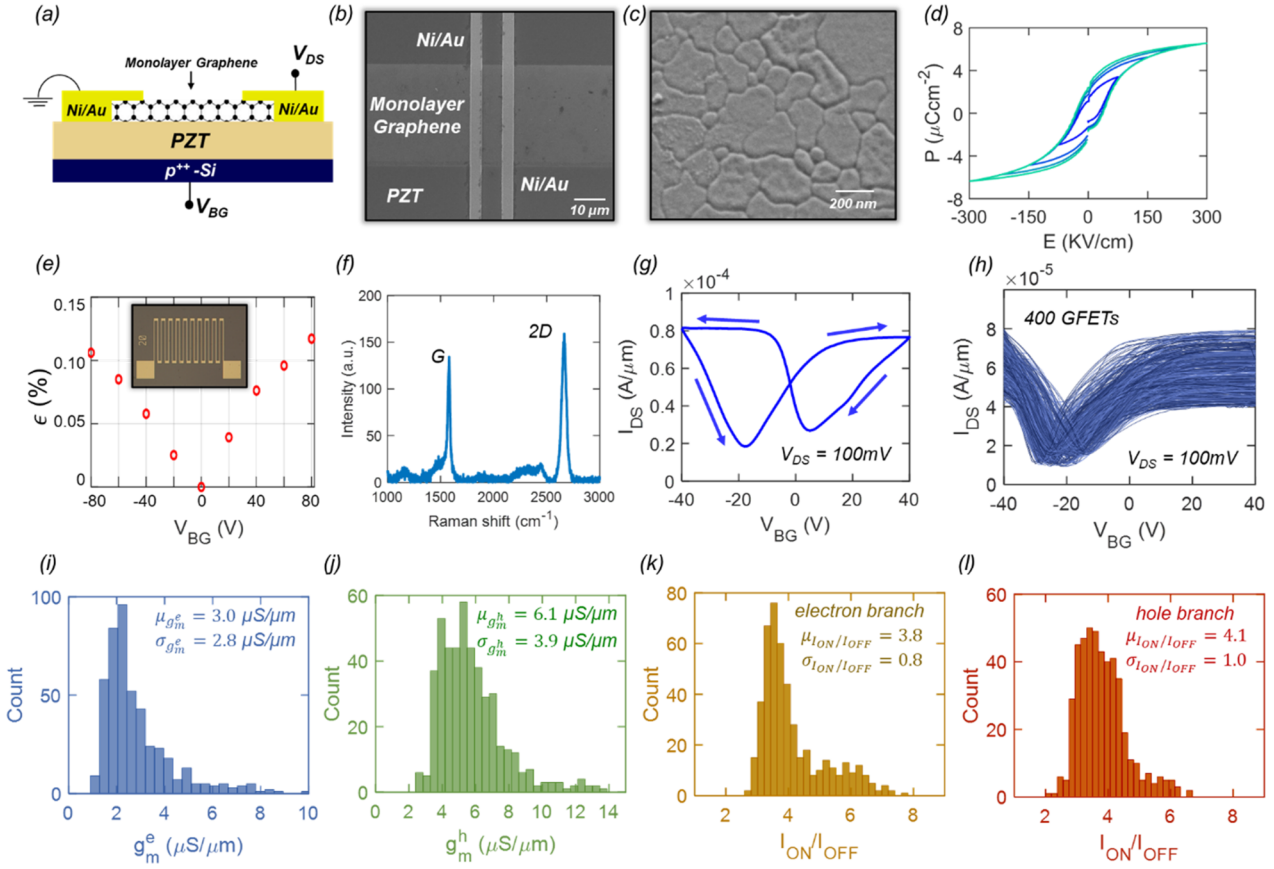


Figure 1. Fabrication and characterization of piezoelectric-gated straintronic graphene field-effect transistors (GFETs). The (a) schematic and (b) scanning electron microscope (SEM) image of the straintronic GFET. A 2 μm thick film of piezoelectric lead zirconate titanate (PZT) grown using the sol-gel technique on a p^{++}-Si substrate was used as the global back-gate. (c) A top-view SEM image of the PZT film shows columnar grains with submicron dimensions. (d) Nested hysteresis loops showing the polarization (P) versus electric field (E) for the PZT film using a metal-insulator-metal (MIM) structure. A remnant polarization of 0.2 C/m^2 and a coercive field of 2 × 10^6 V/m were extracted. (e) Strain as a function of bias across the PZT film extracted by measuring the resistance change across a Ni strain gauge (inset). (f) Raman spectra of a graphene channel obtained using a 532 nm laser. Two characteristic peaks at around 1600 and 2700 cm^{-1} confirm monolayer graphene. (g) Dual sweep transfer characteristics, i.e., source-to-drain current (I_{DS}) versus back-gate voltage (V_{BG}), of a representative as-fabricated GFET, measured under ambient pressure and room temperature at a source-to-drain voltage (V_{DS}) of 100 mV. (h) Device-to-device variation in the transfer characteristics of 400 as-fabricated GFETs. Distribution of peak transconductance for (i) electron and (j) hole branches and the maximum on/off current ratio for (k) electron and (l) hole branches across these 400 GFETs.

however, the SPUF platform with GFETs can provide additional functionalities such as sensing and storage owing to the use of graphene. Finally, unlike many existing and emerging PUFs, the SPUF largely eliminates the need for complex peripheral circuits owing to the large difference in the readout current between strain-transformed and strain-resilient GFETs. To test the strength of the SPUF platform, we fabricated a total of 25 SPUFs, each comprising 16 GFETs, and evaluated some of the key metrics such as entropy, uniformity, Hamming distance, and correlation coefficient. Remarkably, our SPUFs demonstrated near-ideal performance. Supply voltage and temporal stability for the SPUFs were also investigated. SPUFs were also found to be resilient to regression-based machine learning attacks.

FABRICATION AND CHARACTERIZATION OF GFETS ON A PIEZOELECTRIC GATE STACK

A schematic and a representative scanning electron microscope (SEM) image of the straintronic GFET are shown in Figure 1a,b, respectively. A 2 μm thick film of piezoelectric lead zirconate titanate (PZT) grown using the sol-gel technique on a p^{++}-Si substrate was used as a global back-gate. The PZT film was oriented along the (110) crystal direction, and the film composition was optimized to enhance the piezoelectric and dielectric response.[21−23] A top-view SEM image in Figure 1c shows the columnar grains of the PZT film with submicron dimensions. Note that the grain sizes and the location of the grain boundaries are randomly distributed at the film surface. For electrical characterization of the PZT film, separate metal-insulator-metal (MIM) structures were fabricated. Figure 1d shows the nested polarization (P) versus electric field (E) hysteresis loops for the PZT film; a remnant polarization of 0.2 C/m^2 and a coercive field of 2 × 10^6 V/m were extracted. A d_{33} coefficient of ∼50 pm/V was extracted from dual beam laser interferometer (DBLI) measurement. This low d_{33} value can be ascribed to the thin film geometry.[24] To calibrate in-plane strain, a Ni strain gauge was also fabricated. Figure 1e shows the strain as a function of bias across the PZT film; the maximum strain value was found to be ∼0.12% for a bias of 80 V.

GFETs were fabricated on the PZT substrate using commercially purchased monolayer graphene films as described in our earlier work.[25] More than 1000 GFETs

https://doi.org/10.1021/acs.nanolett.3c01145
Nano Lett. 2023, 23, 5171−5179

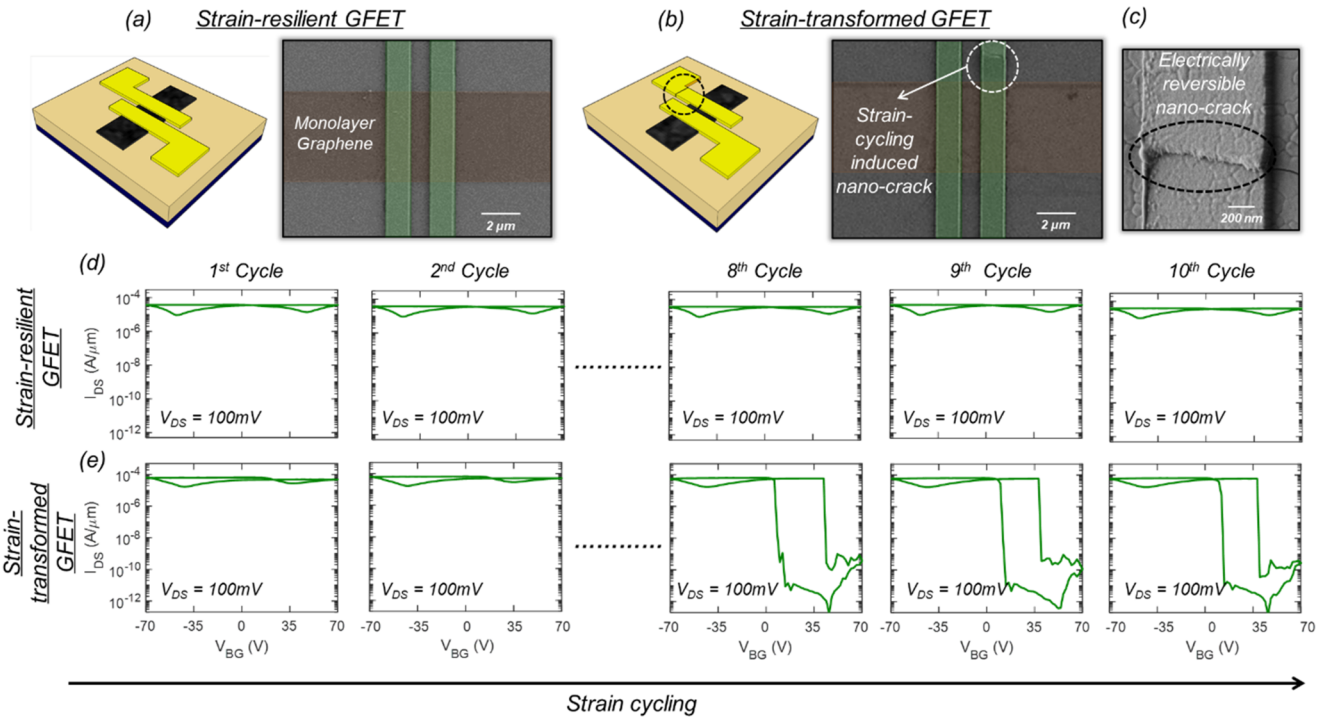


Figure 2. Strain cycling in GFETs. The schematic and SEM images of (a) strain-resilient and (b) strain-transformed GFETs after strain cycling. A nanocrack is visible in the strain-transformed GFET. (c) Zoomed-in SEM image of a representative nanocrack. Once formed, nanocracks are electrically reversible, meaning that they can be opened and closed by sweeping V_{BG}. Evolution of transfer characteristics of (d) strain-resilient and (e) strain-transformed GFETs during strain cycling, i.e., for 10 back-gate voltage sweeps from −70 to 70 V. Strain-transformed GFETs show colossal ON/OFF current ratios in excess of 10^7, whereas strain-resilient GFETs continue to exhibit poor ON/OFF current ratios of <10.

were fabricated, allowing the construction of multiple SPUFs as we will elucidate later. Figure 1f shows the Raman spectra of a graphene channel obtained using a 532 nm laser. Two characteristic peaks at around 1600 and 2700 cm^{-1} confirm monolayer graphene. Figure 1g shows the dual sweep transfer characteristics, i.e., source-to-drain current (I_{DS}) versus back-gate voltage (V_{BG}), of a representative as-fabricated GFET, measured under ambient pressure and room temperature at a source-to-drain voltage (V_{DS}) of 100 mV. The ambipolar transfer characteristics are a result of the zero-bandgap and linear energy-dispersion relationship found in graphene, which allows electrons and holes to be seamlessly injected into the conduction and the valence bands, respectively, from the source/drain metal contacts. The hysteresis observed in the GFET transfer characteristics can be ascribed to adsorbates at the interface between graphene and the PZT film.[26]

Figure 1h shows the device-to-device variation in the transfer characteristics of 400 as-fabricated GFETs. Figure 1i–l shows the distribution of peak transconductance and the maximum ON/OFF current ratio for the electron and hole branches, respectively, across these 400 GFETs. The mean and standard deviation values for the peak transconductance were found to be 3.0 and 2.8 $\mu S/\mu m$ for the electron branch and 6.1 and 3.9 $\mu S/\mu m$ for the hole branch, respectively. Additionally, the mean and standard deviation for the maximum current ON/OFF ratio were found to be 3.8 and 0.8 for the electron branch and 4.1 and 1.0 for the hole branch, respectively. The poor ON/OFF current ratio in GFETs is due to the lack of a finite bandgap in graphene.

CONSTRUCTION OF SPUFS

As described above, the transfer characteristics of the as-fabricated GFETs on the piezoelectric gate stack do not demonstrate large ON/OFF current ratios. However, when the PZT film is subjected to repeated strain cycling by sweeping V_{BG}, nanocracks can form and persist in the source/drain metal contacts of some GFETs. Figure 2a,b shows the schematic and SEM images of two representative GFETs after strain cycling. A nanocrack is clearly visible in one of the two devices. Figure 2c shows the zoomed-in SEM image of a representative nanocrack. Interestingly, once formed, these nanocracks are electrically reversible, meaning that they can be opened and closed by sweeping V_{BG}. GFETs that undergo such nanocrack formation show colossal ON/OFF current ratios in excess of 10^7; we refer to these as strain-transformed GFETs. Conversely, the GFETs where nanocrack formation does not occur continue to exhibit poor ON/OFF current ratios of <10; we refer to these as strain-resilient GFETs. The random distribution of strain-transformed and strain-resilient GFETs forms the basis of SPUF construction. Figure 2d,e, respectively, shows the evolution of the transfer characteristics of a strain-resilient GFET and a strain-transformed GFET as a function of the strain cycling, i.e., for 10 V_{BG} sweeps from −70 to 70 V. Clearly, the strain-resilient device continues to show GFET characteristics with poor ON/OFF current ratio, whereas, once transformed, the strain-transformed GFET shows an ON/OFF current ratio >10^7. The large ON/OFF current ratio can be ascribed to the fact that, with the nanocrack closed, the device exhibits normal GFET characteristics with an ON current in the range of 10 $\mu A/\mu m$, whereas the opening of the crack restricts any current flow through the GFET, and the device current drops down to the leakage floor of the measurement

https://doi.org/10.1021/acs.nanolett.3c01145
Nano Lett. 2023, 23, 5171−5179

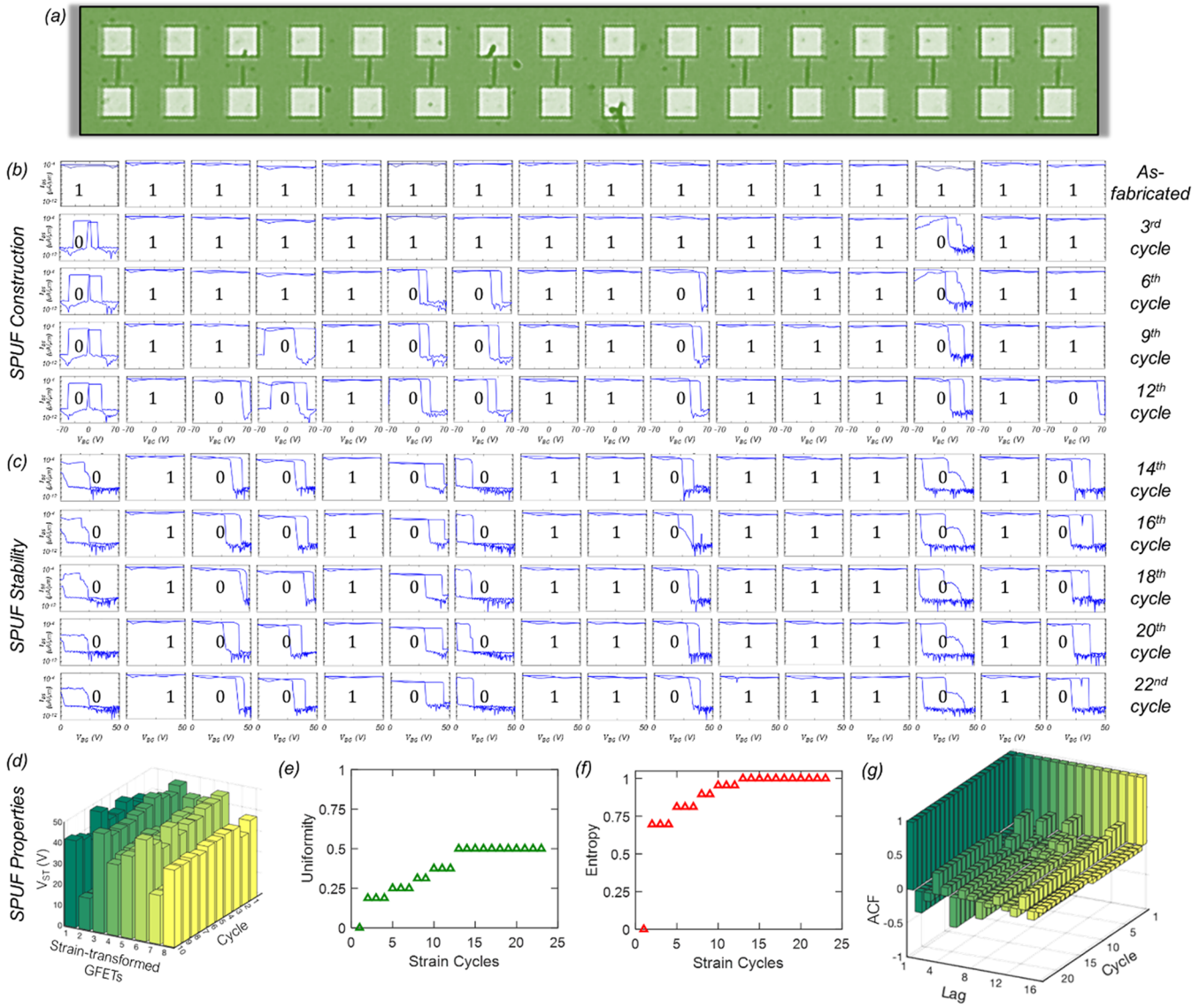


Figure 3. Construction of a straintronic physically unclonable function (SPUF). (a) Optical image of a representative SPUF comprised of 16 GFETs. (b) The process of SPUF construction through strain cycling and (c) subsequent SPUF stability. (d) Distribution of switching threshold (V_{ST}), i.e., the V_{BG} at which the cracks open/close, for the strain-transformed GFETs. Evolution of (e) uniformity (p) and (f) entropy (E) during the SPUF construction and stability testing. As expected, the as-fabricated SPUF has zero uniformity and zero entropy, since all GFETs show similar characteristics. However, at the end of the SPUF construction process both the uniformity and the entropy reach their ideal values of 0.5 and 1, respectively, and continue to maintain the same during subsequent tests of SPUF stability. (g) Autocorrelation function (ACF) as a function of lag (bit delay) during SPUF construction and subsequent stability test cycles. As expected, the as-fabricated SPUF shows strong correlation which diminishes and becomes zero at the end of the SPUF construction and is maintained during the stability test cycles.

tool (<10 pA/μm). The randomness observed in nanocrack formation among a population of GFET devices can be ascribed to the fact that piezoelectric thin films do not switch uniformly but rather switch through the motion of domain walls that are often pinned at surface defects. This results in a highly nonuniform strain distribution across the piezoelectric domains and leads to random in-plane tensile and compressive strains in the metal films that are deposited on the surface of the PZT as the source/drain contacts to the GFETs. Additionally, variations in the film morphology and in the adhesion of metal film with the PZT surface can also play important roles in introducing randomness to nanocrack formation in the GFETs.

Next, we exploit the discussed variation in strain-induced transformation of piezoelectric-gated GFETs to construct the SPUFs. Figure 3a shows the optical images of a representative SPUF. Each SPUF is comprised of 16 GFETs. A total of 25 SPUFs were characterized. Figure 3b,c shows the process of SPUF construction through strain cycling and the subsequent SPUF stability, respectively. We have used 12 cycles of sweepingV_{BG} from −70 to 70 V for SPUF construction followed by 10 more cycles of sweepingV_{BG} from 0 to 50 V for evaluating SPUF stability. We have also used V_{BG} = 50 V as the challenge and noted the I_{DS} value measured using V_{DS} = 100 mV as the response to generate corresponding CRPs. If I_{DS} > 100 nA/μm, we mark the GFET as "1"; otherwise, it represents "0" in the SPUF bit-stream. Initially, all GFETs show I_{DS} > 100 nA/μm at V_{BG} = 50 V owing to the poor ON/OFF current ratio of as-fabricated GFETs and are marked as "1". However, as each GFET is subjected to strain cycling for multiple cycles,

https://doi.org/10.1021/acs.nanolett.3c01145
Nano Lett. 2023, 23, 5171−5179

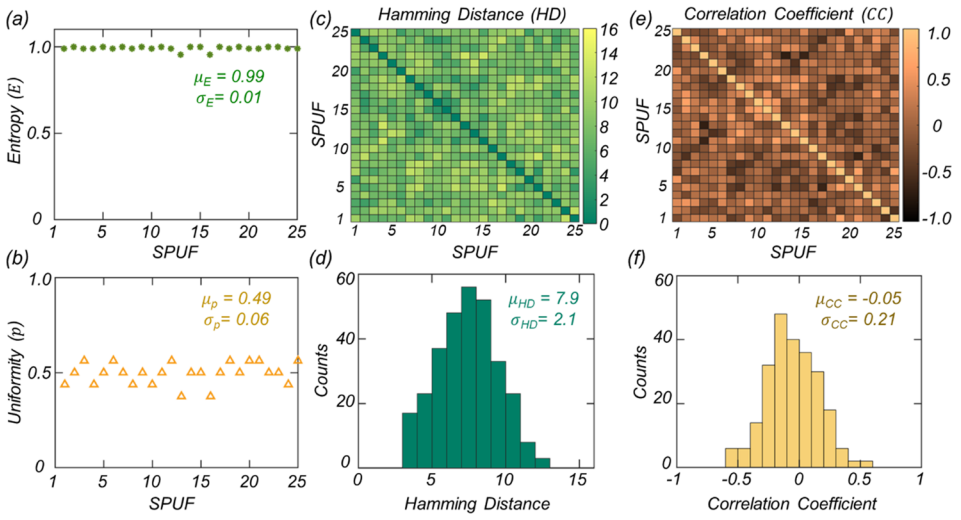


Figure 4. Properties of SPUFs. (a) Entropy (E) and (b) uniformity (p) for 25 SPUFs. (c) Colormap and (d) histogram of the Hamming distance (HD) among the 300 ($^{25}C_2$) pairs of challenge-response pairs (CRPs) obtained from the 25 SPUFs. (e) Colormap and (f) histogram of the correlation coefficient (CC) among the 300 pairs of CRPs.

some show nanocrack formation leading to large ON/OFF current ratios and are transformed into "0". After 12 strain cycles, the SPUF construction process is considered complete. Since each GFET represents 1 bit of information, our SPUFs have CRPs of 16 bit length. Figure 3d shows the distribution of switching threshold (V_{ST}), i.e., the V_{BG} at which the cracks open/close, for the strain-transformed GFETs. The mean and standard deviation for V_{ST} were found to be ∼36 and 9 V, respectively. While there exists cycle-to-cycle and device-to-device variation in V_{ST} across the strain-transformed GFETs, for sufficiently low V_{BG} (e.g., 0 V) the cracks are always closed, whereas for sufficiently large V_{BG} (> 45 V), the cracks are always open. This ensures stable operation of the SPUF when a V_{BG} of 50 V is used as the challenge. Note that once the reversible nanocrack is formed in one GFET, the corresponding V_{ST} can decrease and stabilize as more strain cycling is applied. Figure S1 (Supporting Information 1) shows 100 strain cycles performed on one representative strain-transformed device, where V_{ST} becomes less than 50 V after SPUF construction cycles and stabilizes around 42 V after subsequent strain cycling, ensuring proper SPUF generation for the bit "0" read at V_{BG} = 50 V.

PROPERTIES OF SPUFS

The entropy (E) of a PUF is a measure of its randomness and can be evaluated by noting the PUF uniformity (p). Uniformity is defined as the distribution of 1s and 0s in the CRP. Ideally, the uniformity should be p = 0.5 to ensure an equal number of 1s and 0s, which leads to maximum randomness. Ideal uniformity leads to unity entropy (E) following eq 1.

$$E = -[p\log_2 p + (1-p)\log_2(1-p)] \quad (1)$$

Figure 3e,f shows the evolution of p and E during one SPUF construction and their respective stabilities. As expected, the as-fabricated SPUF has zero uniformity and zero entropy since all GFETs show similar characteristics. However, at the end of the SPUF construction process both the uniformity and the entropy reach their ideal values of 0.5 and 1, respectively, and continue to maintain the same during subsequent tests of SPUF stability. Similarly, the autocorrelation function (ACF) may be used to examine any short-ranged periodicity in a PUF. The ACF lies in the interval [−1,1], where values of −1 and 1 indicate perfect anticorrelation and correlation, respectively. A value of 0 suggests no correlation among the bits. Figure 3g shows ACF as a function of lag (bit delay) during SPUF construction and subsequent stability test cycles. As expected, the as-fabricated SPUF shows strong correlation which diminishes and becomes zero at the end of the SPUF construction and is maintained during the stability test cycles. The entropy and uniformity tests were also performed for all 25 postconstruction SPUFs, as shown in Figure 4a,b, respectively. The mean values were found to be 0.99 and 0.49 with corresponding standard deviations of 0.01 and 0.06 for the entropy and uniformity, respectively, indicating that all SPUFs offer near-ideal performance. Figure 4c,d, respectively, shows the colormap and histogram of the Hamming distance (HD) among the 300 ($^{25}C_2$) pairs of CRPs obtained from the 25 SPUFs. The HD between two CRPs is defined as the number of nonidentical bits. Note that if the HD between a pair of CRPs is too short or too long, one can decipher one CRP from the knowledge of the other CRP. Ideally, an HD that is equal to half of the bit length ensures a maximum uniqueness of 50%. For the SPUFs, the mean HD between the CRPs was found to be ∼7.9, corresponding to a uniqueness of ∼49%. Furthermore, Figure 4e,f, respectively, shows the colormap and histogram of the correlation coefficient (CC) among the 300 pairs of CRPs. The CC is a measure of linear correlation between two statistical quantities and must be zero for independently and identically distributed random variables. The mean CC was found to be ∼−0.05, which is very close to zero, reaffirming that the SPUFs are uncorrelated and random in nature.

RELIABILITY OF SPUFS

Reliability is an essential aspect of PUFs. A PUF must be stable, i.e., the CRPs generated when a PUF is subjected to the same challenge should not change over time or due to variations in the supply voltage. At the same time, a PUF should not be vulnerable to attacks by adversaries. To this end, we investigated SPUF stability over 5 consecutive days. Figure

https://doi.org/10.1021/acs.nanolett.3c01145
Nano Lett. 2023, 23, 5171−5179

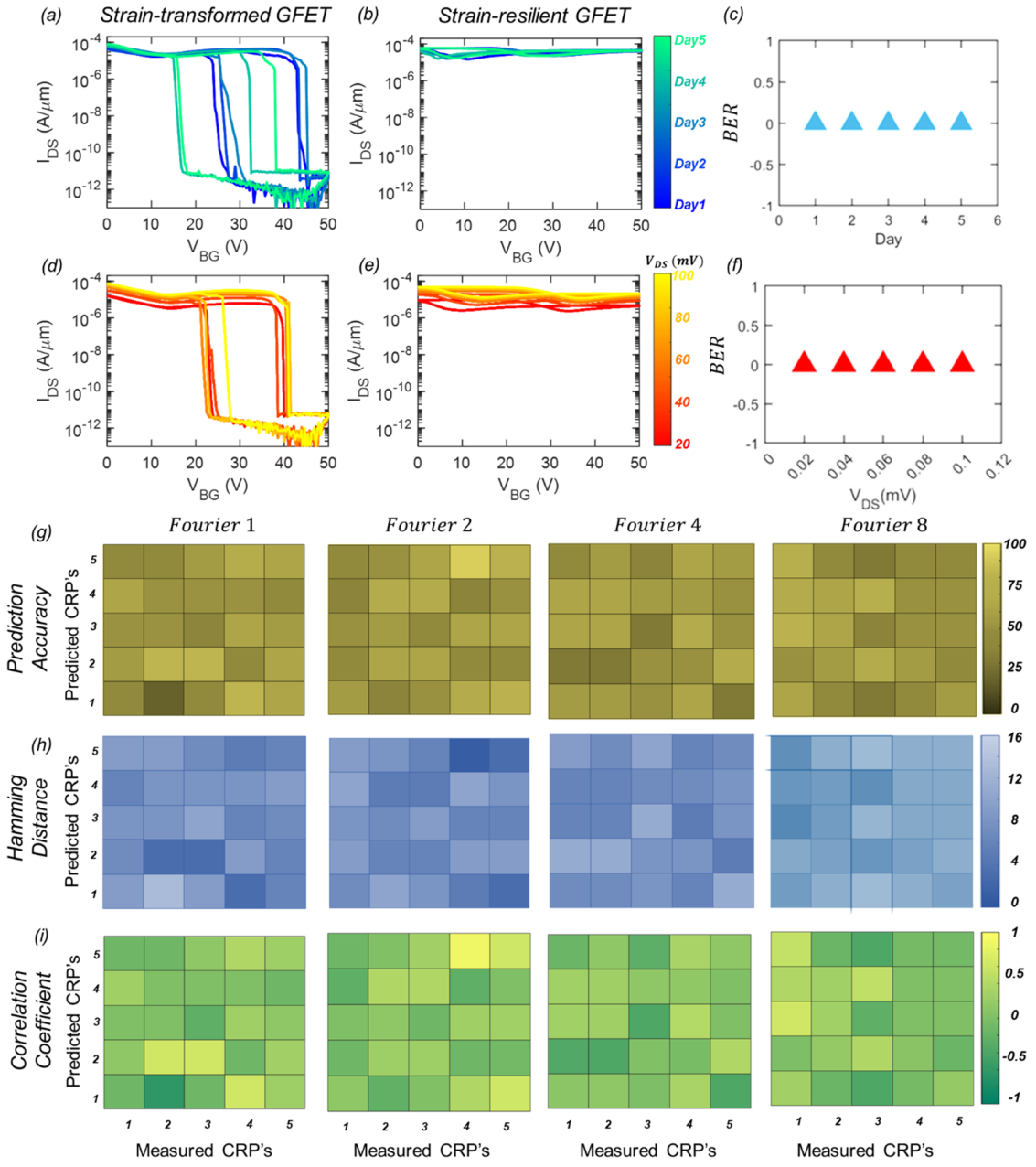


Figure 5. SPUF reliability. Transfer characteristics of representative (a) strain-transformed and (b) strain-resilient GFETs as a function of number of days. (c) Corresponding bit-error rate (BER) as a function of number of days. None of the 16 bits in the CRP were flipped, leading to BER = 0 and affirming that the SPUF is stable over time. Transfer characteristics of representative (d) strain-transformed and (e) strain-resilient GFETs measured using different V_{DS} ranging from 20 to 100 mV. (f) Corresponding BER as a function of V_{DS}. BER = 0, confirming resilience of the SPUF to supply voltage variation. Colormaps for (g) prediction accuracy, (h) HD, and (i) CC between experimentally measured CRPs and the predicted CRPs obtained from the regression analysis based on Fourier series of order N_F = 1, 2, 4, and 8.

5a,b, respectively, shows the transfer characteristics of one representative strain-transformed GFET and one representative strain-resilient GFET as a function of number of days. Figure 5c shows the bit-error rate (BER) as a function of number of days for one SPUF. The BER remains stable at zero, i.e., none of the 16 bits in the CRP were flipped, affirming that the SPUF is stable over time. We also tested the SPUF stability against supply voltage variation. Figure 5d,e, respectively, shows the transfer characteristics of one representative strain-resilient GFET and one representative strain-transformed GFET measured using V_{DS} ranging from 20 to 100 mV. Figure 5f shows that the BER remains zero and confirms the stability of the SPUF to large supply voltage variation. Furthermore, we have tested our SPUF against attacks using a predictive regression model. Regression models are the most powerful machine learning (ML) attacks for various strong PUFs since they use CRP information more efficiently than reinforcement learning or evolutionary methods.[27,28] For our purposes, we have used estimation functions constructed using a Fourier regression model to predict the CRPs. We have also used 20 estimator CRPs that were randomly chosen from the experimentally measured 25 CRPs obtained from the SPUFs. Figure 5g,i, respectively, shows the colormaps for prediction accuracy, n-HD, and CC between the remaining five

https://doi.org/10.1021/acs.nanolett.3c01145
Nano Lett. 2023, 23, 5171−5179

experimentally measured CRPs and five predicted CRPs obtained from the regression analysis based on Fourier series of order N_F = 1, 2, 4, and 8. We found that the prediction accuracy is in the range of 40−75%, CC is very close to zero, and the n-HD is close to 0.5 even for higher order regression models, indicating that the CRPs are resilient to regression-based ML attacks. We have also summarized the various state-of-the-art PUF technologies/platforms in Table 1, showing various mechanisms and materials for PUF generation. Our straintronic approach exploits stochastic strain-response on PZT grains, resulting in unique PUF generation.

Table 1. Summary Table of State-of-the-Art PUFs

PUF Type	Material	Mechanism	Ref.
Si PUF	Silicon	Circuit design	29−32
Optical PUF	Light scattering particles	Stochastic light-particle interaction	18, 33
Bio-PUF	T-cell	Stochastic cell colonization	19
PCM PUF	Chalcogenide alloy ($Ge_2Sb_2Te_5$)	Variation in crystal-structure programmability	34,35
Memristor PUF (MPUF)	Metal oxide	Ion diffusion variation	36, 37
		Variation in write-time	38
MTJ PUF	Tunneling oxide with ferromagnetic materials	Process variation in magnetic material	39−42
Organic PUF	Polyimide	Frequency dependency of organic ring oscillator (RO)	43
CNT PUF	Carbon nanotube	Randomness in self-assembly	16, 44, 45
NW PUF	Si nanowire	Stochastic stiction of electromechanical switch	46
Gr PUF	Graphene	Fluctuation in electrical conductivity	15
Strain PUF (SPUF)	**Ni/graphene on PZT**	**Stochastic strain-response on PZT**	This work

CONCLUSION

In conclusion, we have introduced a novel straintronic physically unclonable function (SPUF) based on graphene field-effect transistors (GFETs). We exploit strain-cycling in a piezoelectric gate stack to transform as-fabricated GFETs into two distinct categories. First are the strain-transformed GFETs, where electrically reversible nanocracks are formed in the source/drain metal contacts leading to colossal current ON/OFF ratios $>10^7$ in the device characteristics. Meanwhile, the strain-resilient GFETs, wherein nanocrack formation does not occur, continue to maintain low ON/OFF current ratios <10. The random distribution of strain-transformed and strain-resilient GFETs forms the basis of SPUFs. We constructed a total of 25 SPUFs, each comprising 16 GFETs, and tested their uniformity, uniqueness, and temporal and supply voltage stability. We found that these SPUFs offer near-ideal performance. Additionally, our SPUFs also demonstrated resilience to regression-based machine learning attacks. Given the rapid rise in graphene-based electronic devices and sensors for various edge applications and their security vulnerabilities, our SPUFs can be quite useful. Note that the concept of SPUFs can be translated to other materials beyond graphene as the channel of the transistor does not play a significant role in nanocrack formation.

ASSOCIATED CONTENT

Supporting Information

The Supporting Information is available free of charge at https://pubs.acs.org/doi/10.1021/acs.nanolett.3c01145.

Evolution of transfer characteristics of a strain-transformed GFET for a total of 100 strain cycles (PDF)

AUTHOR INFORMATION

Corresponding Author

Saptarshi Das − *Department of Engineering Science and Mechanics, Penn State University, University Park, Pennsylvania 16802, USA; Department of Electrical Engineering, Department of Materials Science and Engineering, and Materials Research Institute, Penn State University, University Park, Pennsylvania 16802, USA;* orcid.org/0000-0002-0188-945X; Email: sud70@psu.edu

Authors

Subir Ghosh − *Department of Engineering Science and Mechanics, Penn State University, University Park, Pennsylvania 16802, USA*

Yikai Zheng − *Department of Engineering Science and Mechanics, Penn State University, University Park, Pennsylvania 16802, USA*

Shiva Subbulakshmi Radhakrishnan − *Department of Engineering Science and Mechanics, Penn State University, University Park, Pennsylvania 16802, USA*

Thomas F Schranghamer − *Department of Engineering Science and Mechanics, Penn State University, University Park, Pennsylvania 16802, USA*

Complete contact information is available at: https://pubs.acs.org/10.1021/acs.nanolett.3c01145

Author Contributions

S.G. and Y.Z. contributed equally. S.D. conceived the idea, designed the experiments, and wrote the paper. S.G., Y.Z., and S.S.R. performed the experiments and analyzed the data. T.S. performed SEM analysis. All authors discussed the results and agreed on their implications.

Notes

The authors declare no competing financial interest.

ACKNOWLEDGMENTS

The work was supported by National Science Foundation (NSF) through a CAREER Award under grant no. ECCS-2042154.

REFERENCES

(1) Tehranipoor, M.; Wang, C. *Introduction to hardware security and trust*; Springer Science & Business Media, 2011.

(2) Zhao, K.; Ge, L. A survey on the internet of things security. *2013 9th International Conference on Computational Intelligence and Security (CIS)* **2013**, 663−667.

(3) Oberoi, A.; Dodda, A.; Liu, H.; Terrones, M.; Das, S. Secure Electronics Enabled by Atomically Thin and Photosensitive Two-Dimensional Memtransistors. *ACS Nano* **2021**, *15* (12), 19815−19827.

(4) Dodda, A.; Trainor, N.; Redwing, J.; Das, S. All-in-one, bio-inspired, and low-power crypto engines for near-sensor security based on two-dimensional memtransistors. *Nat. Commun.* **2022**, *13* (1), 3587.

(5) Wali, A.; Das, S. Hardware and Information Security Primitives Based on 2D Materials and Devices. *Adv. Mater.* **2023**, *35*, 2205365.
(6) Das, S.; Chakrabarti, S.; Wali, A.; Ravichandran, H.; Kundu, S.; Schranghamer, T. F.; Basu, K. Logic Locking of Integrated Circuits Enabled by Nanoscale MoS2-Based Memtransistors. *Acs Applied Nano Materials* **2022**, *5* (10), 14447−14455.
(7) Maes, R. Physically Unclonable Functions: Properties. *Physically Unclonable Functions* **2013**, 49−80.
(8) Suh, G. E.; Devadas, S. Physical unclonable functions for device authentication and secret key generation. In *Proceedings of the 44th annual Design Automation Conference*, San Diego, CA, 2007; pp 9−14.
(9) Maes, R.; Verbauwhede, I. Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions. *Towards Hardware-Intrinsic Security* **2010**, 3−37.
(10) Herder, C.; Yu, M.-D.; Koushanfar, F.; Devadas, S. Physical unclonable functions and applications: A tutorial. *Proceedings of the IEEE* **2014**, *102* (8), 1126−1141.
(11) Gao, Y.; Ranasinghe, D. C.; Al-Sarawi, S. F.; Kavehei, O.; Abbott, D. Emerging physical unclonable functions with nanotechnology. *IEEE access* **2016**, *4*, 61−80.
(12) Yu, J. M.; Yun, G. J.; Kim, M. S.; Han, J. K.; Kim, D. J.; Choi, Y. K. A Poly-Crystalline Silicon Nanowire Transistor with Independently Controlled Double-Gate for Physically Unclonable Function by Multi-States and Self-Destruction. *Advanced Electronic Materials* **2021**, *7* (5), 2000989.
(13) Koeberl, P.; Kocabaş, Ü; Sadeghi, A. R. Memristor PUFs: A new generation of memory-based Physically Unclonable Functions. *2013 Design, Automation & Test in Europe Conference & Exhibition (DATE)* **2013**, 428−431.
(14) John, R. A.; et al. Halide perovskite memristors as flexible and reconfigurable physical unclonable functions. *Nat. Commun.* **2021**, *12* (1), 3681.
(15) 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 (in English). *Nature Electronics* **2021**, *4* (5), 364−374.
(16) Hu, Z.; et al. Physically unclonable cryptographic primitives using self-assembled carbon nanotubes. *Nat. Nanotechnol* **2016**, *11* (6), 559−565.
(17) Fernández-Benito, A.; Hoyos, M.; López-Manchado, M. A.; Sørensen, T. J. A Physical Unclonable Function Based on Recyclable Polymer Nanoparticles to Enable the Circular Economy. *ACS Applied Nano Materials* **2022**, *5* (10), 13752−13760.
(18) Pappu, R.; Recht, B.; Taylor, J.; Gershenfeld, N. Physical one-way functions. *Science* **2002**, *297* (5589), 2026−30.
(19) Wali, A.; et al. Biological physically unclonable function. *Communications Physics* **2019**, *2* (1), 39.
(20) Dodda, A.; Wali, A.; Wu, Y.; Pannone, A.; Reddy, L. K.; Raha, A.; Ozdemir, S. K.; Ozbolat, I. T.; Das, S. Biological One-Way Functions for Secure Key Generation. *Advanced Theory and Simulations* **2019**, *2* (2), 1800154.
(21) Wolf, R. A.; Trolier-McKinstry, S. Temperature dependence of the piezoelectric response in lead zirconate titanate films. *J. Appl. Phys.* **2004**, *95* (3), 1397−1406.
(22) Karapuzha, A. S.; James, N. K.; Khanbareh, H.; van der Zwaag, S.; Groen, W. A. Structure, dielectric and piezoelectric properties of donor doped PZT ceramics across the phase diagram. *Ferroelectrics* **2016**, *504* (1), 160−171.
(23) Kayasu, V.; Ozenbas, M. The effect of Nb doping on dielectric and ferroelectric properties of PZT thin films prepared by solution deposition. *Journal of the European Ceramic Society* **2009**, *29* (6), 1157−1163.
(24) Torah, R.; Beeby, S.; White, N. Experimental investigation into the effect of substrate clamping on the piezoelectric behaviour of thick-film PZT elements. *J. Phys. D: Appl. Phys.* **2004**, *37* (7), 1074.
(25) Zheng, Y.; Sen, D.; Das, S.; Das, S. Graphene Strain-Effect Transistor with Colossal ON/OFF Current Ratio Enabled by Reversible Nanocrack Formation in Metal Electrodes on Piezoelectric Substrates. *Nano Lett.* **2023**, *23* (7), 2536−2543.
(26) Schranghamer, T. F.; Oberoi, A.; Das, S. Graphene memristive synapses for high precision neuromorphic computing. *Nat. Commun.* **2020**, *11* (1), 5474.
(27) Rührmair, U.; et al. PUF modeling attacks on simulated and silicon data. *IEEE Transactions on Information Forensics and Security* **2013**, *8* (11), 1876−1891.
(28) 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* **2010**, 237−249.
(29) Gehrer, S.; Sigl, G. Reconfigurable PUFs for FPGA-based SoCs. *2014 International Symposium on Integrated Circuits (ISIC)* **2014**, 140−143.
(30) Lao, Y.; Parhi, K. K. Reconfigurable architectures for silicon Physical Unclonable Functions. *2011 IEEE INTERNATIONAL CONFERENCE ON ELECTRO/INFORMATION TECHNOLOGY* **2011**, 1−7.
(31) Yamamoto, D. Uniqueness Enhancement of PUF Responses Based on the Locations of Random Outputting RS Latches. *Cryptographic Hardware and Embedded Systems − CHES 2011* **2011**, *6917*, 390.
(32) Anderson, J. H. A PUF design for secure FPGA-based embedded systems. *2010 15th Asia and South Pacific Design Automation Conference (ASP-DAC)* **2010**, 1−6.
(33) Kursawe, K.; Sadeghi, A. R.; Schellekens, D.; Skoric, B.; Tuyls, P. Reconfigurable Physical Unclonable Functions - Enabling technology for tamper-resistant storage. *2009 IEEE International Workshop on Hardware-Oriented Security and Trust* **2009**, 22−29.
(34) Zhang, Q.; Chen, H.; Lu, Y.; Li, X.; Song, Z. Design and security evaluation of PCM-based rPUF using cyclic refreshing strategy. *IEICE Electronics Express,* **2018**, *15* (10), 20180239−20180239.
(35) Zhang, L.; Kong, Z. H.; Chang, C.-H.; Cabrini, A.; Torelli, G. Exploiting Process Variations and Programming Sensitivity of Phase Change Memory for Reconfigurable Physical Unclonable Functions. *IEEE Transactions on Information Forensics and Security* **2014**, *9* (6), 921−932.
(36) Ibrahim, H. M.; Abunahla, H.; Mohammad, B.; AlKhzaimi, H. Memristor-based PUF for lightweight cryptographic randomness. *Sci. Rep* **2022**, *12* (1), 8633.
(37) Gao, B.; et al. Concealable physically unclonable function chip with a memristor array. *Sci. Adv,* **2022**, *8* (24), No. eabn7753.
(38) Rose, G. S.; McDonald, N.; Yan, L. K.; Wysocki, B. A write-time based memristive PUF for hardware security applications. *2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)* **2013**, *18* (21), 830−833.
(39) Marukame, T.; Tanamoto, T.; Mitani, Y. Extracting Physically Unclonable Function From Spin Transfer Switching Characteristics in Magnetic Tunnel Junctions. *IEEE Trans. Magn.* **2014**, *50* (11), 1−4.
(40) Zhang, L.; Fong, X.; Chang, C. H.; Kong, Z. H.; Roy, K. Highly reliable memory-based Physical Unclonable Function using Spin-Transfer Torque MRAM. *2014 IEEE International Symposium on Circuits and Systems (ISCAS),* **2014**, *1* (5), 2169−2172.
(41) Kahleifeh, Z.; Thapliyal, H.; Alam, S. M. Adiabatic/MTJ-Based Physically Unclonable Function for Consumer Electronics Security. *IEEE Transactions on Consumer Electronics* **2023**, *69* (1), 1−8.
(42) Lim, S.; Song, B.; Jung, S.-O. Highly Independent MTJ-Based PUF System Using Diode-Connected Transistor and Two-Step Postprocessing for Improved Response Stability. *IEEE Transactions on Information Forensics and Security,* **2020**, *15*, 2798−2807.
(43) Kuribara, K.; Hori, Y.; Katashita, T.; Kakita, K.; Tanaka, Y.; Yoshida, M. Organic physically unclonable function on flexible substrate operable at 2 V for IoT/IoE security applications. *Org. Electron.* **2017**, *51*, 137−141.
(44) Konigsmark, S. T. C.; Hwang, L. K.; Chen, D.; Wong, M. D. F. CNPUF: A Carbon Nanotube-based Physically Unclonable Function for secure low-energy hardware design. *2014 19th Asia and South Pacific Design Automation Conference (ASP-DAC)* **2014**, 73−78.

https://doi.org/10.1021/acs.nanolett.3c01145
Nano Lett. 2023, 23, 5171−5179

(45) Moon, D.-I.; et al. Physically Unclonable Function by an All-Printed Carbon Nanotube Network. *ACS Applied Electronic Materials,* **2019**, *1* (7), 1162−1168.
(46) Hwang, K. M.; et al. Nano-electromechanical Switch Based on a Physical Unclonable Function for Highly Robust and Stable Performance in Harsh Environments. *ACS Nano,* **2017**, *11* (12), 12547−12552.

https://doi.org/10.1021/acs.nanolett.3c01145
Nano Lett. 2023, 23, 5171−5179