ACS NANO

www.acsnano.org

ARTICLE

# A Peripheral-Free True Random Number Generator Based on Integrated Circuits Enabled by Atomically Thin Two-Dimensional Materials

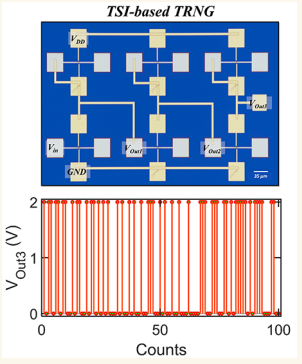
Harikrishnan Ravichandran, Dipanjan Sen, Akshay Wali, Thomas F. Schranghamer, Nicholas Trainor, Joan M. Redwing, Biswajit Ray, and Saptarshi Das*

Cite This: *ACS Nano* 2023, 17, 16817−16826

Read Online

ACCESS | Metrics & More | Article Recommendations | Supporting Information

**ABSTRACT:** **A true random number generator (TRNG) is essential to ensure information security for Internet of Things (IoT) edge devices. While pseudorandom number generators (PRNGs) have been instrumental, their deterministic nature limits their application in security-sensitive scenarios. In contrast, hardware-based TRNGs derived from physically unpredictable processes offer greater reliability. This study demonstrates a peripheral-free TRNG utilizing two cascaded three-stage inverters (TSIs) in conjunction with an *XOR* gate composed of monolayer molybdenum disulfide ($MoS_2$) field-effect transistors (FETs) by exploiting the stochastic charge trapping and detrapping phenomena at and/or near the $MoS_2$/dielectric interface. The entropy source passes the NIST SP800-90B tests with a minimum normalized entropy of 0.8780, while the generated bits pass the NIST SP800-22 randomness tests without any postprocessing. Moreover, the keys generated using these random bits are uncorrelated with near-ideal entropy, bit uniformity, and Hamming distances, exhibiting resilience against machine learning (ML) attacks, temperature variations, and supply bias fluctuations with a frugal energy expenditure of 30 pJ/bit. This approach offers an advantageous alternative to conventional silicon, memristive, and nanomaterial-based TRNGs as it obviates the need for extensive peripherals while harnessing the potential of atomically thin 2D materials in developing low-power TRNGs.**




**KEYWORDS:** *Random numbers, Charge trapping and detrapping, Field effect transistors, 2D materials, Peripheral-free, Integrated circuits, Hardware security*



The explosive growth of global data exchange has necessitated the development of highly secure information systems to ensure data integrity, confidentiality, and authentication. A true random number generator (TRNG) is one such cryptographic primitive which offers that security.[1,2] Besides security, TRNGs are also employed in machine learning (ML), image processing, and weather forecasting, among others.[3−5] Software-based RNGs, also known as pseudo-RNGs (PRNGs), expand mathematical seeds into bit sequences using a polynomial algorithm.[6−8] However, they are often vulnerable to security attacks due to the deterministic nature of their initial seed, making them inadequate for ensuring the security of Internet of Things (IoT) edge devices. In contrast, a TRNG generates statistically independent bits by utilizing a physical attribute of a hardware system which is random and unpredictable, therefore making it less susceptible to security attacks.[9]

State-of-the-art complementary metal-oxide-semiconductor (CMOS)-based TRNGs such as bit-latch,[10−12] ring oscillator (RO) jitter,[13] and bit-line static random-access memory (SRAM) cells[14] primarily utilize thermal noise as their entropy source for the generation of random bits. However, postprocessing units such as von Neumann correctors are often required to remove residual biases and correlations among the generated random bits. Additionally, CMOS-derived TRNGs are known to suffer from low entropy and require peripherals to eliminate device mismatches. Recent years have also witnessed the development of stochastic

Received: April 21, 2023
Accepted: August 16, 2023
Published: August 24, 2023




https://doi.org/10.1021/acsnano.3c03581
*ACS Nano* 2023, 17, 16817−16826

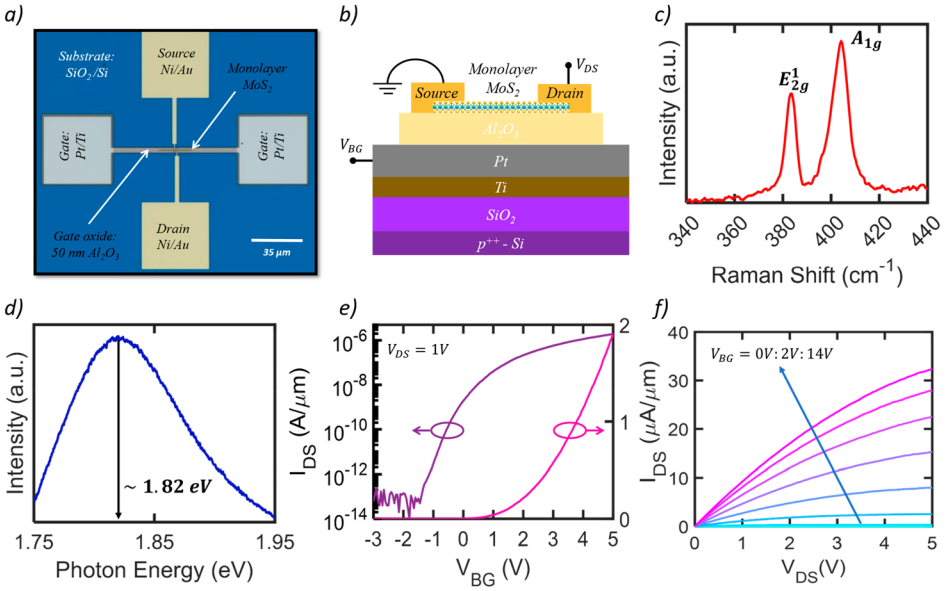



**Figure 1. Monolayer $MoS_2$ characterization and FET fabrication. (a) Optical image and (b) schematic of a representative monolayer $MoS_2$ FET. Each device is fabricated on a predefined local back-gate island consisting of a platinum/titanium (Pt/Ti) gate electrode and a 50 nm ALD-grown $Al_2O_3$ dielectric stack. Monolayer $MoS_2$ serves as the channel material, with Ni/Au (40/30 nm) as the source and drain contact pads. Each monolayer $MoS_2$ FET has a channel length ($L$) of 1 $\mu$m and a channel width ($W$) of 1 $\mu$m. (c) Raman and (d) photoluminescence (PL) spectra, respectively, obtained from a representative transferred $MoS_2$ film where the characteristic in-plane $E^1_{2g}$ mode and out-of-plane $A_{1g}$ mode were observed at 385 and 403 $cm^{-1}$, respectively, with the PL peak at 1.82 eV. (f) Transfer characteristics, i.e., source-to-drain current ($I_{DS}$) plotted with respect to the local back-gate voltage ($V_{BG}$), of a representative monolayer $MoS_2$ FET measured at a source-to drain-bias ($V_{DS}$) of 1 V and plotted in the logarithmic and linear scales. A clear n-type dominated carrier transport is observed. (g) Plot of the output characteristics where $I_{DS}$ is plotted against $V_{DS}$ as a function of different $V_{BG}$ biases with excellent $I_{ON}$ values of 32 $\mu$A/$\mu$m for $V_{DS}$ = 5 V at $V_{BG}$ = 14 V.**

switching mechanisms in memristors,[15,16] random spin flips in magnetic devices,[17] polarization switching in ferroelectric materials,[18] and stochastic charge trapping in nanoscale devices[9,19] as high entropy sources for generating TRNGs. However, integrating peripherals such as comparators, logic gates, registers, and counters increases their energy and area overheads, posing a challenge in enabling a peripheral-free TRNG for low-power security solutions in emerging IoT devices.

In this paper, we demonstrate a peripheral-free TRNG by exploiting the inherent stochasticity in the voltage transfer characteristics (VTC) of two cascaded three-stage inverters (TSI) in conjunction with an *XOR* gate based on monolayer molybdenum disulfide ($MoS_2$) field-effect transistors (FETs) utilizing atomic layer deposition (ALD) grown $Al_2O_3$ as the gate dielectric. The fluctuations in the VTC are attributed to the stochastic nature of charge trapping and detrapping at and/or near the $Al_2O_3/MoS_2$ interface.[9,20−22] Subsequently, the stochastic voltage fluctuations obtained from the two TSIs are fed to the logical *XOR* gate to generate a total of 256 random bit keys, each 256 bits long. Examination of the strength of randomness reveals that the generated keys are uncorrelated, exhibiting near-ideal entropy, Hamming distances, and uniformity. The generated random bits pass the NIST SP800-22 randomness tests without any postprocessing. Additionally, the entropy source of our TSI-based TRNG passes the specified NIST SP 800-90B tests with a minimum normalized entropy of 0.8780 and an average entropy of 0.8875, which is at par with other advanced TRNGs.[23−25] Our TRNG consumes a miniscule energy of 30 pJ/bit and requires no peripherals or postprocessing elements. Moreover, our TRNG was also found to be physically unclonable and resilient to regression-based attack models, temperature variations, and supply bias fluctuations. Our results highlight the importance of integrating nanomaterials and exploiting interfacial phenomena with innovative circuit designs to realize energy-efficient TRNGs for resource-constrained IoT applications.

## RESULTS

**Fabrication and Characterization of 2D FETs Based on Monolayer $MoS_2$.** Our choice of using $MoS_2$ as the channel material stems from its technological maturity in comparison to other transition metal dichalcogenide (TMD) channel materials. This is evident through recent demonstrations in sensing,[26,27] computing,[21,22,28] storage,[29] and communication[30] domains. Therefore, augmenting hardware security primitives has the potential to accelerate their adoption process and make them more attractive for IoT implementation.[31] In this context, some of the recently demonstrated hardware security applications[20,32−34] with $MoS_2$ as the channel material are encouraging. Before the operational assessment of our $MoS_2$ TSI-based TRNG, we first evaluated the quality of the grown $MoS_2$ film. Figure 1a,b, respectively, show the optical image and a schematic of a representative back-gated 2D FET based on monolayer $MoS_2$ grown via a metal−organic chemical vapor deposition (MOCVD) technique on an epitaxial sapphire substrate at 950 °C. Figure 1c,d, respectively, show the Raman and PL spectra obtained from a representative monolayer film where the in-plane $E^1_{2g}$ and out-of-plane $A_{1g}$ Raman active modes were observed at 385 and 403 $cm^{-1}$, respectively, with a peak


https://doi.org/10.1021/acsnano.3c03581
ACS Nano 2023, 17, 16817−16826

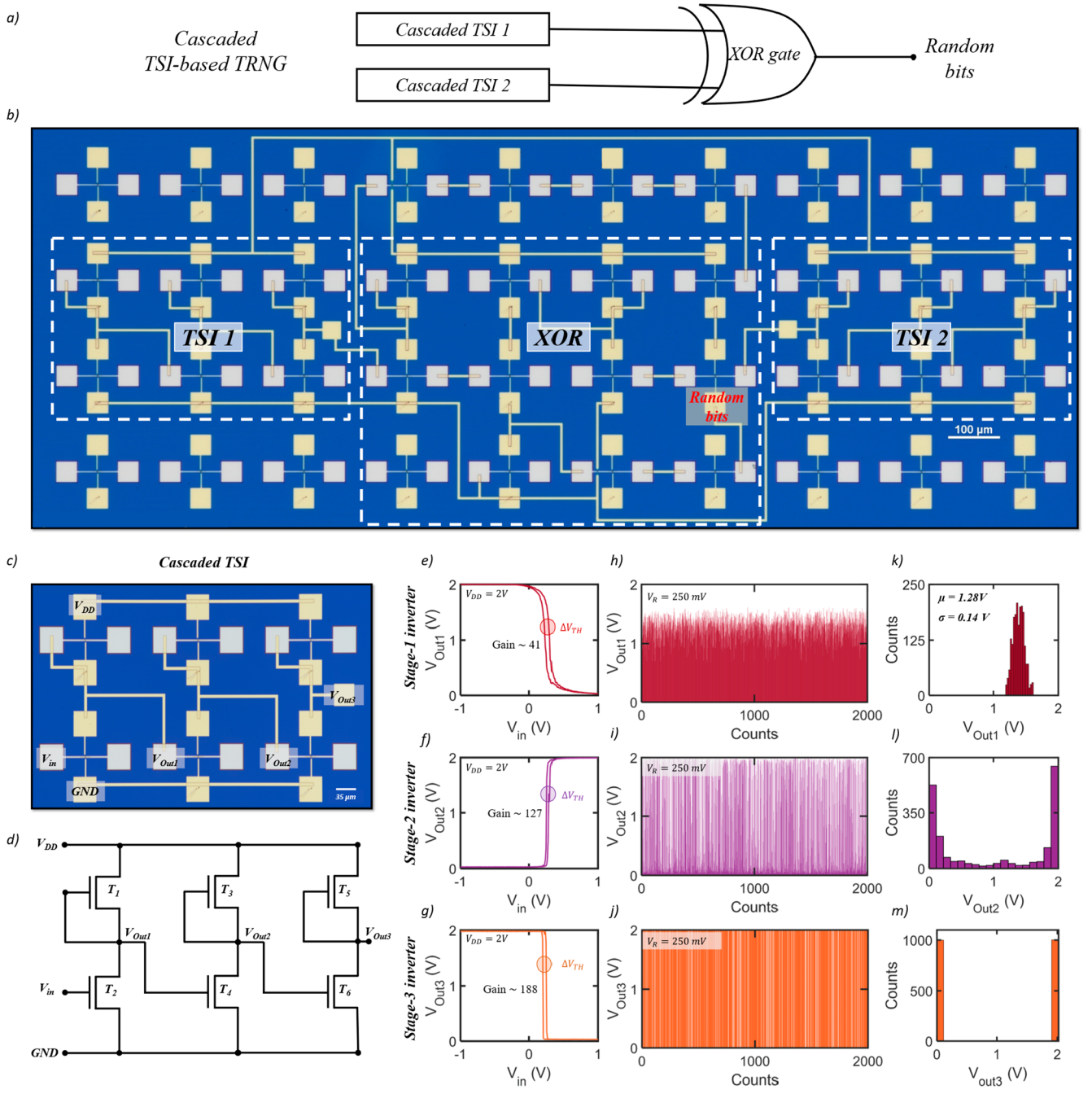



**Figure 2. Monolayer $MoS_2$ cascaded TSI-based TRNG. (a) Schematic and (b) optical image of the cascaded TSI-based TRNG consisting of two cascaded TSIs and an *XOR* gate. (c) Optical image and (d) corresponding circuit schematic of a cascaded TSI consisting of three inverters connected in series where the $V_{Out}$ from a single inverter is fed as the $V_{in}$ to the next stage inverter. Voltage transfer characteristics (*VTC*) of (e) stage 1, (f) stage 2, and (g) stage 3 of the cascaded TSI, respectively, for $V_{DD}$ = 2 V. The gain of the stage 1, stage 2, and stage 3 inverters was found to be 41, 127, and 188, respectively. Stochastic fluctuation was observed for (h) stage 1 ($V_{Out1}$) (i) stage 2 ($V_{Out2}$) and (j) stage 3 ($V_{Out3}$) inverters measured at $V_R$ = 250 mV with a sampling rate $\tau_s$ = 5 ms, respectively. (k) Distribution of measured $V_{Out}$ for stage 1 ($V_{Out1}$) following a Gaussian random distribution with a mean of 1.28 V and standard deviation of 0.14 V. (l) Distribution of measured $V_{Out}$ for stage 2 ($V_{Out2}$). The measured $V_{Out2}$ follows a broadened two-tailed Gaussian distribution owing to the higher gain of the stage 2 inverter. (m) Distribution of measured $V_{Out}$ for stage 3 ($V_{Out3}$) of the cascaded TSI. The $V_{Out3}$ stochastically fluctuates between the lower logic level (0 V) and higher logic level (2 V) of the third stage inverter, which forms the basis of TSI-based on-chip TRNG.**

separation of 18 $cm^{-1}$. The PL peak position was observed at 1.82 eV, which is consistent with a monolayer $MoS_2$ film.

Next, $MoS_2$ FETs were fabricated on local islands consisting of an atomic layer deposition (ALD)-grown 50 nm $Al_2O_3$ gate dielectric stack with electron beam (e-beam) evaporated 20 nm of titanium (Ti) and 50 nm of platinum (Pt) as the back-gate electrode on a commercially purchased $SiO_2/p^{++}$-Si substrate. The $Al_2O_3$ layer was dry-etched using $BCl_3$ at 5 °C to access the local back-gate. Monolayer $MoS_2$ was then transferred onto the local back-gate islands using a poly-(methyl) methacrylate (PMMA)-assisted wet transfer technique. The device channel was patterned using e-beam


https://doi.org/10.1021/acsnano.3c03581
ACS Nano 2023, 17, 16817−16826

lithography followed by reactive ion etching (RIE) using $SF_6$ plasma at 5 °C to define its geometry ($L$ = 1 $\mu$m and $W$ = 1 $\mu$m). The source/drain contacts were patterned using e-beam lithography followed by e-beam evaporation of 40/30 nm nickel/gold (Ni/Au). Interconnects (60 nm Ni and 40 nm Au) were then defined and deposited to connect individual devices for circuit formation. Further details on monolayer $MoS_2$ synthesis, film transfer, and fabrication of the local back-gate gate islands and $MoS_2$ FETs can be found in the **Methods** section and our previous works.[21,22,28,32,33,35−37] The electrical response of the $MoS_2$ FETs was assessed by measuring its transfer characteristics in both logarithmic and linear scale where the source-to-drain current ($I_{DS}$) was plotted against the local back-gate voltage ($V_{BG}$) at a drain-to-source voltage ($V_{DS}$) of 1 V. With an expected dominant *n*-branch, as shown in Figure 1e, an ON/OFF ratio of ∼$10^7$, a subthreshold slope ($SS$) of 250 mV/decade averaged over three orders of $I_{DS}$ change, and low gate leakage current, our FETs demonstrate impressive gate electrostatic control. Finally, output characteristics, as shown in Figure 1f for the same representative $MoS_2$ FET, reveal good performance with the ON-state current ($I_{ON}$) reaching ∼32 $\mu$A/$\mu$m for $V_{DS}$ = 5 V and $V_{BG}$ = 14 V.

**Monolayer $MoS_2$ FET-Based Cascaded TSI as a TRNG.** To demonstrate our TRNG, two cascaded TSI circuits and an *XOR* logic gate were constructed using $MoS_2$ FETs. Figure 2a,b, respectively, show the schematic and the optical image of the TRNG, where the outputs from the cascaded TSIs were fed as inputs to the *XOR* gate to generate the random bits. A TSI consists of three inverters cascaded in series, where the output from one inverter is fed as an input to the next inverter. Figure 2c,d, respectively, show the optical image and circuit schematic of a representative 2D TSI circuit comprising six $MoS_2$ FETs ($T_1$ through $T_6$). Note that each inverter consists of two $MoS_2$ FETs and that the source and gate terminals of $T_1$, $T_3$, and $T_5$ are shorted as depletion loads, thus enabling inverter operation. Figure 2e−g show the dual sweep VTC, i.e., the output voltage ($V_{Out}$) versus the input voltage ($V_{in}$), for the first ($V_{Out1}$), second ($V_{Out2}$), and third stage ($V_{Out3}$) of the TSI, respectively, when $V_{in}$ is swept from −1 V to 1 V for a supply voltage ($V_{DD}$) of 2 V. Note that the transition between the two logic levels becomes steeper, or in other words, that the gain, which is defined as the slope of the VTC at the switching threshold, increases with an increasing number of stages. For our demonstration, the gain was found to be 41, 127, and 188 for the 1st, 2nd, and 3rd stages of the TSI, respectively.

An interesting aspect of the TSI VTC is the presence of a finite hysteresis window ($\Delta V_{TH}$), which is attributed to the presence of trap states at and/or near the $MoS_2/Al_2O_3$ interface. As reported in earlier studies,[9,21,22] the intrinsic stochasticity of the carrier trapping/detrapping process within the trap states can be successfully exploited as the source of randomness for our TRNG. Figure 2h−j show the output ($V_{Out}$) plots for the 1st, 2nd, and 3rd TSI stages, respectively, measured at a read voltage ($V_R$) of 250 mV with a sampling rate ($\tau_s$) of 5 ms; Figure 2k−m, respectively, show their corresponding distribution. Note that we used a supply voltage ($V_{DD}$) of 2 V for our operations. Interestingly, while the fluctuations in $V_{Out1}$ follow a Gaussian random distribution with a mean ($\mu_{VOut1}$) of 1.28 V and standard deviation ($\sigma_{VOut1}$) of 0.14 V, $V_{Out2}$ and $V_{Out3}$ instead follow a broadened two-tailed Gaussian distribution and a delta-like distribution, respectively, owing to increasing switching transitions in the subsequent TSI stages. In other words, $V_{Out3}$ toggles randomly between the lower (0 V) and higher logic levels (2 V). Note that it is also critical to have a $V_R$ which lies within the $\Delta V_{TH}$ for observing maximum stochasticity corresponding to the trapping/detrapping process. Finally, the random bits were obtained by feeding $V_{Out3}$ from the two TSIs to the *XOR* gate. Supporting Information (SI), Figure S1 shows similar output plots generated from the second TSI and SI, Figure S2 shows the optical image, circuit schematic, and output characteristics for our $MoS_2$-based *XOR* gate. Overall, while the TSI amplifies the stochastic fluctuations, the *XOR* operation generates output voltage trains that are random in nature, which is critical for eliminating the need for peripheral circuits. Because the TSI fluctuations are stochastic, the *XOR* output also fluctuates stochastically, generating random bitstreams. The energy expenditure per bit generation was found to be miniscule at ∼30 pJ/bit. SI, Figure S3 shows the details of the energy expenditure calculations.

**Assessment of Quality of Random Bits through NIST tests.** Before the evaluation of the cryptographic security, three sequences obtained from the TRNG, each comprising $10^6$ random bitstreams, were assessed using the statistical test NIST SP800-90B test suite developed by the National Institute of Standards and Technology (NIST).[38] The test focuses on assessing the unpredictability and randomness of the entropy source. The implementation of this test involves the identification of the track as either independent and identically distributed (IID) or non-IID followed by the estimation of the minimum entropy. Table 1 shows the results of the NIST SP800-90B test under the non-IID track, where the minimum entropy obtained from the compression test was found to be 0.8838, 0.9006, and 0.8780, respectively, for the three sequences. Moreover, the performance of the restart test on the random sequences, for which 1000 bits were collected by restarting the entropy source 1000 times, was also carried out successfully. With a minimum normalized entropy of 0.8780 and an average minimum entropy of 0.8875, our results are at par with earlier studies that utilize frequency collapse in multimodal ring oscillators (RO),[23,39] jitter in RO,[24] metastability in latches,[40] and natural decay in radio isotopes[25] as entropy sources. After collecting the bit streams, they were subjected to test protocols under the NIST SP800-22 tests assessing a particular null hypothesis, which assumes that the sequence is random. The evaluation produces a *p*-value with a 99% confidence level. For the bits to be deemed random, the *p*-value must exceed 0.01. All three generated random bit sequences pass all of the 15 NIST SP800-22 tests without any

**Table 1. NIST SP 800-90B Test Results**

| Non-IID estimators | Entropy rate | | |
|---|---|---|---|
| | Sequence 1 | Sequence 2 | Sequence 3 |
| Most common value | 0.9956 | 0.9942 | 0.9949 |
| Collision | 0.9105 | 0.9105 | 0.9241 |
| Markov | 0.9988 | 0.9963 | 0.9979 |
| Compression | 0.8838 | 0.9006 | 0.8780 |
| t-tuple | 0.9433 | 0.9330 | 0.9381 |
| Longest repeated substring (LRS) | 0.9281 | 0.9148 | 0.9176 |
| Multi most common | 0.9943 | 0.9959 | 0.9940 |
| Lag prediction | 0.9963 | 0.9961 | 0.9952 |
| Multi MMC prediction | 0.9968 | 0.9954 | 0.9983 |
| LZ78Y prediction | 0.9957 | 0.9960 | 0.9969 |
| Minimum entropy | 0.8838 | 0.9006 | 0.8780 |


https://doi.org/10.1021/acsnano.3c03581
ACS Nano 2023, 17, 16817−16826

postprocessing[41] as shown in Table 2. It is important to note that both TRNGs and PRNGs pass the NIST SP800-22 tests,

**Table 2. NIST SP 800-22 Test Results**

| | Sequence 1 | | Sequence 2 | | Sequence 3 | |
|---|---|---|---|---|---|---|
| Statistical test | *p*-value | Result | *p*-value | Result | *p*-value | Result |
| Frequency monobit | 0.611 | PASS | 0.144 | PASS | 0.321 | PASS |
| Block frequency | 0.196 | PASS | 0.406 | PASS | 0.579 | PASS |
| Cumulative sums (forward) | 0.483 | PASS | 0.199 | PASS | 0.526 | PASS |
| Cumulative sums (backward) | 0.924 | PASS | 0.181 | PASS | 0.397 | PASS |
| Runs | 0.764 | PASS | 0.268 | PASS | 0.626 | PASS |
| Longest run of ones | 0.521 | PASS | 0.629 | PASS | 0.411 | PASS |
| Rank | 0.805 | PASS | 0.368 | PASS | 0.348 | PASS |
| DFT | 0.774 | PASS | 0.783 | PASS | 0.102 | PASS |
| Non-overlapping template | 0.919 | PASS | 0.976 | PASS | 0.895 | PASS |
| Overlapping template | 0.126 | PASS | 0.676 | PASS | 0.088 | PASS |
| Approximate entropy | 0.947 | PASS | 0.677 | PASS | 0.519 | PASS |
| Universal | 0.98 | PASS | 0.906 | PASS | 0.107 | PASS |
| Random excursions | 0.135 | PASS | 0.348 | PASS | 0.508 | PASS |
| Random excursions variant | 0.015 | PASS | 0.231 | PASS | 0.381 | PASS |
| Serial | 0.857 | PASS | 0.025 | PASS | 0.393 | PASS |
| Linear complexity | 0.513 | PASS | 0.170 | PASS | 0.273 | PASS |

and hence passing them is not sufficient to guarantee true randomness. It acts as the first step in determining whether the results produced by an entropy source apply to cryptography or not. It is crucial to evaluate the quality of the entropy source following the guidelines provided by tests such as NIST SP 800-90B. This assessment is essential to determine whether the source of random numbers used in data encryption processes possesses the necessary level of unpredictability and true randomness.

**Assessment of Strength of Randomness.** We divided the generated 65536 random bits into 256 keys of 256 bits each and assessed the strength of their randomness using five distinct figures of merit (FOMs): the Hamming distance (HD), correlation coefficient (CC), autocorrelation function (ACF), entropy (E), and uniformity (U). Figure 3a shows the distribution of the intra-Hamming distance ($HD_{intra}$) for all possible $^{256}C_2$ key combinations from a representative TSI-based TRNG. HD is defined as the number of binary bit flips required to successfully decipher a given binary key from a different but already known key sequence. For any cryptographic security application, the HD should ideally be 50% of the total key length to maximize the number of brute force trials (BFTs) required to successfully decode a key.[42,43] For our case, the mean value of $HD_{intra}$ ($\mu_{HD_{intra}}$)was found to be 127.7, which is very close to the ideal value of 128 for a 256-bit key. Similarly, Figure 3b shows the distribution of the intra-correlation coefficient ($CC_{intra}$) for all possible $^{256}C_2$ key combinations. CC is a measure of linear similarity between two keys with values lying in the range [−1, 1], where "−1", "0", and "1", respectively, signify anticorrelation, noncorrelation, and complete correlation between the keys. The mean $CC_{intra}$ ($\mu_{CC_{intra}}$) for our TSI-based TRNG was found to be 0.0035, which is very close to the ideal value of 0.

Next, it is also critical to detect the presence of any short-range periodicity within the generated random bit sequence. This is typically evaluated using the autocorrelation function (ACF), which represents the correlation of a given key with a time series delayed copy of itself. Figure 3c shows ACF as a function of lag for a single key and Figure 3d shows ACF as a function of lag for all 256-bit keys; the presence of very low magnitude spikes near the ideal value of 0 confirms the absence of any short-range periodicity in our generated keys. Figure 3e,f, respectively, show plots of entropy and bit uniformity, where entropy is defined as the degree of uncertainty with an ideal value of 1, and uniformity refers to the overall weightage of "1s" and "0s" with an ideal value of 0.5. It should be noted that, for 1-bit information, a uniformity of 0.5 corresponds to the maximum entropy value of 1, which can be calculated using the equation below.

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

Here, $E$ represents the entropy, and $p$ and $(1 - p)$ represent the probabilities of obtaining "1" and "0", respectively. As evident from the plots, our TSI random bits demonstrate near-ideal entropy and uniformity with mean values of $\mu_E = 0.9968$ and $\mu_U = 0.5004$, respectively. Additionally, we have also performed Monte Carlo (MC) simulations by evaluating the integral of $\sin(x)$ within the limit $[0,1]$ and estimating the value of $\pi$. We were able to achieve simulated values of 0.47 and 3.17, which are very close to the actual values of 0.46 and 3.14 for the integral and $\pi$, respectively.

**Physical Unclonability of TRNG.** We also analyzed the physical unclonability of 256 × 256 random bits generated from three different TSI-based TRNGs to ensure their distinguishability and unclonability, which are other critical parameters for safe and secure cryptographic encryptions. Figure 4a,b, respectively, show histograms of inter-Hamming distance ($HD_{inter}$) and inter-correlation coefficient ($CC_{inter}$) between the three possible TSI combinations (#C) for all the possible key pair values. Note that the term "inter" here refers to comparisons between physically different TRNG entities. Clearly, the histograms for both $HD_{inter}$ and $CC_{inter}$ are centered at their respective ideal values of 128 and 0, which further corroborates the true random nature of our generated bits.

**Resilience to Machine Learning (ML) Attacks.** Next, a regression model based on the Fourier series was developed to assess the resilience of our TRNG to machine learning (ML) attacks. Figure 5a shows the representative outline of the attack model, which derives the estimation function $f(x_i)$ for each bit to predict the $i^{th}$ bit in the 256-bit key from the training set. Thereafter, the model tries to predict the remaining generated keys. For our analysis, we utilized a total of 2,686,976 bits as a training set to develop the estimation functions, while 262,144 bits were obtained as the predicted set post training. Figure 5b shows the histogram of the $HD_{inter}$ values for four combinations, while Figure 5c shows the colormap of the corresponding $\mu_{HD_{inter}}$ values between the predicted and the experimentally measured keys for all the combinations. With the $\mu_{HD_{inter}}$ values lying very close to the ideal value of 128, it is evident that the predicted and experimentally generated keys are independent. Similarly, Figure 5d shows the histogram of the $CC_{inter}$ values, while Figure 5e shows the colormap of the


https://doi.org/10.1021/acsnano.3c03581
ACS Nano 2023, 17, 16817−16826

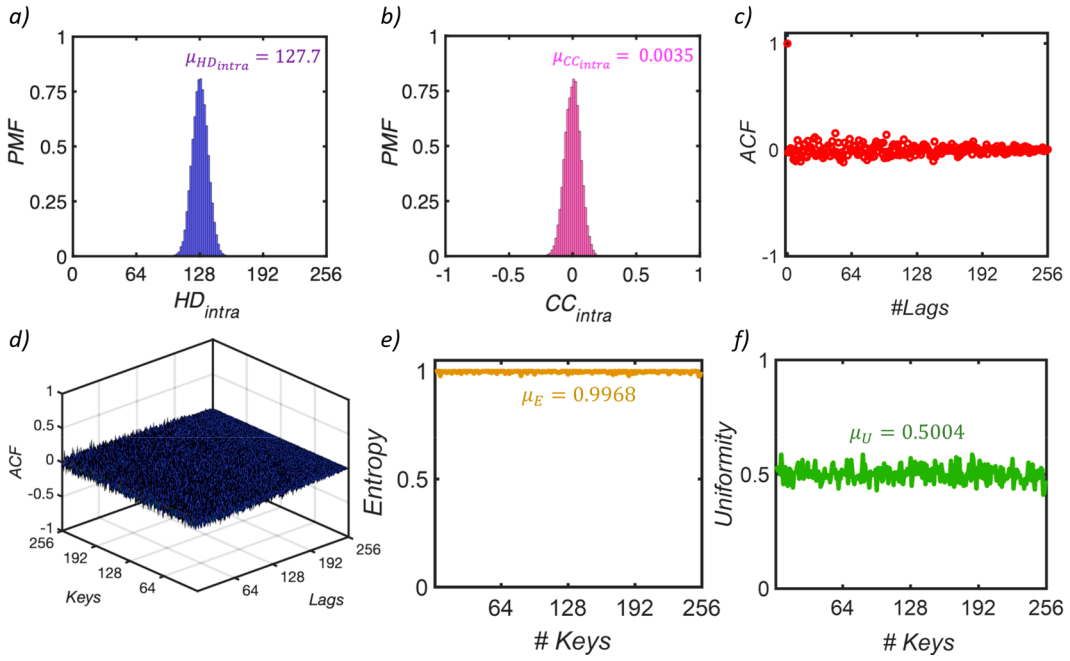



**Figure 3. Strength of randomness for the 256-bit key. (a) Distribution of intra-Hamming distance ($HD_{intra}$) between $^{256}C_2$, or 32640, pairs of keys generated/measured at $V_R = -50$ mV with a mean value ($\mu_{HD_{intra}}$) of ∼127.7, which is close to the ideal value of 128 for a 256-bit random key. (b) Distribution of intra-correlation coefficient ($CC_{intra}$) between $^{256}C_2$ pairs of 256-bit keys with a mean value of $\mu_{CC_{intra}} = 0.0035$, which is very close to the ideal value of zero, confirming that the generated keys are uncorrelated. Autocorrelation function (ACF) plotted as a function of lags for (c) a single key and (d) all the 256 keys. The presence of miniscule narrow spikes near the ideal value of 0 confirm the absence of any short-range periodicity in the bit sequence. (e) Entropy and (f) Uniformity for 256 keys of bit-length 256 with a mean value of $\mu_E = 0.9968$ and $\mu_U = 0.5004$, respectively, both of which are very close to the ideal values 1 and 0.5.**

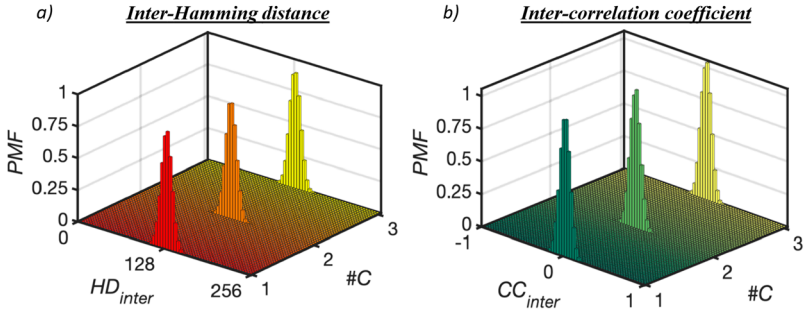



**Figure 4. Physical unclonability of TSI-based TRNG: Three-dimensional (3D) histogram plots of inter-Hamming distances ($HD_{inter}$) and inter-correlation coefficients ($CC_{inter}$) between the 256 × 256 random bits generated from three different TSI-based TRNGs for all the possible combinations. The mean histogram values for both $HD_{inter}$ and $CC_{inter}$ centered at their respective ideal values of 128 and 0 further corroborate the true random nature of our generated bits.**

corresponding $\mu_{CC_{inter}}$ values between the predicted and the experimentally measured keys. Once again, the $\mu_{CC_{inter}}$ values were found to be very close to 0, which further corroborates the lack of any correlation between the predicted and experimentally measured keys. As such, these results confirm the resilience of our TRNG to the regression attack model.

**Resilience to Temperature and Supply Bias Variations.** Finally, we have also analyzed the robustness and stability of our TSI-based TRNG against temperature ($T$) and supply bias ($V_{DD}$) variations, both of which are critical for any TRNG. SI, Figure S4 shows the VTC of a representative TSI obtained at different temperatures (25, 50, 75, and 100 °C). An increase in $\Delta V_{TH}$ is observed with increasing temperature owing to increased charge trapping.[44,45] However, the increase in $\Delta V_{TH}$ does not affect the stochasticity, as $V_{Out3}$ obtained at each of the temperature toggles randomly between the lower and higher logic levels, enabling seamless generation of random bits. SI, Figure S5 shows the VTC, stochastic fluctuations, and the distribution of the stochastic fluctuations of a representative TSI for different supply biases (1, 2, 3, 4, and 5 V). The output, $V_{Out3}$, fluctuates stochastically between the lower and higher logic levels irrespective of the variations in the supply bias, ensuring the consistent generation of random bits. Figure 6a,b show the 3D histogram plots of $HD_{intra}$ and $CC_{intra}$ at different temperatures (25, 50, 75, and 100 °C), whereas Figure 6c,d show the 3D histogram plots of $HD_{intra}$ and $CC_{intra}$ with different $V_{DD}$ ($V_{DD}$ = 2, 3, 4, and 5 V). Clearly, our TRNGs show resilience that can be confirmed


https://doi.org/10.1021/acsnano.3c03581
ACS Nano 2023, 17, 16817−16826

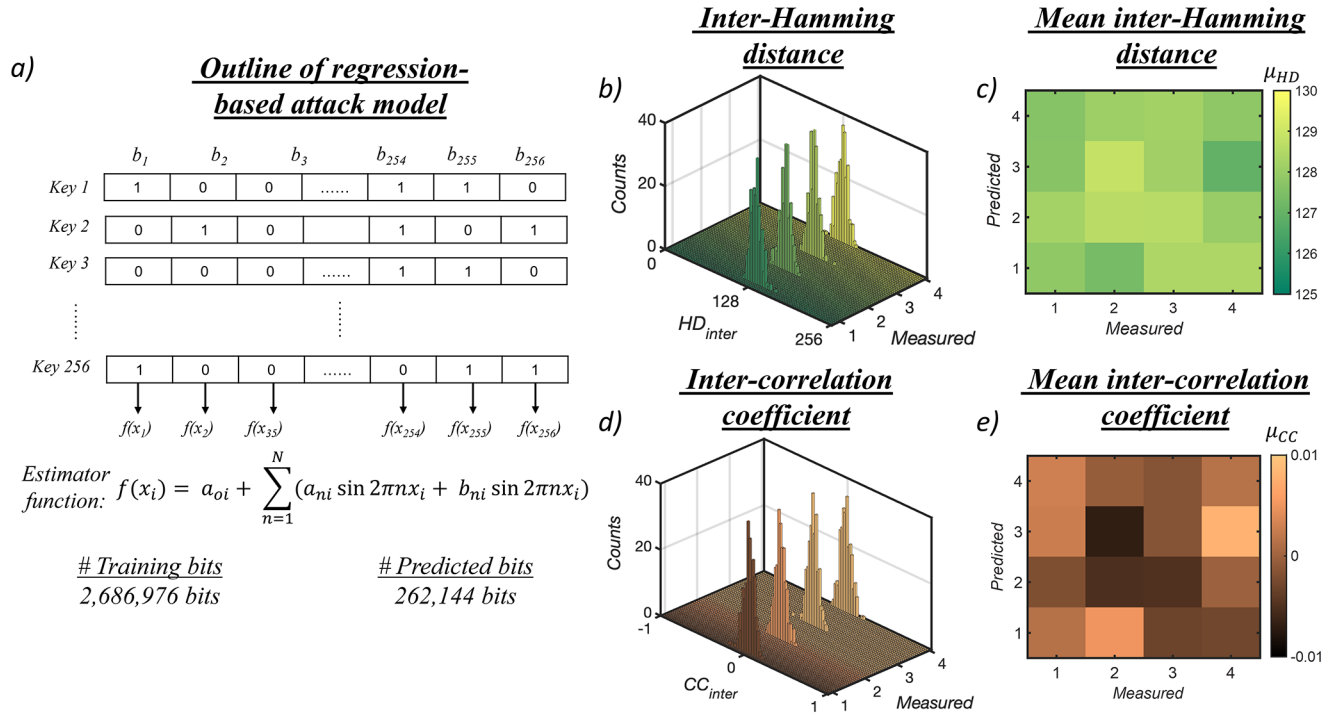



**Figure 5. Resilience to machine learning (ML) attack. (a) Representative outline of the attack model which derives the estimation function $f(x_i)$ for each bit to predict the $i^{th}$ bit in the 256-bit key from the training set. Thereafter, the model tries to predict the remaining generated keys. (b) Histogram of the $HD_{inter}$ values along with the (c) colormap of the corresponding $\mu_{HD_{inter}}$ values between the predicted and the experimentally measured keys. With the $\mu_{HD_{inter}}$ values lying very close to the ideal value of 128, it is evident that the predicted and experimentally generated keys are independent from one another. (d) Histogram of the $CC_{inter}$ values along with the (e) colormap of the corresponding $\mu_{CC_{intra}}$ values measured between the predicted and the experimentally measured keys. Once again, the $\mu_{CC_{intra}}$ values were found to be very close to 0, which further corroborates the lack of any correlation between the predicted and experimentally measured keys. These results confirm the resilience of our TRNG to the regression attack model.**

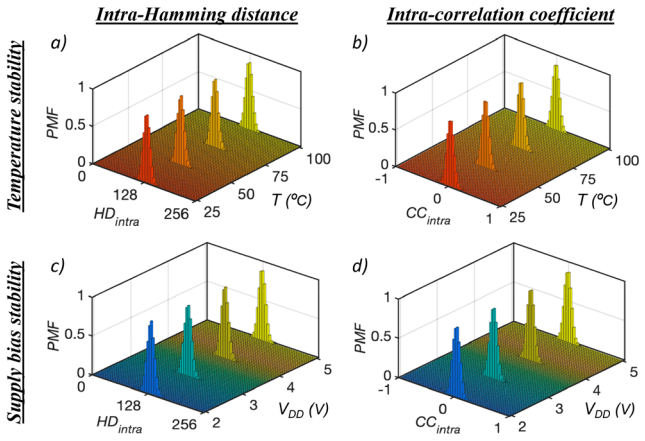



**Figure 6. Resilience to temperature and supply bias variations: 3D histogram plots of (a) $HD_{intra}$ and (b) $CC_{intra}$ plotted against different temperatures of 25, 50, 75, and 100 °C along with 3D histogram plots of (c) $HD_{intra}$ and (d) $CC_{intra}$ plotted against different $V_{DD}$ = 2, 3, 4, and 5 V. Clearly, our TRNG is resilient to both temperature and $V_{DD}$ variations which can be confirmed through the $\mu_{HD\text{-}intra}$ and $\mu_{CC\text{-}intra}$ values which were found to be close to the ideal value of 128 and 0, respectively, for all the $^{256}C_2$ key combinations.**

through the $\mu_{HD\text{-}intra}$ and $\mu_{CC\text{-}intra}$ values that were found to be close to the ideal values of 128 and 0, respectively, for all possible $^{256}C_2$ key combinations in both cases. Moreover, SI, Figures S6 and S7 show the entropy and uniformity of our TRNG at different temperatures and $V_{DD}$ values, respectively; these were also found to be very close to the ideal values of 1 and 0.5. SI, Figure S8 shows the benchmarking of non-IID entropy sources based on NIST SP800-90B used for true randomness. Our TRNG has a minimum normalized entropy that is at par with most of the non-IID entropy-source based TRNGs while also offering advantages including peripheral-free operation, no postprocessing requirements, resilience to ML attacks, and resilience to temperature and supply bias variations.

## CONCLUSION

In conclusion, we have demonstrated a peripheral-free cascaded TSI-based TRNG by exploiting the inherent stochasticity in 2D FETs arising due to the phenomenon of charge trapping and detrapping at and/or near the $MoS_2$/$Al_2O_3$ interface. Our TRNG design mitigates the need for external peripherals due to the digital nature of stochastic voltage fluctuations. The generated random bits pass all the specified tests under NIST SP 800-22 without any postprocessing. The entropy source also passes all of the specified tests under NIST SP 800-90B with a minimum entropy of 0.8875. Moreover, all the 256-bit keys generated by our TRNG were uncorrelated, exhibited high entropy with near-ideal uniformity and Hamming distances, and were found to be resilient to regression-based attack models as well as


https://doi.org/10.1021/acsnano.3c03581
ACS Nano 2023, 17, 16817−16826

temperature and supply bias variations. Our results showcase the efficacy of 2D-FET-based TRNGs for hardware security and cryptographic primitives in next-generation computing and IoT edge devices.

## METHODS

**Large-Area Monolayer $MoS_2$ Film Growth.** Monolayer $MoS_2$ was deposited on epi-ready 2" c-sapphire substrate by metal−organic chemical vapor deposition (MOCVD). An inductively heated graphite susceptor equipped with wafer rotation in a cold-wall horizontal reactor was used to achieve uniform monolayer deposition. Molybdenum hexacarbonyl ($Mo(CO)_6$) and hydrogen sulfide ($H_2S$) were used as precursors. $Mo(CO)_6$ maintained at 25 °C and 375 Torr in a stainless-steel bubbler was used to deliver $2.0 \times 10^{-2}$ sccm of the metal precursor for the growth, while 400 sccm of $H_2S$ was used for the process. $MoS_2$ deposition was carried out at 950 °C and 50 Torr in ambient $H_2$ with monolayer growth being achieved in 18 min. Prior to growth, the substrate was baked at 1000 °C in $H_2$ for 10 min. Following growth, the substrate was cooled in $H_2S$ to 300 °C to inhibit decomposition of the $MoS_2$ film. More details on the growth process can be found in an earlier work.[46]

**Fabrication of Local Back-Gate Islands.** To define the back-gate island regions, a commercially purchased substrate (thermally grown 285 nm $SiO_2$ on $p^{++}$-Si) was spin-coated at 4000 rpm for 45 s with a bilayer photoresist consisting of Lift-Off-Resist (LOR 5A) and Series Photoresist (SPR 3012); following application, these resists were baked at 185 °C for 120 s and 95 °C for 60 s, respectively. The bilayer photoresist was then patterned using a Heidelberg Maskless Aligner (MLA 150) to define the islands and developed by immersing the substrate in MF CD26 Microposit for 75 s, followed by a 60 s deionized (DI) water rinse. The back-gate electrodes of 20/50 nm Ti/Pt were then deposited using electron-beam (e-beam) evaporation in a Temescal FC-2000 bell jar deposition system. Liftoff of the remaining photoresist and excess metal was achieved using acetone and photo resist stripper (PRS 3000); the substrate was then cleaned using 2-propanol (IPA) and DI water. An atomic layer deposition (ALD) process was then implemented to grow the back-gate dielectric stack consisting of 50 nm of $Al_2O_3$ ($\varepsilon_{ox} \approx 10$), across the entire substrate, including the island regions. Access to the individual Pt back-gate electrodes was achieved via a reactive ion etch (RIE) process conducted in a Plasma-Therm Versalock 700. First, etch patterns were defined using the same bilayer photoresist (LOR 5A and SPR 3012) used previously. The bilayer photoresist was again exposed using an MLA 150 and developed using MF CD26 microposit with a DI water rinse. The dielectric stack was then dry etched using a $BCl_3$ RIE chemistry at 5 °C for 80 s; this process was split into four 20 s etch steps separated by 60 s stabilization steps to minimize heating in the substrate. Finally, the photoresist was removed using the same process described earlier for liftoff.

**$MoS_2$ Film Transfer to Local Back-Gate Island Substrate.** Film transfer from the growth substrate to the application substrate was performed using a poly(methyl) methacrylate (PMMA) assisted wet transfer process.[47] First, the as-grown $MoS_2$ on the sapphire substrate was spin-coated with PMMA and left to sit for 24 h to ensure good PMMA/$MoS_2$ adhesion. The corners of the spin-coated film were then scratched using a razor blade and immersed inside a 2 M NaOH solution kept at 90 °C. Capillary action caused the NaOH to be preferentially drawn into the substrate/$MoS_2$ interface, owing to the hydrophilic nature of sapphire and the hydrophobic nature of $MoS_2$ and PMMA, separating the PMMA/$MoS_2$ stack from the sapphire substrate. The separated film was then fished from the NaOH solution using a clean glass slide and rinsed in three separate water baths for 15 min each before finally being transferred onto the application substrate. Subsequently, the substrate was baked at 50 and 70 °C for 10 min each to remove moisture and promote film adhesion, thus ensuring a pristine interface, before the PMMA was removed by immersing the sample in acetone for 1 h, and the substrate was cleaned with a subsequent 30 min IPA bath.

**Fabrication of 2D $MoS_2$ Transistors.** To define the channel regions of the $MoS_2$ transistors discussed in this work, the application substrate, with $MoS_2$ transferred on top, was spin-coated with PMMA A6 (4000 rpm for 45 s) and baked at 180 °C for 90 s. The resist was then exposed using a Raith EBPG5200 e-beam lithography tool, developed using a 1:1 mixture of 4-methyl-2-pentanone (MIBK) and IPA (60 s) and then rinsed using IPA (45 s). The exposed monolayer $MoS_2$ film was subsequently etched using a sulfur hexafluoride ($SF_6$) RIE process at 5 °C for 30 s. Next, the sample was rinsed in acetone and IPA to remove the e-beam resist. A subsequent lithography step was conducted to form source/drain electrodes. The substrate was spin-coated at 4000 rpm for 45 s with methyl methacrylate (MMA) EL6 and PMMA A3; following application, these resists were baked at 150 °C for 90 s and 180 °C for 90 s, respectively. E-beam lithography was again used to pattern the source and drain, and development was again performed using a 1:1 mixture of MIBK/IPA and an IPA rinse for the same times as previously. Then 40 nm of Ni and 30 nm of Au (Au) were deposited using e-beam evaporation to form the electrodes. Finally, a lift-off process was performed to remove the excess Ni/Au by immersing the sample in acetone for 1 h, followed by IPA for another 30 min to clean the substrate. At this stage, each island contains one $MoS_2$ transistor to allow for individual gate control of each device.

**Integration of 2D $MoS_2$ Transistors for TSI Fabrications.** To define the connections between individual transistors for circuit creation, the substrate was first spin-coated at 4000 rpm for 45 s with MMA EL11 and PMMA A3 and baked at 150 °C for 90 s and 180 °C for 90 s, respectively. Note that this bilayer resist differs from that used previously to define the source/drain electrodes; MMA EL11 is thicker under these spin/bake conditions than MMA EL6, allowing for the deposition of a thicker metal layer without risking sidewall coverage. The bilayer resist was then patterned using e-beam lithography and developed using the same 1:1 MIBK/IPA and IPA rinse processes mentioned previously. E-beam evaporation was performed to deposit 60 nm Ni and 40 nm Au, forming the connections between neighboring devices; a thicker metal layer was deposited at this step to ensure the continuity of the connections over the features defined in the previous lithography steps. Finally, the e-beam resist and excess metal were rinsed away in a lift-off process using acetone (1 h) and IPA (30 min).

**Raman and Photoluminescence (PL) Spectroscopy.** Raman and PL spectroscopy of the pre- and postirradiation $MoS_2$ film were performed on a Horiba LabRAM HR Evolution confocal Raman microscope with a 532 nm laser. The power was 34 mW filtered at 5% to 1.7 mW. The objective magnification was 100× with a numerical aperture of 0.9, and the grating had a spacing of 1800 gr/mm for Raman and 300 gr/mm for PL. The spectral resolution of each Raman and PL measurement was approximately 0.5 $cm^{-1}$ and $3 \times 10^{-4}$ eV, respectively. Each Raman and PL measurement was taken from a single accumulation with a dwell time of 0.5 s.

**Electrical Characterization.** Electrical characterization of the fabricated devices was performed in a Lake Shore CRX-VF probe station under atmospheric conditions using a Keysight B1500A parameter analyzer.

## ASSOCIATED CONTENT

### Data Availability Statement

The data sets generated during and/or analyzed during the current study are available from the corresponding author upon reasonable request.

### Supporting Information

The Supporting Information is available free of charge at https://pubs.acs.org/doi/10.1021/acsnano.3c03581.

Stochastic fluctuations and their corresponding distribution for stage 3 of the second cascaded TSI, measured for $V_{DD}$ of 2 V at a $V_R$ of 250 mV with a sampling rate $\tau_S$ = 5 ms. Optical image and corresponding circuit schematic of an XOR gate consisting of 9 $MoS_2$ FETs



https://doi.org/10.1021/acsnano.3c03581
ACS Nano 2023, 17, 16817−16826

and input-output characteristics of the XOR gate performing the desired logic operation. Estimation of energy expenditure for the random bit generation process. Impact of temperature variation on the output of TSI. Impact of supply bias ($V_{DD}$) variations on the output of TSI. Entropy and uniformity plots of the generated random bits at different temperatures. Entropy and uniformity plots of the generated random bits at different supply biases ($V_{DD}$). Benchmarking of non-IID entropy sources for TRNG (PDF)

### Accession Codes

The codes used for plotting the data are available from the corresponding authors on reasonable request.

## AUTHOR INFORMATION


### Corresponding Author

**Saptarshi Das** − *Engineering Science and Mechanics, Pennsylvania State University, University Park, Pennsylvania 16802, United States; Materials Science and Engineering, 2D Crystal Consortium, Materials Research Institute, and Electrical Engineering and Computer Science, Pennsylvania State University, University Park, Pennsylvania 16802, United States;* orcid.org/0000-0002-0188-945X; Email: Email: sud70@psu.edu, das.sapt@gmail.com

### Authors

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

**Dipanjan Sen** − *Engineering Science and Mechanics, Pennsylvania State University, University Park, Pennsylvania 16802, United States*

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

**Thomas F. Schranghamer** − *Engineering Science and Mechanics, Pennsylvania State University, University Park, Pennsylvania 16802, United States*

**Nicholas Trainor** − *Materials Science and Engineering and 2D Crystal Consortium, Materials Research Institute, Pennsylvania State University, University Park, Pennsylvania 16802, United States*

**Joan M. Redwing** − *Materials Science and Engineering and 2D Crystal Consortium, Materials Research Institute, Pennsylvania State University, University Park, Pennsylvania 16802, United States;* orcid.org/0000-0002-7906-452X

**Biswajit Ray** − *Department of Electrical and Computer Engineering, Colorado State University, Fort Collins, Colorado 80523, United States*

Complete contact information is available at: https://pubs.acs.org/10.1021/acsnano.3c03581


### Author Contributions

All authors contributed to the preparation of the manuscript.

### Notes

The authors declare no competing financial interest.

## ACKNOWLEDGMENTS

This work was funded by the Department of Defense, Defense Threat Reduction Agency (DTRA) as part of the Interaction of Ionizing Radiation with Matter University Research Alliance (IIRM-URA) under contract number HDTRA1-20-2-0002. The content of the information does not necessarily reflect the position or the policy of the federal government, and no official endorsement should be inferred. This work was also supported by the National Science Foundation (NSF) through the CAREER Award under grant number ECCS-2042154 and supported by the Army Research Office (ARO) through contract number W911NF1920338. The authors also acknowledge the materials support from the NSF through the Pennsylvania State University 2D Crystal Consortium−Materials Innovation Platform (2DCC-MIP) under NSF cooperative agreement DMR-2039351. This work was supported in part by the NSF through the CAREER Award under grant number 2145311. N.T. would like to acknowledge support through NSF Graduate Research Fellowships Program under grant number DGE1255832.

## REFERENCES


(1) Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74* (1), 145−195.

(2) Ferguson, N.; Schneier, B.; Kohno, T. *Cryptography Engineering: Design Principles and Practical Applications*; John Wiley & Sons, 2011.

(3) Metropolis, N.; Ulam, S. The Monte Carlo Method. *Journal of the American Statistical Association* **1949**, *44* (247), 335−341.

(4) Stipčević, M.; Koç, Ç. K. True random number generators. In *Open Problems in Mathematics and Computational Science*; Springer, 2014; pp 275−315.

(5) Banks, S.; Beadling, P.; Ferencz, A. FPGA Implementation of Pseudo Random Number Generators for Monte Carlo Methods in Quantitative Finance. *2008 International Conference on Reconfigurable Computing and FPGAs* **2008**, 271−276.

(6) Gupta, M. D.; Chauhan, R. K. Secure image encryption scheme using 4D-Hyperchaotic systems based reconfigurable pseudo-random number generator and S-Box. *Integration* **2021**, *81*, 137−159.

(7) Kelsey, J.; Schneier, B.; Wagner, D.; Hall, C. Cryptanalytic Attacks on Pseudorandom Number Generators. In *Fast Software Encryption*; Berlin, Heidelberg, 1998; Vaudenay, S., Ed.; *FSE '98: Proceedings of the 5th International Workshop on Fast Software Encryption*; Springer: Berlin, Heidelberg; pp 168−188.

(8) 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.

(9) Wali, A.; Ravichandran, H.; Das, S. A Machine Learning Attack Resilient True Random Number Generator Based on Stochastic Programming of Atomically Thin Transistors. *ACS Nano* **2021**, *15* (11), 17804−17812.

(10) Satpathy, S. K.; Mathew, S. K.; Kumar, R.; Suresh, V.; Anders, M. A.; Kaul, H.; Agarwal, A.; Hsu, S.; Krishnamurthy, R. K.; De, V. An All-Digital Unified Physically Unclonable Function and True Random Number Generator Featuring Self-Calibrating Hierarchical Von Neumann Extraction in 14-nm Tri-gate CMOS. *IEEE Journal of Solid-State Circuits* **2019**, *54* (4), 1074−1085.

(11) Zhang, R.; Wang, X.; Liu, K.; Shinohara, H. A 0.186-pJ per Bit Latch-Based True Random Number Generator Featuring Mismatch Compensation and Random Noise Enhancement. *IEEE Journal of Solid-State Circuits* **2022**, *57* (8), 2498−2508.

(12) Pamula, V. R.; Sun, X.; Kim, S. M.; Rahman, F. u.; Zhang, B.; Sathe, V. S. A 65-nm CMOS 3.2-to-86 Mb/s 2.58 pJ/bit Highly Digital True-Random-Number Generator With Integrated De-Correlation and Bias Correction. *IEEE Solid-State Circuits Letters* **2018**, *1* (12), 237−240.

(13) 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.

(14) Taneja, S.; Rajanna, V. K.; Alioto, M. 36.1. Unified In-Memory Dynamic TRNG and Multi-Bit Static PUF Entropy Generation for

Ubiquitous Hardware Security. In *IEEE International Solid-State Circuits Conference (ISSCC)*; IEEE, 2021; Vol. *64*, pp 498−500
(15) Jiang, H.; Belkin, D.; Savel'ev, S. E.; Lin, S.; Wang, Z.; Li, Y.; Joshi, S.; Midya, R.; Li, C.; Rao, M.; et al. A novel true random number generator based on a stochastic diffusive memristor. *Nat. Commun.* **2017**, *8* (1), 882.
(16) Woo, K. S.; Wang, Y.; Kim, J.; Kim, Y.; Kwon, Y. J.; Yoon, J. H.; Kim, W.; Hwang, C. S. A True Random Number Generator Using Threshold-Switching-Based Memristors in an Efficient Circuit Design. *Advanced Electronic Materials* **2019**, *5* (2), No. 1800543.
(17) Fukushima, A.; Seki, T.; Yakushiji, K.; Kubota, H.; Imamura, H.; Yuasa, S.; Ando, K. Spin dice: A scalable truly random number generator based on spintronics. *Appl. Phys. Express* **2014**, *7* (8), No. 083001.
(18) Mulaosmanovic, H.; Mikolajick, T.; Slesazeck, S. Random number generation based on ferroelectric switching. *IEEE Electr Device L* **2018**, *39* (1), 135−138.
(19) Kim, S.; Kim, M.-S.; Lee, Y.; Kim, H.-D.; Choi, Y.-K.; Choi, S.-J. Low-Power True Random Number Generator Based on Randomly Distributed Carbon Nanotube Networks. *IEEE Access* **2021**, *9*, 91341−91346.
(20) 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.
(21) Zheng, Y.; Ravichandran, H.; Schranghamer, T. F.; Trainor, N.; Redwing, J. M.; Das, S. Hardware implementation of Bayesian network based on two-dimensional memtransistors. *Nat. Commun.* **2022**, *13* (1), 5578.
(22) Ravichandran, H.; Zheng, Y.; Schranghamer, T. F.; Trainor, N.; Redwing, J. M.; Das, S. A Monolithic Stochastic Computing Architecture for Energy Efficient Arithmetic. *Adv. Mater.* **2023**, *35* (2), No. 2206168.
(23) Serrano, R.; Duran, C.; Hoang, T. T.; Sarmiento, M.; Nguyen, K. D.; Tsukamoto, A.; Suzaki, K.; Pham, C. K. A Fully Digital True Random Number Generator With Entropy Source Based in Frequency Collapse. *IEEE Access* **2021**, *9*, 105748−105755.
(24) Lu, Y.; Liang, H.; Yao, L.; Wang, X.; Qi, H.; Yi, M.; Jiang, C.; Huang, Z. Jitter-Quantizing-Based TRNG Robust Against PVT Variations. *IEEE Access* **2020**, *8*, 108482−108490.
(25) Park, S.; Choi, B. G.; Kang, T. W.; Park, K. W.; Lee, J. J.; Kang, S. W.; Kim, J. B. Analysis of Entropy Estimator of True Random Number Generation Using Beta Source. *2019 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC)* **2019**, 1−3.
(26) Nasr, J. R.; Simonson, N.; Oberoi, A.; Horn, M. W.; Robinson, J. A.; Das, S. Low-Power and Ultra-Thin $MoS_2$ Photodetectors on Glass. *ACS Nano* **2020**, *14* (11), 15440−15449.
(27) Dodda, A.; Oberoi, A.; Sebastian, A.; Choudhury, T. H.; Redwing, J. M.; Das, S. Stochastic resonance in $MoS_2$ photodetector. *Nat. Commun.* **2020**, *11* (1), 4406.
(28) Subbulakshmi Radhakrishnan, S.; Chakrabarti, S.; Sen, D.; Das, M.; Schranghamer, T. F.; Sebastian, A.; Das, S. A Sparse and Spike-Timing-Based Adaptive Photoencoder for Augmenting Machine Vision for Spiking Neural Networks. *Adv. Mater.* **2022**, *34* (48), No. 2202535.
(29) Li, J.; Zhang, H.; Ding, Y.; Li, J.; Wang, S.; Zhang, D. W.; Zhou, P. A non-volatile AND gate based on $Al_2O_3/HfO_2/Al_2O_3$ charge-trap stack for in-situ storage applications. *Science Bulletin* **2019**, *64* (20), 1518−1524.
(30) Zhu, L.; Farhat, M.; Salama, K. N.; Chen, P.-Y. Two-dimensional materials-based radio frequency wireless communication and sensing systems for Internet-of-things applications. In *Emerging 2D Materials and Devices for the Internet of Things: Information, Sensing and Energy Applications*, Tao, L., Akinwande, D., Eds.; Elsevier, 2020; pp 29−57.
(31) Wali, A.; Das, S. Hardware and Information Security Primitives Based on 2D Materials and Devices. *Adv. Mater.* **2023**, *35* (18), No. 2205365.
(32) 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*, 3587.
(33) Chakrabarti, S.; Wali, A.; Ravichandran, H.; Kundu, S.; Schranghamer, T. F.; Basu, K.; Das, S. Logic Locking of Integrated Circuits Enabled by Nanoscale MoS2-Based Memtransistors. *ACS Applied Nano Materials* **2022**, *5* (10), 14447−14455.
(34) Wali, A.; Ravichandran, H.; Das, S. Hardware Trojans based on Two-dimensional Memtransistor. *Nanoscale Horizons* **2023**, *8*, 603.
(35) Pendurthi, R.; Jayachandran, D.; Kozhakhmetov, A.; Trainor, N.; Robinson, J. A.; Redwing, J. M.; Das, S. Heterogeneous integration of atomically thin semiconductors for non-von Neumann CMOS. *Small* **2022**, *18* (33), No. 2202590.
(36) Dodda, A.; Jayachandran, D.; Pannone, A.; Trainor, N.; Stepanoff, S. P.; Steves, M. A.; Radhakrishnan, S. S.; Bachu, S.; Ordonez, C. W.; Shallenberger, J. R.; et al. Active pixel sensor matrix based on monolayer MoS2 phototransistor array. *Nat. Mater.* **2022**, *32*, 1379.
(37) Jayachandran, D.; Pannone, A.; Das, M.; Schranghamer, T. F.; Sen, D.; Das, S. Insect-Inspired, Spike-Based, in-Sensor, and Night-Time Collision Detector Based on Atomically Thin and Light-Sensitive Memtransistors. *ACS Nano* **2023**, *17* (17), 1068.
(38) Turan, M. S.; Barker, E.; Kelsey, J.; McKay, K. A.; Baish, M. L.; Boyle, M. Recommendation for the entropy sources used for random bit generation. *NIST Special Publication 800-90-B* **2018**, *800* (90B), 102.
(39) Serrano, R.; Duran, C.; Sarmiento, M.; Hoang, T. T.; Tsukamoto, A.; Suzaki, K.; Pham, C. K. A Robust and Healthy Against PVT Variations TRNG Based on Frequency Collapse. *IEEE Access* **2022**, *10*, 41852−41862.
(40) Tao, S.; Dubrova, E. TVL-TRNG: Sub-Microwatt True Random Number Generator Exploiting Metastability in Ternary Valued Latches. In *2017 IEEE 47th International Symposium on Multiple-Valued Logic (ISMVL)*; IEEE, 2017; pp 130−135,.
(41) Lawrence, B.; Andrew, R.; Juan, S.; James, N.; Miles, S.; Stefan, L.; Levenson, M.; Vangel, M.; Nathanael, H.; Banks, D. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications; Special Publication (NIST SP), National Institute of Standards and Technology: Gaithersburg, MD, 2010.
(42) Wali, A.; Dodda, A.; Wu, Y.; Pannone, A.; Reddy Usthili, L. K.; Ozdemir, S. K.; Ozbolat, I. T.; Das, S. Biological physically unclonable function. *Communications Physics* **2019**, *2* (1), 39.
(43) 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), No. 1800154.
(44) Illarionov, Y. Y.; Rzepa, G.; Waltl, M.; Knobloch, T.; Grill, A.; Furchi, M. M.; Mueller, T.; Grasser, T. The role of charge trapping in MoS2/SiO2 and MoS2/hBN field-effect transistors. *2D Materials* **2016**, *3* (3), No. 035004.
(45) Gusev, E. P.; D'Emic, C.; Zafar, S.; Kumar, A. Charge trapping and detrapping in HfO2 high-$\kappa$ gate stacks. *Microelectron. Eng.* **2004**, *72* (1), 273−277.
(46) Xuan, Y.; Jain, A.; Zafar, S.; Lotfi, R.; Nayir, N.; Wang, Y.; Choudhury, T. H.; Wright, S.; Feraca, J.; Rosenbaum, L. Multi-scale modeling of gas-phase reactions in metal-organic chemical vapor deposition growth of $WSe_2$. *J. Cryst. Growth* **2019**, *527*, 125247.
(47) Sebastian, A.; Zhang, F.; Dodda, A.; May-Rawding, D.; Liu, H.; Zhang, T.; Terrones, M.; Das, S. Electrochemical Polishing of Two-Dimensional Materials. *ACS Nano* **2019**, *13* (1), 78−86.


https://doi.org/10.1021/acsnano.3c03581
*ACS Nano* 2023, 17, 16817−16826