ACS NANO

www.acsnano.org

ARTICLE

A Machine Learning Attack Resilient True Random Number Generator Based on Stochastic Programming of Atomically Thin Transistors

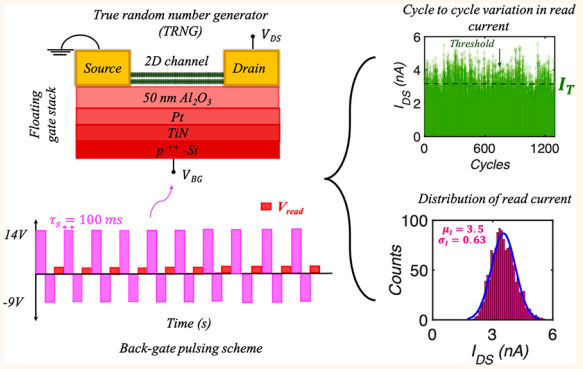
Akshay Wali, Harikrishnan Ravichandran, and Saptarshi Das*

Cite This: *ACS Nano* 2021, 15, 17804–17812

Read Online

ACCESS | Metrics & More | Article Recommendations | Supporting Information

ABSTRACT: **A true random number generator (TRNG) is a critical hardware component that has become increasingly important in the era of Internet of Things (IoT) and mobile computing for ensuring secure communication and authentication schemes. While recent years have seen an upsurge in TRNGs based on nanoscale materials and devices, their resilience against machine learning (ML) attacks remains unexamined. In this article, we demonstrate a ML attack resilient, low-power, and low-cost TRNG by exploiting stochastic programmability of floating gate (FG) field effect transistors (FETs) with atomically thin channel materials. The origin of stochasticity is attributed to the probabilistic nature of charge trapping and detrapping phenomena in the FG. Our TRNG also satisfies other requirements, which include high entropy, uniformity, uniqueness, and unclonability. Furthermore, the generated bit-streams pass NIST randomness tests without any postprocessing. Our findings are important in the context of hardware security for resource constrained IoT edge devices, which are becoming increasingly vulnerable to ML attacks.**

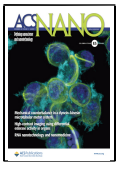


KEYWORDS: *random numbers, Internet of things, hardware security, charge trapping/detrapping, floating gate, machine learning, field effect transistors*

Random numbers are widely used in areas such as cryptography, numerical simulations, information security, testing of manufactured goods, modeling of complex phenomena, and stochastic computing. Due to recent advancements in digital technologies such as the Internet of Things (IoT) and cloud computing, massive amounts of critical public and personal information is being constantly exchanged between communicating devices over highly complex and integrated networks.[1,2] Unfortunately, this explosive growth coupled with an overwhelming reliance on cyberspace has coincided with digital information becoming increasingly more susceptible to a wide range of security threats. This has necessitated robust and rigorous information security[3,4] protocols where random numbers play a pivotal role.

Random number generators (RNGs) can be broadly classified into two major categories: pseudo-RNGs (PRNGs) and true-RNGs (TRNGs). PRNGs are primarily software-based, utilizing an initial seed with mathematical algorithms to generate random numbers.[5] However, due to their periodic nature, random sequences generated by PRNGs become predictable if the input seed is known, thus making them vulnerable to various cryptanalysis attacks.[6,7] Additionally, PRNGs require multiple layers of encryption, increasing their demand for computation and energy requirements thus severely limiting their use in resource-constrained IoT edge devices.[8] In contrast, TRNGs are hardware based, generating random numbers based on a physically unpredictable process or phenomenon, which is nearly impossible to model. TRNGs are less vulnerable to security attacks and are significantly more energy efficient. The first ever hardware-based TRNG was the Manchester Mark I, which utilized electrical noise as the source

Received: July 14, 2021
Accepted: October 4, 2021
Published: October 19, 2021



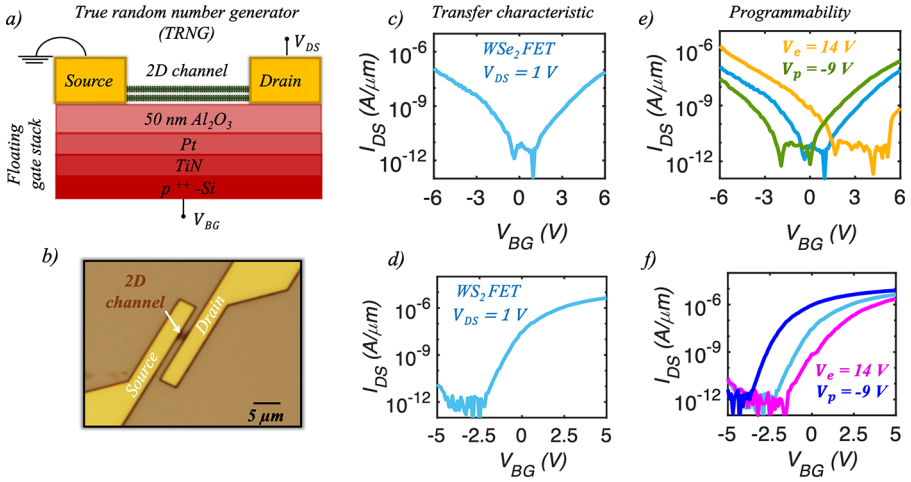


Figure 1. Programmable two-dimensional (2D) field effect transistors (FETs). (a) Schematic (side view) and (b) optical image (top-view) of a representative 2D FET based on few-layer exfoliated transition metal dichalcogenide such as WSe_2 and WS_2 as the channel material, Ni/Au (40 nm/30 nm) as the source and drain contacts, and a programmable stack consisting of atomic layer deposition (ALD) grown 50 nm Al_2O_3 on Pt/TiN/p^{++}-Si as the floating gate (FG). The device has a channel length of 1 μm. Transfer characteristics in logarithmic scale for (c) WSe_2 and (d) WS_2 FETs measured using a drain bias, V_{DS} = 1 V. WSe_2 shows ambipolar conduction, that is, the presence of both electron and hole transport, whereas WS_2 shows only electron conduction. Transfer characteristics in logarithmic scale after the application of a positive programming (V_p = −9 V) and a negative erase pulse (V_e = 14 V) of fixed pulse width = 100 ms for e) WSe_2 and f) WS_2 FETs. Application of V_p shifts the transfer characteristics to the left, whereas V_e shifts the transfer characteristics to the right indicating electron trapping and detrapping, respectively, in the FG stack.

of randomness.[9] Subsequently, thermal noise via oscillator jitter,[10] capacitive feedback elements,[11] and resistor-amplifier analog to digital converters[12] have been exploited to realize TRNGs. Other approaches like oxide breakdown induced current fluctuations,[13] random telegraph noise,[14] and numerous spatiotemporal phenomena at the deep-micrometer and nanometer scale have also been used as high entropy sources.[15−18] Although sufficiently random, most state-of-the-art TRNGs often require postprocessing steps such as von Neumann correction to remove any residual biases.[10−14] Recently, diffusive memristor-based TRNGs[19−22] were proposed that required no additional postprocessing steps while providing attractive properties such as low power consumption. Nanoscale materials and devices have also been explored as postsilicon alternatives for generating true random numbers (TRNs).[23−26] In addition, several optical,[27−29] quantum,[30−35] and biological[36−38] TRNGs have been proposed. While these developments are impressive, vulnerability of TRNGs to machine learning (ML) attacks is relatively less studied. It should be noted that ML attacks pose severe threat to hardware security.

In this article, we demonstrate a ML attack resilient TRNG that exploits programming stochasticity in floating gate (FG) two-dimensional (2D) field effect transistors (FETs). The random bits obtained from FG 2D FETs offer near ideal entropy, uniformity, uniqueness, and lack of correlation, and can pass standard randomness tests from NIST without any postprocessing. We also found that TRNGs based on different devices are statistically independent and hence physically unclonable. Additionally, the generated bits demonstrated resilience against regression-based ML attacks. Finally, the energy expenditure for random bit generation was also found to be miniscule at ∼10 pJ/bit. In short, our results highlight the potential for 2D FET-based high-entropy and low-power TRNGs for resource constrained edge applications.

Our choice of 2D materials such as transition-metal dichalcogenides (TMDs) for hardware security applications is motivated by their potential in future technologies. TMDs are layered compounds with strong in-plane covalent and weak out-of-plane van der Waals (vdW) bonding,[39] and are promising candidates for the postsilicon era due to their ultrathin body allowing aggressive dimensional scaling without invoking detrimental quantum confinement effects.[40,41] In addition, recent studies on hardware camouflaging based on 2D heterostructures,[42] reconfigurable polymorphic gates based on black phosphorus,[43] ML resilient physically unclonable functions (PUFs) based on graphene FETs,[44] and advanced encryption using metal/insulator/metal and hexagonal boron nitride (h-BN)[45] have demonstrated the potential of 2D materials for developing future hardware security primitives.

RESULTS AND DISCUSSION

Programmable 2D FETs. Our 2D FET-based TRNG uses mechanically exfoliated few-layer tungsten diselenide (WSe_2) and tungsten disulfide (WS_2) as the channel material, and 50 nm atomic layer deposition (ALD) grown alumina (Al_2O_3) on Pt/TiN/p^{++}-Si as the FG stack. Figure 1a,b, respectively, shows the schematic and optical image (top-view) of a representative FG 2D FET (see Methods section for more details on the fabrication). Figure 1c,d shows the transfer characteristics of WSe_2 and WS_2FETs, respectively, in logarithmic scale, measured at a drain bias, V_{DS} = 1 V. The difference in the carrier transport behavior in WSe_2 and WS_2 FETs can be attributed to the location of the metal Fermi level pinning with respect to the conduction and valence band edges of these materials.[46] In WSe_2, the metal Fermi level pins closer to the center of the bandgap promoting ambipolar conduction,[47] that is, the presence of both electron and hole transport, whereas in WS_2, the metal Fermi level pins near the conduction band, resulting in electron conduction.[48]

Figure 1e shows the programmability of WSe_2 and WS_2 FETs using the FG stack. The transfer characteristics shift toward the left when a negative programming voltage pulse, V_p

https://doi.org/10.1021/acsnano.1c05984
ACS Nano 2021, 15, 17804−17812

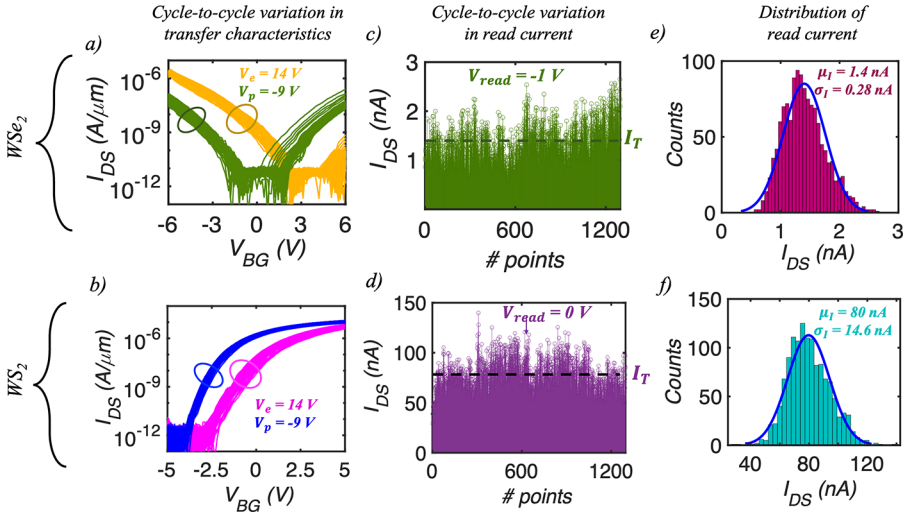


Figure 2. Programming stochasticity in 2D FETs. Transfer characteristics in logarithmic scale measured after the application of every programming (V_p = −9 V) and erase (V_e = 14 V) pulse for a total of 60 cycles for (a) WSe_2 and (b) WS_2 FETs. Cycle-to-cycle variation in postprogrammed I_{DS} measured at V_{read} = −1 and 0 V for (c) WSe_2 and (d) WS_2 FETs, respectively. Corresponding distribution of I_{DS} and Gaussian fit using means (μ_I) of 1.4 nA and 80 nA, and standard deviations (σ_I) of 0.28 nA and 14.6 nA for (e) WSe_2 and (f) WS_2 FETs, respectively. Binarization of I_{DS} is achieved by using a threshold current I_T, which is defined as the mean of all I_{DS} values as shown using the dotted lines in (c) and (d). Any I_{DS} values above and below I_T are assigned to bit "1" and bit "0", respectively.

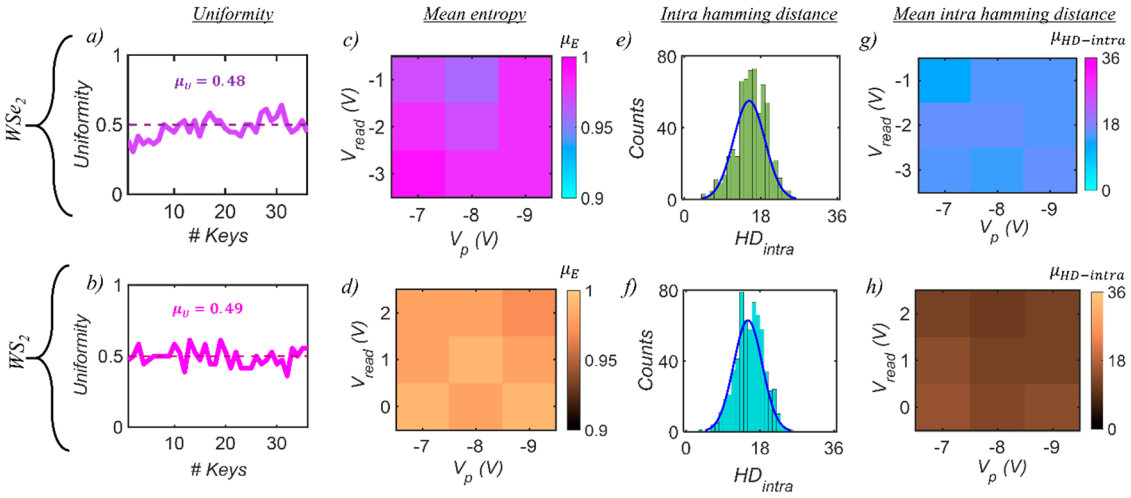


Figure 3. Randomness test using uniformity, entropy, and hamming distance. Uniformity for 36 keys each with 36-bit generated by binarizing I_{DS} values measured using V_{read} = −1 and 0 V for (a) WSe_2 and (b) WS_2 FETs, respectively, when V_p = −9 V and V_e = 14 V are used for programming and erase cycles. Mean uniformity values (dotted lines) are found to be 0.48 and 0.49 for keys obtained from WSe_2 and WS_2 FETs, respectively, which are close to the ideal value of 0.5. Colormaps of mean entropy (μ_E) of keys obtained from (c) WSe_2 and (d) WS_2 FETs by using different V_p and V_{read}. Distribution of intra hamming distance (HD_{intra}) between $^{36}C_2$ = 630 pairs of 36-bit keys obtained from (e) WSe_2 and (f) WS_2 FETs by using V_p = −9 V, V_e = 14 V, and V_{read} = −1 and 0 V, respectively. Mean HD_{intra} (μ_{HD} − $_{intra}$) values are found to be ∼15 and 16 for the keys obtained from WSe_2 and WS_2 FETs, respectively, which are close to the ideal value of 18. Colormaps of μ_{HD} − $_{intra}$ of 36 keys obtained from (g) WSe_2 and (h) WS_2 FETs by using different V_p and V_{read}.

= −9 V is applied to the FG, whereas the characteristics shift toward the right when a positive erase voltage pulse, V_e = 14 V is applied to the FG. Each pulse has a fixed duration of τ_s = 100 ms. The shift in the transfer characteristics can be attributed to the FG stack, which has been described in detail in a previous work.[49] In short, electron trapping/detrapping in the FG leads to the corresponding shift in the device threshold when a positive/negative voltage pulse is applied to the back-gate stack. The amount of threshold shift depends on the pulse magnitude (V_p and V_e) and the pulse width (τ_s). It is important to note that even though we define negative and positive magnitude voltage pulses as programming and erase pulses, respectively, there is no limitation in using them interchangeably.

Next, the 2D FETs were subjected to programming and erase cycles. Figure 2a,b shows the transfer characteristics of WSe_2 and WS_2 FETs, respectively, measured each time after the application of V_p = −9 V and V_e = 14 V pulses for τ_s = 100 ms, for a total of 60 cycles. The post-programmed and post-erased states show cycle-to-cycle variability, which, while deterrent from the point of view of programming/erase reproducibility, offers tremendous opportunity to be exploited as a TRNG. The origin of cycle-to-cycle variability can be ascribed to the probabilistic nature of the carrier trapping/

https://doi.org/10.1021/acsnano.1c05984
ACS Nano 2021, 15, 17804−17812

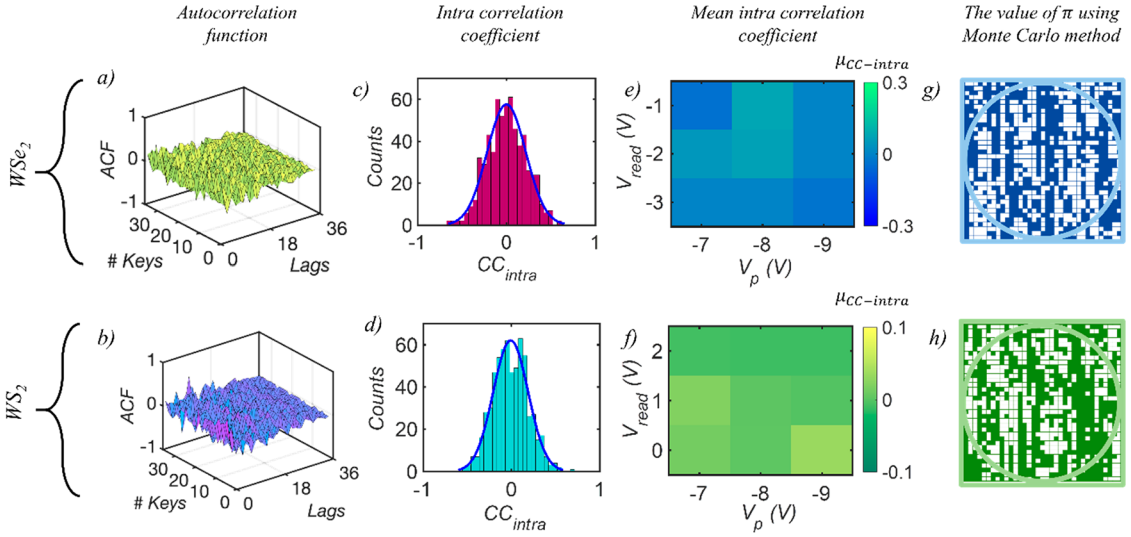


Figure 4. Randomness test using correlation and the value of π. Autocorrelation as a function of lag or bit delay for each of the 36 keys of length 36-bit obtained by using $V_p = -9$ V, $V_e = 14$ V, and $V_{read} = -1$ and 0 V from (a) WSe_2 and (b) WS_2 FETs, respectively. Distribution of corresponding zero-lag intra correlation coefficient (CC_{intra}) between the $^{36}C_2 = 630$ pairs of keys obtained from (c) WSe_2 and (d) WS_2 FETs. Mean CC_{intra} ($\mu_{CC-intra}$) values of ∼−0.035 and −0.01 for the keys obtained from WSe_2 and WS_2 FETs, respectively, confirm that the keys are uncorrelated. Colormaps $\mu_{CC-intra}$ for keys obtained using different combinations of V_p and V_{read} from (e) WSe_2 and (f) WS_2 FETs. Estimation of the value of π using a Monte Carlo method using random bits obtained from (g) WSe_2 and (h) WS_2 FETs.

detrapping phenomena in the FG leading to stochastic fluctuations in the shift in the device characteristics, which we exploit as a high entropy source for the construction of a TRNG. For quantitative evaluation of the randomness associated with the carrier trapping/detrapping process, the pulsing scheme shown in Supporting Information (SI) 1, where each cycle consisted of three consecutive pulses, V_p, V_e, and a read voltage,V_{read}, was applied for 100 ms to the FG stack. The drain-to-source current (I_{DS}) values were measured using $V_{DS} = 1$ V at a back-gate voltage,$V_{BG} = V_{read}$. Figure 2c,d shows the cycle-to-cycle variability in I_{DS} for $V_{read} = -1$ and 0 V for WSe_2 and WS_2 FETs, respectively, for a total of 1296 cycles. Figure 2e,f shows the corresponding histograms of the distribution of I_{DS}, which can be fitted using Gaussian functions with means (μ_I) of 1.4 nA and 80 nA, and standard deviations (σ_I) of 0.28 nA and 14.6 nA for WSe_2 and WS_2FETs, respectively. Note that the I_{DS} values extracted using different V_{read} also follow Gaussian distributions, but with different μ_I and σ_I as shown in SI 2. Similarly, V_p values for programming can be tuned to adjust μ_I and σ_I as shown in SI 3. Nevertheless, the above demonstrations confirm programming stochasticity in the FG 2D FETs, making post-programmed I_{DS} a Gaussian random variable.

Construction of Binary Bit-Streams, Keys, And Assessment of Their Randomness. First, analog I_{DS} values are binarized by establishing a threshold current, I_T, which is defined as the mean of all I_{DS} values as shown using the dotted lines in Figure 2c,d. I_{DS} values above and below I_T are converted to binary bit "1" and "0", respectively. Next, the generated 1296 bits are divided into 36 keys of 36 binary bits each. These 36 keys are then subjected to various tests to evaluate the strength of their randomness. This includes assessing the uniformity, uniqueness, and correlation among the keys.

Uniformity is defined as the proportion of "0"s and "1"s in a given bit sequence. For an ideal random source, uniformity is expected to be 0.5 since the probabilities of obtaining a "0" or a "1" are equal. Figure 3a,b shows the uniformity for all 36 keys obtained by using $V_p = -9$ V, $V_e = 14$ V, and $V_{read} = -1$ and 0 V for WSe_2 and WS_2 FETs, respectively. The mean uniformity values (dotted line) are found to be 0.48 and 0.49 for keys generated by WSe_2 and WS_2 FETs, respectively, which are close to the ideal value of 0.5. Note that a uniformity of 0.5 is equivalent to the maximum entropy (E) of 1 for 1-bit information calculated using eq 1

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

Here, p and $(1-p)$ are the probability of obtaining a "1" and a "0", respectively. SI 4 and 5 show the uniformity and entropy for 36 keys extracted using different combinations of V_p and V_{read} from WSe_2 and WS_2 FETs, respectively, while Figure 3c,d shows the corresponding colormaps for mean entropy (μ_E), which are found to be close to the ideal value of 1.

Next, we assess the randomness of the binary keys using another metric called the intra hamming distance (HD_{intra}) between a pair of keys, which is defined as the number of bit substitutions required to transform one key to another. Note that the term "intra" here is used for keys generated using the same device. To be cryptographically secure, HD_{intra} should ideally be 50% of the total key length, that is, 18 for a 36-bit key in the present case. Keys with an HD_{intra} value that is too low or too high are relatively easy to decipher through brute force trials (BFTs). The number of BFTs required to decipher an unknown key of length N from a known key is ^NC_k for $HD_{intra} = k$. BFT is maximum when $k = N/2$. Figure 3e,f shows the distribution of HD_{intra} among the $^{36}C_2$ or 630 pairs of 36-bit keys obtained by using $V_p = -9$ V,$V_e = 14$ V, and $V_{read} = -1$ and 0 V from WSe_2 and WS_2 FETs, respectively. We found that the corresponding mean HD_{intra} ($\mu_{HD-intra}$) values are ∼15 and 16 for the keys obtained from WSe_2 and WS_2 FETs, respectively. SI 6 and 7 show the distribution of HD_{intra} when the keys are obtained using different combinations of V_p and V_{read} from WSe_2 and WS_2 FETs, respectively, and Figure 3g,h

https://doi.org/10.1021/acsnano.1c05984
ACS Nano 2021, 15, 17804−17812

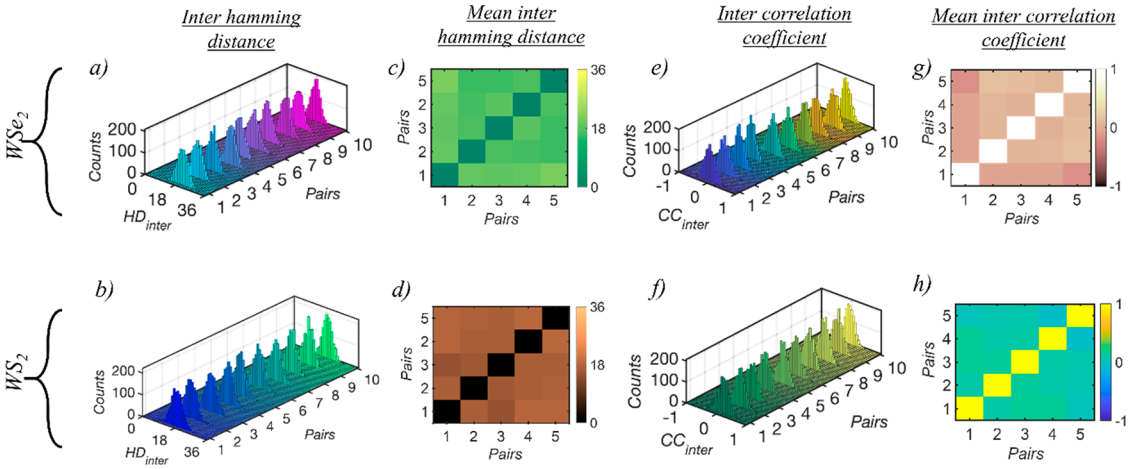


Figure 5. Unclonability of 2D-FET based TRNG. 3D histogram of the interhamming distance HD_{inter} among the 36 keys obtained from each of the $^5C_2$ or 10 possible pairs using V_p = −9 V, V_e = 14 V, and V_{read} = −1 and 0 V for (a) WSe_2 and (b) WS_2 FETs, respectively. The histogram is centered close to the ideal value of 18 as seen using the colormap of the extracted mean HD_{inter} ($\mu_{HD-inter}$) values for (c) WSe_2 and (d) WS_2 FETs, respectively, confirming that the TRNs generated by different devices are unique. 3D histogram of the inter correlation coefficient CC_{inter} among the 36 keys obtained from each of the $^5C_2$ or 10 possible pairs of (e) WSe_2 and (f) WS_2 FETs, respectively. The histogram is centered close to the ideal value of 0 as seen using the colormap of the corresponding mean CC_{inter} ($\mu_{CC-inter}$) values, confirming that the TRNs generated are uncorrelated.

shows the colormap of corresponding $\mu_{HD-intra}$, which are found to be very close to the ideal value of 18.

Correlation coefficient is another measure of randomness in a bit sequence. For example, the autocorrelation function (ACF) is used to examine any short-ranged periodicity in a bit stream. ACF lies in the interval [−1,1], wherein a value of −1 and 1 indicate anticorrelation and correlation, respectively, and a value of 0 suggests no correlation among the bits in a given sequence. Figure 4a,b shows the autocorrelation as a function of lag or bit delay for each of the 36 keys of length 36-bit obtained by using V_p = −9 V, V_e = 14 V, and V_{read} = −1 and 0 V from WSe_2 and WS_2 FETs, respectively. The absence of any high magnitude spike indicates little-to-no periodicity in the keys, that is, the generated bit-streams are truly random in nature. Figure 4c,d shows the distribution of the corresponding zero-lag intra correlation coefficient (CC_{intra}) between the 630 pairs of 36-bit keys obtained from WSe_2 and WS_2 FETs, respectively. Mean CC_{intra} ($\mu_{CC-intra}$) of ∼ −0.035 and −0.01 further confirms that the keys are uncorrelated. SI 8 and 9 shows the distribution of CC_{intra} when the keys are obtained using different combinations of V_p and V_{read} from WSe_2 and WS_2 FETs and Figure 4e,f, respectively, shows the colormap of corresponding $\mu_{CC-intra}$, which are found to be very close to the ideal value of 0.

Additionally, we also estimated the value of π using a Monte Carlo method, which uses the fact that the area of a circle of radius r divided by the area of a square with sides of length $2r$ is equal to $\pi/4$. To implement this method, we created black and white images consisting of 36 × 36 pixels using the binary keys obtained from WSe_2 and WS_2 FETs, as shown in Figure 4g,h. Here, white pixels represent bit "1" and black pixels represents bit "0". Next, we calculate the ratio of number of the white pixels inside the largest circle to the number of white pixels within the square image to estimate the value of π. We obtained π = 3.1 and 3.07 for WSe_2 and WS_2 FETs, respectively.

To further assess the performance of our FG 2D FET based TRNG, we carried out randomness testing using the standard statistical test package developed by the National Institute of Standards and Technology (NIST Sp 800−22 rev. 1a).[50] These tests are useful in determining whether or not a generator is suitable for realizing TRNs as security primitives. As such, a total of 13 different random bit streams, each consisting of 1296 bits for a total of 16 484 bits, were collected. The collected bit streams were then evaluated according to the test protocols that evaluates a specific null hypothesis that the sequence is random and returns a P-value with 99% confidence level. The bits are considered truly random only if the P-value is greater than 0.01. As shown in SI 10, our bit-sequence passes all the specified NIST tests without requiring any postprocessing steps. It must be noted that other NIST tests require longer bit streams consisting of at least 1 million bits.

Unclonability of 2D FET-based TRNG. Physical unclonability is a basic requirement for TRNGs, as it ensures that the digital bit streams generated by one TRNG are unique and distinguishable from the digital bit streams generated by another TRNG. This prohibits reverse engineering of the TRNG. To assess the unclonability of FG 2D FET-based TRNGs, we identified five WSe_2 and five WS_2 FETs and generated 36-bit keys from each using V_p = −9 V and V_e = 14 V. Figure 5a,b shows the histograms of inter hamming distance (HD_{inter}) values among the 36 keys obtained from each of the $^5C_2$ or 10 possible pairs of WSe_2 and WS_2 FETs, respectively, while Figure 5c,d shows the colormaps of the corresponding mean HD_{inter} ($\mu_{HD-inter}$) values. The term "inter" here refers to hamming distance between key pairs generated using different devices. From Figure 5c,d, it is clear that the $\mu_{HD-inter}$ values are found to be close to the ideal value of 18, thus confirming that the TRNs generated by different devices are unique. Similarly, Figure 5e,f shows the histograms of inter correlation coefficient (CC_{inter}) values among the 36 keys obtained from each of the 10 possible pairs of WSe_2 and WS_2 FETs, respectively, while Figure 5g,h shows the colormaps of corresponding mean CC_{inter} ($\mu_{CC-inter}$) values. The $\mu_{CC-inter}$ values are found to be close to the ideal value of 0, confirming that the TRNs generated by different devices are uncorrelated. Note that the channel thickness for each device is different due to the random nature of the exfoliation process, which

https://doi.org/10.1021/acsnano.1c05984
ACS Nano 2021, 15, 17804−17812

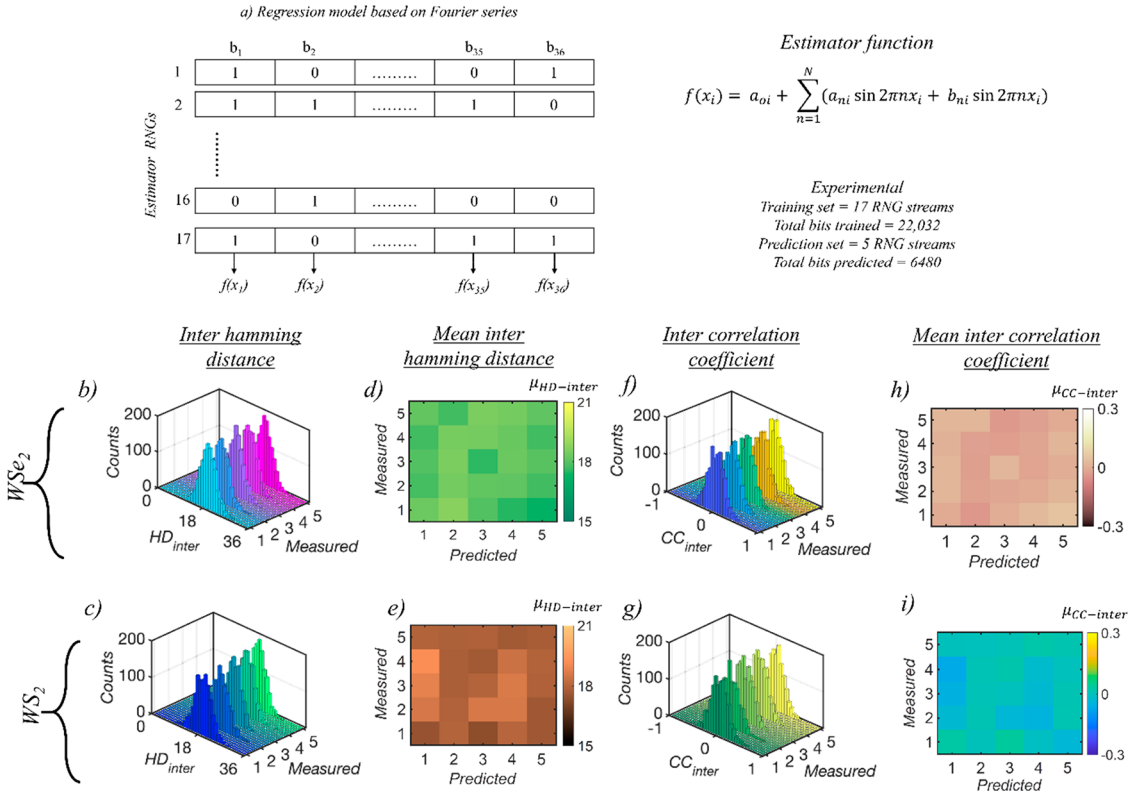


Figure 6. Resilience of 2D FET based TRNGs to machine learning attack. (a) Schematic showing the construction of the estimation functions using a Fourier regression model from 17 estimator TRNGs chosen from the experimentally measured 22 TRNGs. A total of 22 032 bits were utilized as training set and 6480 bits were obtained as prediction set. Distribution of HD_{inter} between the keys obtained from the predictor TRNGs and the keys obtained from remaining five experimentally measured (b) WSe_2 and (c) WS_2 FET-based TRNGs. The colormap of the corresponding $\mu_{HD\ -\ inter}$ for (d) WSe_2 and (e) WS_2 FET-based TRNGs. Values close to the ideal value of 18 indicate that the experimentally obtained keys are unique from the predicted keys. Distribution of CC_{inter} between the keys obtained from the predictor TRNGs and the keys obtained from remaining five experimentally measured (f) WSe_2 and (g) WS_2 FET-based TRNGs. The colormap of the corresponding $\mu_{HD\ -\ inter}$ for (h) WSe_2 and (i) WS_2 FET-based TRNGs. Values close to 0 confirms that that the experimentally obtained keys are uncorrelated to the predicted keys.

enhances the overall entropy of the system through device-to-device variations.

Resilience to Machine Learning Attacks. We have examined the resilience of our FG 2D FET-based TRNG against a predictive regression model formulated using Fourier series, which has demonstrated effectiveness against strong security primitives such as PUFs.[51] First, we generated 36 keys of length 36-bit from each of the 22 WSe_2 and 22 WS_2 FET-based TRNGs. Next, we derived the estimation functions $f(x_i)$, where i = 1,2,3, ...,36, for predicting the ith-bit of the 36-bit key by using 17 out of the 22 TRNGs for WSe_2 and WS_2, as shown in Figure 6a. Finally, the estimation functions are used to predict the keys generated by the remaining 5 WSe_2 and WS_2 FET-based TRNGs. A total of 22 032 bits were utilized as the training set to develop the estimation functions and 6480 bits were obtained post-training for predicting the keys. Figure 6b,c shows the histograms of HD_{inter} values between the keys obtained from the predictor TRNGs and the keys obtained from the 5 experimentally measured WSe_2 and WS_2 FET-based TRNGs, respectively. Figure 6d,e shows the colormaps of the corresponding $\mu_{HD-\ inter}$ values. From these results, the $\mu_{HD\ -\ inter}$ values are found to be close to the ideal value of 18, indicating that the keys obtained from experimentally measured TRNGs are unique from the keys obtained from predictor TRNGs. Similarly, Figure 6f,g shows the histograms of the CC_{inter} values and Figure 6h,i shows the colormaps of the corresponding $\mu_{CC-\ inter}$ values between the keys obtained from the predictor TRNGs and the keys obtained from the 5 experimentally measured WSe_2 and WS_2 FET-based TRNGs, respectively. Once again, the $\mu_{CC\ -\ inter}$ values are found to be close to the ideal value of 0, confirming that the experimentally measured keys and predicted keys are uncorrelated. The above analysis confirms the resilience of FG 2D FET based TRNGs to regression based ML attacks.

Energy Consumption for Bit Generation. The energy expenditure for the bit generation process (E_{TRN}) is calculated based on eq 1a−c.

$$E_{read} = I_{DS}V_{DS}\tau_s \tag{1a}$$

$$E_{write} = \frac{1}{2}C_g(V_e^2 + V_p^2) \tag{1b}$$

$$E_{TRN} = \frac{1}{N}(E_{read} + E_{write}) \tag{1c}$$

Here, E_{read} and E_{write} are read and write energy, respectively, and $C_g = {WL\varepsilon_0\varepsilon_{ox}}/{t_{ox}}$ is the gate-capacitance, W and L are channel length and channel width, respectively, $\varepsilon_0 = 8.85 \times 10^{-12}$ F/m is the vacuum permittivity, and $\varepsilon_{ox} = 10$ and $t_{ox} = 50$ nm are relative dielectric constant and thickness of the Al_2O_3 gate dielectric.SI 11 shows E_{TRN} as a function of V_p and V_{read}. Note that in our demonstration, $E_{read} \gg E_{write}$ and, hence, E_{TRN}

https://doi.org/10.1021/acsnano.1c05984
ACS Nano 2021, 15, 17804−17812

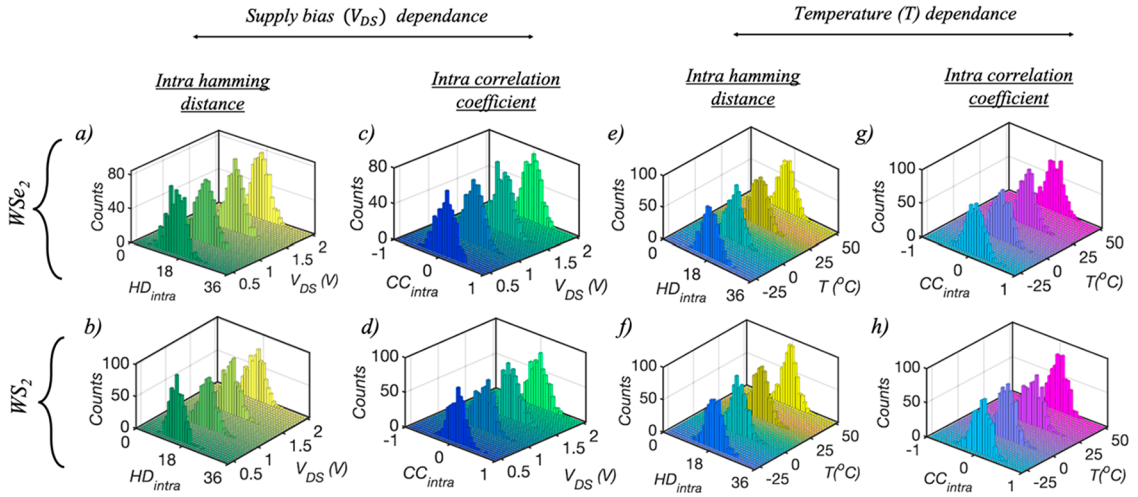


Figure 7. Robustness to supply bias and temperature variations. 3D histograms of (a,b) intrahamming distances (HD_{intra}) and (c,d) intracorrelation coefficients (CC_{intra}) between the $^{36}C_2$ = 630 pairs of keys for WSe_2 and WS_2 FETs, respectively, evaluated against different supply bias or V_{DS} values of 0.5 V, 1 V, 1.5 V, and 2 V. The histograms are centered close to the ideal values of 18 and 0 for $\mu_{HD-intra}$ and $\mu_{CC-intra}$, respectively, indicating that the TRNG remains stable against fluctuations in V_{DS} values. 3D histograms of (e,f) intrahamming distances (HD_{intra}) and (g,h) intracorrelation coefficients (CC_{intra}) for WSe_2 and WS_2 FETs, respectively, evaluated at different temperatures (T) of −25 °C, 0 °C, 25 °C, and 50 °C. Once again, the histogram means are close to 18 and 0 for $\mu_{HD-intra}$ and $\mu_{CC-intra}$, respectively, further confirming the robustness and resilience of TRNG against temperature gradients. The keys were obtained using V_p = −7 V, V_e = 14 V, and V_{read} = −3 and 3 V for WSe_2 and WS_2 FETs, respectively, for both the V_{DS} and temperature variation study.

mainly depends on E_{read}. This is why we have specifically chosen V_{read} values that correspond to the subthreshold regimes of the respective 2D FET operation to ensures low E_{read}. It is interesting to note that the magnitude of V_p impacts the overall E_{TRN} for WSe_2 and WS_2 FETs differently. In WSe_2, a higher V_p causes a significant decrease in the p-branch I_{DS} values, whereas for WS_2, the same V_p leads to an increase in the n-branch I_{DS} value. As such, for any given V_{read}, E_{read} increases for WS_2 and decreases for WSe_2 FETs with increasing magnitude of V_p. Nevertheless, the energy expenditure for bit generation can be as frugal as 10 pJ/bit. E_{TRN} can be scaled further by scaling V_{DS} and τ_s. Note that our energy calculations do not involve the energy expenditure for the thresholding devices.

Robustness of TRNGs to Supply Voltage and Temperature Variations. Finally, we evaluated the robustness of our TRNG against two important challenges: supply voltage (V_{DS}) and temperature (T) variations. Figure 7a–d shows the histogram plots of the HD_{intra} and CC_{intra} values among all possible combinations of 36 keys for different V_{DS} values of 0.5, 1, 1.5, and 2 V for WSe_2 FETs (a,c) and WS_2 FETs (b,d). From these results, the $\mu_{HD-intra}$ and $\mu_{CC-intra}$ values were found to be close to the ideal value of 18 and 0, respectively, confirming that the generated TRNs remain stable under supply voltage fluctuations. Similarly, Figure 7e–h shows the histogram plots of HD_{intra} and CC_{intra} for all 630 pairs of keys at temperatures of −25 °C, 0 °C, 25 °C, and 50 °C. Once again, the $\mu_{HD-intra}$ and $\mu_{CC-intra}$ values were found to be close to 18 and 0, respectively, demonstrating the robustness and resilience of our TRNG against temperature variations. It must be noted that the digital keys were obtained using V_p = −7 V, V_e = 14 V, and V_{read} = −3 and 3 V for WSe_2 and WS_2 FETs, respectively, for both the V_{DS} and temperature variation studies. In addition, we found that our FG 2D FETs are stable over 60 days (SI 12), an attribute which is critical toward their successful integration in developing future hardware security primitives.

CONCLUSION

In conclusion, we have experimentally demonstrated an FG 2D FET-based TRNG by exploiting the cycle-to-cycle variation in programmed/erased device characteristics originating from the inherent stochasticity in the carrier trapping/detrapping mechanism in the FG stack. Digital keys constructed using our TRNG demonstrate near ideal entropy, uniformity, distinctness, and lack of correlation, and pass NIST randomness tests without any postprocessing. Furthermore, we demonstrate that the FG 2D FET-based TRNGs are unclonable and resilient against ML attacks based on predictive regression models. The energy consumption for random bit generation was miniscule and on the order of ∼10pJ/bit. Finally, we evaluated the robustness of our TRNG against supply bias and temperature variations. Our findings shows the promise of programmable 2D FETs in hardware security applications for energy-constrained IoT edge devices.

METHODS

Back-Gate Stack Fabrication. Replacing thermally oxidized SiO_2 with a high-k dielectric such as Al_2O_3 is a logical choice for scaling the effective oxide thickness (EOT). However, we found that Al_2O_3/P^{++}–Si interface is not ideal for the fabrication of back-gated FETs due to higher leakage current, additional interface trap states, and larger hysteresis which negatively impacts the device performance. Replacing Si with Pt, a large work function metal (5.6 eV), reduces hysteresis and trap state effects.[52] Since Pt readily forms a Pt silicide at temperatures as low as 300 °C, a 20 nm TiN diffusion barrier was deposited via reactive sputtering between the P^{++}–Si and Pt to allow high temperature processing.[53] This conductive TiN diffusion barrier allows the back-gate voltage to be applied to the substrate, thus simplifying the fabrication and measurement procedures. The polycrystalline Pt introduces very little surface roughness to the final Al_2O_3 surface, which sports an rms roughness of 0.7 nm.

Device Fabrication. Multilayer WSe_2 and WS_2 TMD flakes were mechanically exfoliated onto the described Al2O3/Pt/TiN/p^{++}-Si substrate. The transferred flakes were mapped in terms of their location and dimensions using an optical microscope. The sample is then spin coated with EL6 and A3 PMMA followed by baking at 150

https://doi.org/10.1021/acsnano.1c05984
ACS Nano 2021, 15, 17804–17812

and 180 °C, respectively, to get rid of any excess solvent. Source and drain (S/D) contacts are patterned and defined using electron-beam lithography and developed using a 1:1 mixture of 4-methyl −2-pentanone (MIBK) and Iso-propyl alcohol (IPA) for 60s. The sample is then rinsed using IPA for 45s to remove any excess developing solution. 40 nm of Nickel (Ni) and 30 nm of Gold (Au) are then deposited using electron-beam evaporation. Finally, lift-off of the evaporated materials is done by immersing the sample in Acetone for 30 min followed by a final rinse with IPA.

Electrical Characterization. Electrical characterization of the fabricated devices are performed using Lake Shore CRX-VF probe station under atmospheric conditions and at room temperature using a Keysight B1500A parameter analyzer. Temperature measurements were performed in air using Form Factor 11000 ATT-C60 probe station and a Keysight B1500A parameter analyzer.

ASSOCIATED CONTENT

Supporting Information

The Supporting Information is available free of charge at https://pubs.acs.org/doi/10.1021/acsnano.1c05984.

Floating gate (FG) pulsing schematic consisting of three consecutive pulses: a programming pulse (V_p), an erase pulse (V_e), and a read voltage (V_{read}), each with a pulse width (τ_s) of 100 ms, I_{DS} values extracted using V_p of −9 V and V_e of 14 V for different V_{read} values for WSe_2 and WS_2 FETs along with their corresponding Gaussian distributions. Distribution of I_{DS} values extracted using different $V_p$and V_{read} values for WSe_2 and WS_2 FETs. Uniformity and entropy for 36 keys extracted using different combinations of V_p and V_{read} from WSe_2 FETs. Uniformity and entropy for 36 keys extracted using different combinations of V_p and V_{read} from WS_2 FETs. Distribution of intrahamming distance (HD_{intra}) for keys obtained using different combination of V_p and V_{read} from WSe_2 FETs. Distribution of intrahamming distance (HD_{intra}) for keys obtained using different combination of V_p and V_{read} from WS_2 FETs. Distribution of intracorrelation coefficient (CC_{intra}) for keys obtained using different combinations of V_p and V_{read} from WSe_2 FETs. Distribution of intracorrelation coefficient (CC_{intra}) for keys obtained using different combinations of V_p and V_{read} from WS_2 FETs. Specified NIST test results. Energy expenditure for bit generation process (E_{TRN}) as a function of V_p and V_{read} for WSe_2 and WS_2 FETs. stability of WSe_2 and WS_2 FETs measured 60 days apart (PDF)

AUTHOR INFORMATION

Corresponding Author

Saptarshi Das − *Electrical Engineering and Computer Science, Engineering Science and Mechanics, and Materials Science and Engineering, Penn State University, University Park, Pennsylvania 16802, United States; Materials Research Institute, Pennsylvania State University, University Park, Pennsylvania 16802, United States;* orcid.org/0000-0002-0188-945X; Email: sud70@psu.edu, das.sapt@gmail.com

Authors

Akshay Wali − *Electrical Engineering and Computer Science, Penn State University, University Park, Pennsylvania 16802, United States*

Harikrishnan Ravichandran − *Engineering Science and Mechanics, Penn State University, University Park, Pennsylvania 16802, United States*

Complete contact information is available at: https://pubs.acs.org/10.1021/acsnano.1c05984

Notes

The authors declare no competing financial interest.

ACKNOWLEDGMENTS

This work was supported by the National Science Foundation (NSF) through CAREER Award under Grant Number ECCS-2042154.

REFERENCES

(1) Tariq, N.; Asim, M.; Al-Obeidat, F.; Zubair Farooqi, M.; Baker, T.; Hammoudeh, M.; Ghafir, I. The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey. *Sensors* **2019**, *19* (8), 1788.

(2) Alaba, F. A.; Othman, M.; Hashem, I. A. T.; Alotaibi, F. Internet of Things Security: A Survey. *Journal of Network and Computer Applications* **2017**, *88*, 10−28.

(3) van der Leest, V.; Maes, R.; Schrijen, G.-J.; Tuyls, P., Hardware Intrinsic Security to Protect Value in the Mobile Market. In *ISSE 2014 Securing Electronic Business Processes*, 1st ed; Springer: Vieweg, Wiesbaden, 2014; *13*; pp 188−198.

(4) Bulgurcu, B.; Cavusoglu, H.; Benbasat, I. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly* **2010**, *34*, 523−548.

(5) Dutang, C.; Wuertz, D. A Note on Random Number Generation. In *Overview of Random Generation Algorithms*, 2009; p 2.

(6) Kelsey, J.; Schneier, B.; Wagner, D.; Hall, C. Cryptanalytic Attacks on Pseudorandom Number Generators. In *International Workshop on Fast Software Encryption*, 5th ed; Lecture Notes in Computer Science; Springer: Berlin, Heidelberg, 1998; *1372*; pp 168−188.

(7) Dorrendorf, L.; Gutterman, Z.; Pinkas, B. Cryptanalysis of the Random Number Generator of the Windows Operating System. *ACM Transactions on Information and System Security (TISSEC)* **2009**, *13* (1), 1−32.

(8) Wen, Y.; Yu, W. Machine Learning-Resistant Pseudo-Random Number Generator. *Electron. Lett.* **2019**, *55* (9), 515−517.

(9) Lavington, S. H. The Manchester Mark I and Atlas: A Historical Perspective. *Commun. ACM* **1978**, *21* (1), 4−12.

(10) Bucci, M.; Germani, L.; Luzzi, R.; Trifiletti, A.; Varanonuovo, M. A High-Speed Oscillator-Based Truly Random Number Source for Cryptographic Applications on a Smart Card IC. *IEEE Trans. Comput.* **2003**, *52* (4), 403−409.

(11) Tokunaga, C.; Blaauw, D.; Mudge, T. True Random Number Generator with a Metastability-Based Quality Control. *IEEE J. Solid-State Circuits* **2008**, *43* (1), 78−85.

(12) Petrie, C. S.; Connelly, J. A. A Noise-Based IC Random Number Generator for Applications in Cryptography. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* **2000**, *47* (5), 615−621.

(13) Yasuda, S.; Satake, H.; Tanamoto, T.; Ohba, R.; Uchida, K.; Fujita, S. Physical Random Number Generator Based on MOS Structure after Soft Breakdown. *IEEE J. Solid-State Circuits* **2004**, *39* (8), 1375−1377.

(14) Brederlow, R.; Prakash, R.; Paulus, C.; Thewes, R. A Low-Power True Random Number Generator Using Random Telegraph Noise of Single Oxide-Traps. In *International Solid State Circuits Conference-Digest of Technical Papers, Proceedings of the 1st International Solid State Circuits Conference, San Francisco, CA*, 1st ed; Amiri, M.; Gulak, G.; Mirabbsi, S.; Smith, K. C.; Spencer, R., Eds.; IEEE: ME, 6−9 Feb, 2006; 3, pp 1666−1675.

(15) Yang, K.; Blaauw, D.; Sylvester, D. An All-Digital Edge Racing True Random Number Generator Robust against PVT Variations. *IEEE J. Solid-State Circuits* **2016**, *51* (4), 1022−1031.
(16) Bae, S.-G.; Kim, Y.; Park, Y.; Kim, C. 3-Gb/S High-Speed True Random Number Generator Using Common-Mode Operating Comparator and Sampling Uncertainty of D Flip-Flop. *IEEE J. Solid-State Circuits* **2017**, *52* (2), 605−610.
(17) Kim, M.; Ha, U.; Lee, K. J.; Lee, Y.; Yoo, H.-J. A 82-Nw Chaotic Map True Random Number Generator Based on a Sub-Ranging SAR ADC. *IEEE J. Solid-State Circuits* **2017**, *52* (7), 1953−1965.
(18) Cicek, I.; Pusane, A. E.; Dundar, G. A New Dual Entropy Core True Random Number Generator. *Analog Integrated Circuits and Signal Processing* **2014**, *81* (1), 61−70.
(19) Jiang, H.; Belkin, D.; Savel'ev, S. E.; Lin, S.; Wang, Z.; Li, Y.; Joshi, S.; Midya, R.; Li, C.; Rao, M. A Novel True Random Number Generator Based on a Stochastic Diffusive Memristor. *Nat. Commun.* **2017**, *8* (1), 1−9.
(20) Pickett, M. D.; Williams, R. S. Sub-100 Fj and Sub-Nanosecond Thermally Driven Threshold Switching in Niobium Oxide Crosspoint Nanodevices. *Nanotechnology* **2012**, *23* (21), 215202.
(21) Torrezan, A. C.; Strachan, J. P.; Medeiros-Ribeiro, G.; Williams, R. S. Sub-Nanosecond Switching of a Tantalum Oxide Memristor. *Nanotechnology* **2011**, *22* (48), 485203.
(22) Pi, S.; Lin, P.; Xia, Q. Cross Point Arrays of 8 nm× 8 nm Memristive Devices Fabricated with Nanoimprint Lithography. *J. Vac. Sci. Technol., B: Nanotechnol. Microelectron.: Mater., Process., Meas., Phenom.* **2013**, *31* (6), 06FA02.
(23) 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.
(24) Alharbi, A.; Armstrong, D.; Alharbi, S.; Shahrjerdi, D. Physically Unclonable Cryptographic Primitives by Chemical Vapor Deposition of Layered MoS2. *ACS Nano* **2017**, *11* (12), 12772−12779.
(25) Chen, H.; Song, M.; Guo, Z.; Li, R.; Zou, Q.; Luo, S.; Zhang, S.; Luo, Q.; Hong, J.; You, L. Highly Secure Physically Unclonable Cryptographic Primitives Based on Interfacial Magnetic Anisotropy. *Nano Lett.* **2018**, *18* (11), 7211−7216.
(26) Shao, B.; Choy, T. H.; Zhou, F.; Chen, J.; Wang, C.; Park, Y. J.; Ahn, J.-H.; Chai, Y. Crypto Primitive of MOCVD MoS 2 Transistors for Highly Secured Physical Unclonable Functions. *Nano Res.* **2021**, *14* (6), 1784−1788.
(27) Li, P.; Wang, Y.-C.; Zhang, J.-Z. All-Optical Fast Random Number Generator. *Opt. Express* **2010**, *18* (19), 20360−20369.
(28) Wei, W.; Xie, G.; Dang, A.; Guo, H. High-Speed and Bias-Free Optical Random Number Generator. *IEEE Photonics Technol. Lett.* **2012**, *24* (6), 437−439.
(29) Kanter, I.; Aviad, Y.; Reidler, I.; Cohen, E.; Rosenbluh, M. An Optical Ultrafast Random Bit Generator. *Nat. Photonics* **2010**, *4* (1), 58−61.
(30) Hai-Qiang, M.; Su-Mei, W.; Da, Z.; Jun-Tao, C.; Ling-Ling, J.; Yan-Xue, H.; Ling-An, W. A Random Number Generator Based on Quantum Entangled Photon Pairs. *Chin. Phys. Lett.* **2004**, *21* (10), 1961.
(31) Stipčević, M.; Rogina, B. M. Quantum Random Number Generator Based on Photonic Emission in Semiconductors. *Rev. Sci. Instrum.* **2007**, *78* (4), 045104.
(32) Dynes, J. F.; Yuan, Z. L.; Sharpe, A. W.; Shields, A. J. A High Speed, Postprocessing Free, Quantum Random Number Generator. *Appl. Phys. Lett.* **2008**, *93* (3), 031109.
(33) Rarity, J. G.; Owens, P.; Tapster, P. Quantum Random-Number Generation and Key Sharing. *J. Mod. Opt.* **1994**, *41* (12), 2435−2444.
(34) Sanguinetti, B.; Martin, A.; Zbinden, H.; Gisin, N. Quantum Random Number Generation on a Mobile Phone. *Phys. Rev. X* **2014**, *4* (3), 031056.
(35) Bierhorst, P.; Knill, E.; Glancy, S.; Zhang, Y.; Mink, A.; Jordan, S.; Rommal, A.; Liu, Y.-K.; Christensen, B.; Nam, S. W. Experimentally Generated Randomness Certified by the Impossibility of Superluminal Signals. *Nature* **2018**, *556* (7700), 223−226.
(36) 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.
(37) Wali, A.; Dodda, A.; Wu, Y.; Pannone, A.; Usthili, L. K. R.; Ozdemir, S. K.; Ozbolat, I. T.; Das, S. Biological Physically Unclonable Function. *Communications Physics* **2019**, *2* (1), 1−10.
(38) Meiser, L. C.; Koch, J.; Antkowiak, P. L.; Stark, W. J.; Heckel, R.; Grass, R. N. DNA Synthesis for True Random Number Generation. *Nat. Commun.* **2020**, *11* (1), 1−9.
(39) Manzeli, S.; Ovchinnikov, D.; Pasquier, D.; Yazyev, O. V.; Kis, A. 2D Transition Metal Dichalcogenides. *Nature Reviews Materials* **2017**, *2* (8), 1−15.
(40) Liu, L.; Lu, Y.; Guo, J. On Monolayer ${\Rm Mos} _ {2} $ Field-Effect Transistors at the Scaling Limit. *IEEE Trans. Electron Devices* **2013**, *60* (12), 4133−4139.
(41) Desai, S. B.; Madhvapathy, S. R.; Sachid, A. B.; Llinas, J. P.; Wang, Q.; Ahn, G. H.; Pitner, G.; Kim, M. J.; Bokor, J.; Hu, C. Mos2 Transistors with 1-Nanometer Gate Lengths. *Science* **2016**, *354* (6308), 99−102.
(42) Wali, A.; Kundu, S.; Arnold, A. J.; Zhao, G.; Basu, K.; Das, S. Satisfiability Attack-Resistant Camouflaged Two-Dimensional Heterostructure Devices. *ACS Nano* **2021**, *15* (2), 3453−3467.
(43) Wu, P.; Reis, D.; Hu, X. S.; Appenzeller, J. Two-Dimensional Transistors with Reconfigurable Polarities for Secure Circuits. *Nature Electronics* **2021**, *4* (1), 45−53.
(44) Dodda, A.; Radhakrishnan, S. S.; Schranghamer, T. F.; Buzzell, D.; Sengupta, P.; Das, S. Graphene-Based Physically Unclonable Functions That Are Reconfigurable and Resilient to Machine Learning Attacks. *Nature Electronics* **2021**, *4*, 1−11.
(45) Wen, C.; Li, X.; Zanotti, T.; Puglisi, F. M.; Shi, Y.; Saiz, F.; Antidormi, A.; Roche, S.; Zheng, W.; Liang, X. Advanced Data Encryption Using 2D Materials. *Adv. Mater.* **2021**, *33*, 2100185.
(46) Schulman, D. S.; Arnold, A. J.; Das, S., Contact Engineering for 2D Materials and Devices. *Chem. Soc. Rev.* **2018**.473037
(47) Das, S.; Appenzeller, J. WSe2 Field Effect Transistors with Enhanced Ambipolar Characteristics. *Appl. Phys. Lett.* **2013**, *103* (10), 103501.
(48) Sebastian, A.; Pendurthi, R.; Choudhury, T. H.; Redwing, J. M.; Das, S. Benchmarking Monolayer MoS2 and WS2 Field-Effect Transistors. *Nat. Commun.* **2021**, *12* (1), 693.
(49) Jayachandran, D.; Oberoi, A.; Sebastian, A.; Choudhury, T. H.; Shankar, B.; Redwing, J. M.; Das, S. A Low-Power Biomimetic Collision Detector Based on an In-Memory Molybdenum Disulfide Photodetector. *Nature Electronics* **2020**, *3* (10), 646−655.
(50) Bassham, III, L. E.; Rukhin, A. L.; Soto, J.; Nechvatal, J. R.; Smid, M. E.; Barker, E. B.; Leigh, S. D.; Levenson, M.; Vangel, M.; Banks, D. L. *Sp 800−22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*; National Institute of Standards & Technology: Gaithersburg, MD, 2010.
(51) Rührmair, U.; Sölter, 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 Transactions on Information Forensics and Security* **2013**, *8* (11), 1876−1891.
(52) Rumble, J. R. *CRC Handbook of Chemistry and Physics*, 98th ed.; CRC Press, Taylor & Francis: Boca Raton, FL, Internet Version 2018.
(53) Crider, C.; Poate, J.; Rowe, J.; Sheng, T. Platinum Silicide Formation under Ultrahigh Vacuum and Controlled Impurity Ambients. *J. Appl. Phys.* **1981**, *52* (4), 2860−2868.

https://doi.org/10.1021/acsnano.1c05984
ACS Nano 2021, 15, 17804−17812