Journal of Electrical and Electronic Materials

View Online CrossMark

Academic Progress Report

Recent Advances in True Random Number Generators Based on Emerging Material-Based Semiconductor Devices: Toward Wearable and Flexible Electronics

Yooyeon Jo[1], Daniel Juhyung Joe[2,*], Joon Young Kwak[3,*]

[1] Department of Semiconductor Materials Engineering, Sun Moon University, Asan 31460, Korea
[2] Division of Biomedical Metrology, Korea Research Institute of Standards and Science, Daejeon 34113, Korea
[3] Division of Electronic and Semiconductor Engineering, Ewha Womans University, Seoul 03760, Korea

Corresponding author(s): daniel.joe@kriss.re.kr (D. J. Joe), jykwak@ewha.ac.kr (J. Y. Kwak)

Cite as J. Electr. Electron. Mater., 39(5), 443–461 (2026), DOI: https://doi.org/10.4313/JEEM.2026.39.5.1

Received April 29, 2026; Accepted May 18, 2026

ABSTRACT: As technologies such as artificial intelligence, autonomous driving, the Internet of Things, wearable electronics, and edge computing continue to spread in the era of the Fourth Industrial Revolution, the importance of hardware security for the safe storage, transmission, and processing of large volumes of data has grown substantially. One of the key components of such security systems is the true random number generator (TRNG), which produces unpredictable random numbers for cryptographic use. In recent years, research on TRNGs has increasingly moved beyond conventional CMOS-based approaches toward semiconductor devices built from emerging materials. These material-based TRNGs offer several advantages, including high integration density, low power consumption, compact form factors, and strong suitability for next-generation edge and IoT environments, because they can directly exploit the intrinsic stochasticity of the device itself as an entropy source. In this review, recent studies on TRNGs based on emerging material-based semiconductor devices are examined from the perspectives of entropy sources, device structures, randomness validation, and wearable/flexible extensions. By bringing together the key physical mechanisms, device platforms, evaluation criteria, and prospects for wearable and flexible electronics in edge and IoT environments, this review aims to provide a useful framework for future research on hardware security devices.

KEYWORDS: Emerging materials, Semiconductor devices, Entropy source, True random number generator, Wearable devices, Flexible electronics

1 Introduction

Modern society is undergoing rapid change under the broader trajectory of the Fourth Industrial Revolution, in which technologies such as artificial intelligence, autonomous vehicles, robotics, cloud computing, edge computing, and the Internet of Things are increasingly converging [1,2]. This shift goes beyond incremental technological progress; it is blurring the boundaries among the physical, digital, and biological domains, while improving productivity and efficiency and giving rise to new industrial and service models. In particular, IoT technologies have expanded rapidly, enabling remote control of smart appliances, internet-based connectivity services, the collection and processing of personal, biometric, and health-monitoring data, and a wide range of customized services, all of which have contributed substantially to improvements in quality of life [3,4]. At the same time, as

computing capabilities and network connectivity continue to advance, vulnerabilities associated with the storage, transmission, and processing of large volumes of data have also grown [5–7]. As a result, encryption systems for protecting personal and sensitive information have become increasingly important. One of the fundamental prerequisites for secure information protection is the reliable generation of unpredictable random numbers, which are widely regarded as one of the most essential cryptographic primitives in hardware security [8–10]. In this context, random number generators play an indispensable role in producing key elements used in cryptographic systems, including secret keys, nonces, challenges, and signature parameters [11]. Although software-based pseudo-random number generators are attractive because of their simplicity and speed, they have an inherent limitation in that their outputs may become predictable or reproducible if the seed or internal state is exposed [12–14]. By contrast, true random number generators (TRNGs) derive randomness from physically unpredictable noise or entropy sources and therefore offer security at a more fundamental level [8,15–17]. For this reason, TRNGs are receiving increasing attention as core hardware security primitives for secure communication, authentication hardware, edge-device security, and distributed IoT ecosystems.

Conventional on-chip TRNGs have largely relied on relatively traditional CMOS-compatible entropy sources, such as thermal noise, oscillator jitter, metastability, and resistor-based noise harvesting [18]. However, recent IoT and edge environments demand not only smaller chip area, lower power consumption, and simpler circuit configurations, but in some cases even operation on mechanically flexible substrates. These requirements are difficult to satisfy using conventional approaches alone. Therefore, they have driven growing interest in new strategies that directly exploit the intrinsic stochasticity of the device itself as an entropy source, leading emerging material-based semiconductor devices to become promising next-generation TRNG platforms [17,19]. A wide range of semiconductor devices based on emerging materials have already shown that hardware-level randomness can be obtained from distinct physical entropy sources [20,21]. More importantly, recent work suggests that the key question is no longer which material is used, but rather which physical irregularity is harnessed as the entropy source and how it is realized through a specific device structure and circuit configuration [19]. In parallel with these developments, the evaluation of TRNG performance has also become more rigorous. Earlier studies primarily focused on the statistical randomness of output bitstreams using NIST SP 800-22, whereas more recent discussions increasingly incorporate entropy-source validation under SP 800-90B and the certification-oriented functionality classes defined in AIS 20/31. As a result, TRNG assessment is moving beyond a simple pass/fail view toward a broader framework that considers min-entropy, health testing, restart behavior, robustness, and certification readiness.

This review provides an overview of recent progress in TRNGs based on emerging material-based semiconductor devices. We first classify the relevant entropy sources into stochastic programming/charge fluctuation, stochastic switching delay/relaxation, and random telegraph noise (RTN). We then discuss the device platforms that implement these mechanisms, grouping them into transistor-based TRNGs, threshold-switching-device-based TRNGs, and other emerging-device/platform TRNGs. We also examine how the quality of generated random numbers should be evaluated and interpreted from the standpoint of randomness validation and benchmarking. Finally, we discuss the prospects of wearable and flexible TRNGs, including flexible hardware and biosignal- or sensor-derived entropy. Through this structure, the present review aims to provide an integrated framework for understanding the key physical mechanisms, device architectures, validation criteria, and application directions that define current research on emerging material-based TRNGs.

2 Entropy Source-Based Understanding of TRNG Operation

Although emerging-device-based TRNGs encompass a wide range of device structures and material systems, a more fundamental understanding of this field begins with identifying the physical origins of randomness. In this section, the entropy sources most commonly employed in recent TRNG studies are categorized into three groups. The first, stochastic programming/charge fluctuation, includes entropy arising from charge trapping and detrapping, discrete charge fluctuations, and carrier injection fluctuations near the threshold region. The second, stochastic switching delay/ relaxation, covers temporal irregularities such as turn-on delay, relaxation time, and oscillation period fluctuation in threshold-switching devices. The third, RTN, refers to discrete current fluctuations caused by charge capture and emission at trap sites. This classification provides a useful framework for interpreting the diverse device platforms discussed in later sections, not in terms of material choice or structural form, but in terms of the underlying physical mechanisms responsible for random number generation.

2.1 Stochastic Programming / Charge Fluctuation

Entropy based on stochastic programming and charge fluctuation represents one of the most intuitive and important categories in emerging-device TRNGs. In this approach, the origin of randomness lies in charge trapping and detrapping within the device or at its interfaces, discrete charge occupancy, carrier injection fluctuations near the threshold region, and the resulting threshold shifts or output fluctuations. Thus, the defining feature of this class is not the macroscopic switching amplitude of the device, but rather the extent to which the charge state evolves in an unpredictable manner over time.

A representative example is the floating-gate 2D FET-based TRNG reported by Wali and co-workers [22]. As shown in Fig. 1, random bits were generated by exploiting stochastic programmability during the program/erase process in floating-gate 2D FETs employing WSe_2 and WS_2 channels. The authors attributed this behavior to the inherently probabilistic nature of charge trapping and detrapping in the floating gate. This study illustrates that subtle fluctuations in charge storage and transport within a transistor structure can serve directly as an entropy source. The van der Waals heterojunction device reported by Abraham et al. extended this concept to a more refined level [23]. In that work, discrete charge fluctuations were detected in a BP/WS_2/MoS_2/WS_2/graphene heterostructure and converted into an independent and identically distributed (IID) true random sequence. These results show that charge fluctuation, conventionally regarded as parasitic electrical noise, can in fact serve as a quantitatively high-quality entropy source. Jeon et al. later demonstrated a TRNG based on threshold-near charge fluctuation in a gated silicon nanosheet diode [24]. In this structure, electron injection fluctuations near the threshold induce repeated modulation of the source-side and drain-side potential barriers, thereby establishing either a positive or a negative feedback loop. When the electron injection is sufficiently strong, a positive feedback process yields bit “1”; when it is insufficient, a negative feedback process produces bit “0”. The authors showed that these carrier injection fluctuations could be directly digitized as discrete output-voltage toggling, and that the resulting bit sequence passed the NIST tests without post-processing. This result indicates that charge fluctuation can function not only as an analog irregularity but also as a practical digital entropy source without the need for complex correction schemes.

In summary, stochastic programming and charge-fluctuation-based entropy share a common foundation in the microscopic instability of charge states. This approach is particularly attractive because transistor-compatible platforms can simultaneously offer low power consumption, small footprint, and high integrability. At the same time, however, its behavior may be sensitive to interface quality, trap distribution, bias history, and environmental conditions. For practical applications, randomness quality must therefore be assessed together with long-term stability, temperature robustness, and resistance to predictive attacks.

2.2 Stochastic Switching Delay / Relaxation

Stochastic switching delay/relaxation is one of the most widely used physical mechanisms in threshold-switching TRNGs. In this approach, randomness originates from the turn-on delay required

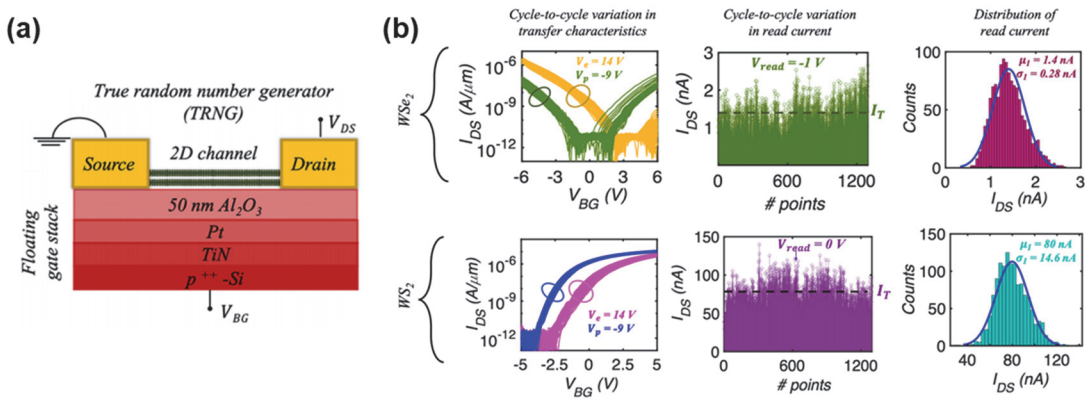

Fig. 1. (a) Schematic illustration of a floating-gate 2D FET device. (b) Programming stochasticity measured in 2D FETs with WSe_2- and WS_2-based channels (Reprinted with permission from Ref. [22]. Copyright 2021 American Chemical Society)

for the formation of a conductive path, the relaxation time associated with the return to the initial state after voltage removal, or the fluctuation of oscillation periods when such dynamics occur repeatedly. The key point is not the average ON/OFF state itself, but the fact that, even under identical operating conditions, the timing and duration of switching events vary slightly from cycle to cycle. Such temporal irregularities are especially pronounced in volatile threshold-switching devices, including diffusive memristors, ovonic threshold-switching devices, and Mott memristors, and can provide a compact and efficient hardware entropy source when combined with reset-free operation.

This concept gained particular momentum through studies that directly linked the stochastic delay and relaxation dynamics of volatile memristors to random number generation. In the 2020 work by Woo et al., a Pt/HfO_2/TiN volatile memristor was combined with a nonlinear feedback shift register (NLFSR) to extend the intrinsic stochasticity of threshold switching toward high-speed encryption-oriented TRNG operation, as shown in Fig. 2 [12]. The delay and relaxation times were used as random seeds, and the generated bitstream passed the NIST tests without post-processing. By introducing a shift-register-based architecture, the authors also sought to alleviate the low bit-generation rates that had limited earlier volatile-memristor TRNGs. Lu et al. later extended the concept of time-domain entropy further in 2022 [25]. Rather than relying only on delay-time counting, they redefined the entire integrate-and-fire process occurring repeatedly in the device as the entropy source. In other words, time-based entropy was no longer restricted to the variability of a single turn-on event, but was instead extracted from the stochasticity embedded in repetitive firing dynamics. This work clarified that stochastic switching delay/relaxation should be understood not as one-shot randomness, but as accumulated dynamical irregularity over repeated operation. More recently, Bian et al. demonstrated that this temporal stochasticity can be exploited in additional forms by using a double threshold-switching memristor structure in which stochastic duration time served as the entropy source [26]. The authors attributed its origin to the gradual dissolution of Ag conductive channels together with double-TS synergy. This suggests that the temporal irregularity of threshold-switching devices can be interpreted more broadly, encompassing not only delay and relaxation but also the duration for which a switching state is maintained.

Overall, entropy based on stochastic switching delay and relaxation is unified by its reliance on the dynamical indeterminacy of

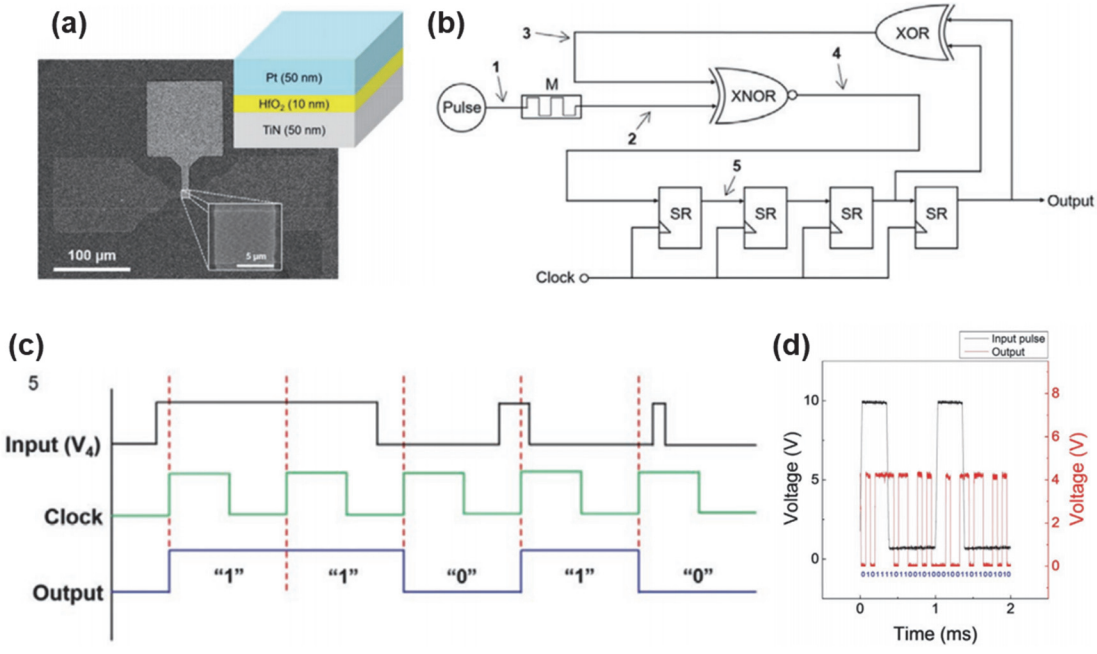

Fig. 2. (a) Schematic illustration of a Pt/HfO_2/TiN memristor device. (b) Concept of a TRNG based on a nonlinear feedback shift register and a memristor, and (c) its operating scheme. (d) Experimental results obtained from the proposed TRNG (Reprinted with permission from Ref. [12]. Copyright 2020 John Wiley and Sons)

threshold-switching devices. This approach is relatively insensitive to reference-value drift and is well suited to reset-free or self-clocking architectures. On the other hand, time-domain entropy sources still require careful consideration of throughput–endurance trade-offs, peripheral circuitry, device drift, and long-term robustness. Even so, recent studies make it clear that stochastic switching delay/relaxation remains one of the most mature and expandable entropy-source classes in emerging-device TRNGs.

2.3 Random Telegraph Noise (RTN)

Random telegraph noise is among the most extensively studied entropy sources in emerging-device TRNGs. RTN generally arises from repeated charge capture and emission at trap sites located in the dielectric or at an interface, resulting in current fluctuations between two or more discrete levels. Although this phenomenon has traditionally been regarded as an undesirable source of read-current instability in memory and sensing applications, it can instead be exploited as an unpredictable entropy source in the context of hardware security. Because RTN can be observed at low read voltages and can be combined with relatively simple readout circuitry, it has attracted considerable attention as a promising low-power entropy source for IoT and edge-device TRNGs. Its usefulness, however, depends strongly on the type and distribution of traps, the asymmetry of capture and emission times, state-to-state drift, and the sampling strategy used at the circuit level. Thus, the presence of RTN is not sufficient; its quality and stability must be evaluated systematically.

A representative circuit-level use of RTN as an entropy source was reported by Brown et al. in 2020. In that study, RTN observed in the channel current of a single CMOS transistor was used as the entropy source [27]. Unlike earlier RTN-based designs that relied primarily on two-level RTN, the authors proposed an edge-to-pulse conversion scheme capable of exploiting multi-level and abnormal RTN as well, as illustrated in Fig. 3(a). By sampling a high-frequency oscillator with digital pulses generated from the RTN signal, they produced a bitstream that passed all 15 NIST tests without complex post-processing. They also demonstrated resistance to machine-learning attacks using an LSTM neural network. A more systematic investigation of RTN quality at the materials level was later carried out by Li et al. in 2021 [28]. As shown in Figs. 3(b) and 3(c), they compared RTN characteristics

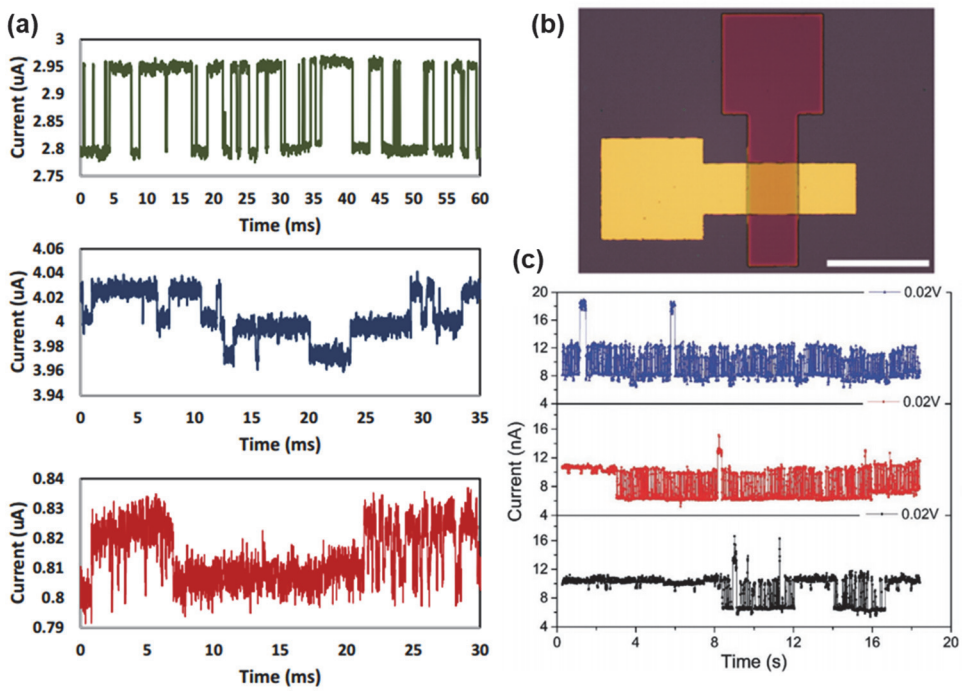

Fig. 3. (a) RTN characteristics measured from individual transistors with identical design and dimensions. (Reprinted from Ref. [27]) (b) Optical microscope image of a Ti/TiO_2/Au memristor device. (c) RTN traces measured over three repeated cycles in a Ni/TiO_2/Au memristor device (Reprinted with permission from Ref. [28]. Copyright 2021 John Wiley and Sons)

across various metal/oxide/metal memristors and proposed practical guidelines for identifying material choices and processing conditions that yield superior RTN behavior. They assessed RTN quality in terms of current level, intra-level fluctuation, capture and emission times, and long-term stability, and further showed that properly obtained RTN signals could satisfy the NIST randomness criteria in high-throughput TRNG circuits.

Subsequent work focused on actively optimizing the RTN characteristics themselves. Song et al. reported in 2023 a two-level-RTN-based TRNG using a TiO_x/Al_2O_3 memristor, showing that the capture-time probability could be tuned toward 50% by adjusting the read voltage and the device conductance state [15]. They found that RTN was more stably observed in low-conductance states, and that discrete RTN signals could be acquired reliably when the sampling frequency was sufficiently high. Yu et al. advanced further in 2024 by directly addressing variation in the RTN time constants [29]. They pointed out that capture and emission times in memristor RTN can vary widely and that, over certain intervals, identical bits may repeat for extended periods, thereby degrading randomness. To mitigate this issue, they proposed a variation-tolerant TRNG circuit incorporating a falling-edge detector, a high-speed clock, and a T flip-flop. Using a breadboard-level implementation, they showed that the resulting bitstream passed more than 14 NIST SP 800-22 tests while maintaining low autocorrelation.

Therefore, these studies demonstrate that RTN, conventionally viewed as an undesired source of read-current instability, can serve as a high-quality hardware entropy source when supported by appropriate device design and circuit implementation. Even so, RTN-based TRNGs still face challenges related to capture/emission-time asymmetry, RTN disappearance, long-term stability, device selection, and peripheral-circuit overhead. Nevertheless, because of its low-bias operation, low power consumption, and relatively simple readout requirements, RTN is likely to remain one of the most important entropy categories in emerging-device TRNGs.

3 Device Structure-Based Classification of Emerging-Device TRNGs

In the previous section, the principal entropy sources employed in emerging-device TRNGs were classified into three categories. In actual TRNG implementations, however, these entropy sources do not exist independently of device structure. Rather, they are manifested in different ways depending on the material combination, charge-transport pathway, interfacial characteristics, and circuit configuration of each device. This section, therefore, revisits the entropy mechanisms discussed above from the standpoint of device architecture to clarify how they are embodied in practical TRNG platforms. For this purpose, emerging-device TRNGs are grouped here into three broad classes: transistor-based TRNGs, threshold-switching-device-based TRNGs, and other emerging-device/platform TRNGs. This classification makes it possible not only to compare how a given entropy source is realized across different device structures, but also to identify which entropy mechanism tends to dominate within a given structural class.

3.1 Transistor-Based TRNGs

As discussed in the previous section, stochastic programming and charge fluctuation constitute the most representative entropy mechanisms in transistor-based TRNGs. Recent studies in this category have predominantly relied on phenomena such as charge trapping and detrapping in floating gates, discrete charge fluctuation at heterointerfaces, carrier injection fluctuation near threshold, or operation-induced carrier multiplication and escape to generate random bits. The principal advantage of this class lies in its ability to preserve the inherent benefits of transistor platforms, including high integrability, small footprint, and low power consumption, while directly exploiting subtle charge dynamics within the device or at its interfaces as a physical entropy source. Recent progress also shows that transistor-based TRNGs have moved well beyond the simple notion of "generating randomness with a transistor" and are instead evolving into more practical hardware-security platforms through structural diversification and functional refinement. The key performance metrics of recently reported transistor-based TRNGs are summarized in Table 1.

Wali and co-workers developed a floating-gate 2D FET-based TRNG using WSe_2 and WS_2 channels together with an Al_2O_3/Pt/TiN/Si floating-gate stack [22]. In this structure, the stochastic nature of charge trapping and detrapping during the program/erase process was exploited as the primary source of randomness. The generated bitstream passed the NIST randomness tests without post-processing, and the device exhibited high entropy, uniformity, uniqueness, and unclonability, together with resistance to regression-based machine-learning attacks. The reported bit-generation energy of approximately 10 pJ/bit further suggests that this architecture is well-suited to low-power hardware-security primitives for edge devices. Abraham et al. approached the

Table 1. Summary of the performance of recently reported transistor-based TRNGs

Ref.	Device type	Material	Entropy sources	Bit rate	Energy per bit	Validation
[22]	FG[1] 2D FET	WSe_2, WS_2	Stochastic programming	NR	~10 pJ/bit	NIST test suite ML[2] attack evaluation
[23]	vdW heterojunction entropy device	BP, WS_2, MoS_2, WS_2, graphene	Discrete charge fluctuation	~162 kb/s	~2.3 pJ/bit of entropy	NIST test suite
[30]	MoS_2 Fe-FET array	MoS_2, HZO[3]	Ferroelectric switching + charge trapping	NR	NR	NIST test suite ML attack evaluation
[31]	Peripheral-free 2D FET	MoS_2	Charge trapping / detrapping	NR	~30 pJ/bit	NIST test suite ML attack evaluation
[16]	Cryptoristor	Floating-body cryptoristor	Stochastic carrier escape	75 kb/s	3.29 pJ/bit	NIST test suite
[24]	Gated silicon nanosheet diode	Gated p-i-n silicon nanosheet diode	Carrier injection fluctuation	25 kb/s	91.8 pJ/bit	NIST test suite
[32]	BHN-NTC[4] transistor	NTC transistor with PTCDI-C13	Correlated trapping/detrapping	3 bit/sample event	NR	NIST test suite

[1] Floating-gate

[2] Machine learning

[3] Hafnium zirconium oxide

[4] bi-heterojunction noise-enhanced negative transconductance

problem from a different angle by identifying discrete charge fluctuation occurring within a van der Waals heterojunction itself as a more fundamental entropy source, rather than relying on threshold shifts or memory-like programming effects [23]. Their BP/WS_2/MoS_2/WS_2/graphene heterostructure used engineered electron traps and quantum-well-like carrier confinement to produce high-quality IID random streams. The min-entropy exceeded 0.98 bits/bit, while the entropy generation rate reached approximately 162 kb/s with an energy cost of about 2.3 pJ per bit of entropy. The authors also showed stable operation from cryogenic to ambient conditions.

Transistor-based TRNGs built from 2D materials were extended to the integrated-circuit level. As shown in Figs. 4(a) and 4(b), Chien et al. reported a MoS_2 ferroelectric Fe-FET TRNG in which ferroelectric switching and charge trapping were combined to enhance stochastic variability [30]. Using a self-corrected TRNG array together with comparator-based circuitry, they demonstrated the feasibility of cryptographic key generation. The study also examined near-ideal entropy, a Hamming distance close to 50%, negligible autocorrelation, endurance beyond 106 cycles, temperature robustness, and resistance to both Fourier-regression- and LSTM-based machine-learning attacks. Ravichandran et al. further advanced this direction by implementing a peripheral-free TRNG composed of two cascaded three-stage inverters and an XOR gate using monolayer MoS2 FETs, as shown in Figs. 4(c) and 4(d) [31]. In this design, the voltage transfer characteristic fluctuated stochastically because of charge trapping and detrapping at the MoS_2/Al_2O_3 interface. The system achieved a minimum normalized entropy of 0.8780 and an average of 0.8875 under NIST SP 800-90B, while the generated bitstream passed NIST SP 800-22 without post-processing. The reported energy consumption, approximately 30 pJ/bit, illustrates that 2D transistor-based TRNGs have progressed from individual stochastic devices to low-power integrated security blocks.

Kim et al. reported a cryptoristor-based TRNG in which irregular oscillation in a floating-body FinFET-type structure served as the entropy source [16]. They attributed the origin of randomness to random carrier multiplication and stochastic carrier escape. In this system, an analog stochastic signal was digitized through a noise-coupling ADC, yielding a bit-generation rate of 75 kb/s with an energy consumption of 3.29 pJ/bit. The device also showed little degradation in randomness quality under repeated electrical stress

or temperature variation. Jeon et al. likewise demonstrated the potential of a silicon-based single-device entropy source using a gated silicon nanosheet diode [24]. In this structure, carrier injection fluctuation near threshold interacted with positive feedback to generate directly digitized outputs, providing a raw signal margin of about 1 V between random bits “0” and “1” without the need for amplification or post-processing. The bit-generation rate was 25 kb/s, with an energy cost of 91.8 pJ/bit, and stable uniformity, Hamming distance, and correlation coefficients were maintained even after 2 × 105 pulse cycles.

More recently, efforts have also been made to increase entropy density itself by deliberately amplifying nonlinear transport characteristics and correlated noise in transistor structures. Han et al. developed a TRNG based on a BHN-NTC transistor with an asymmetric PTCDI-C13 layer inserted into a bi-heterojunction structure, as shown in Fig. 4(e) [32]. This design widened the negative-transconductance region and strongly enhanced the correlation between trapping/detrapping noise and generation/recombination noise. As a result, whereas earlier transistor-based TRNGs produced one bit per sampling event, this device generated three bits per sampling event while still passing the applicable NIST tests. The same stochastic source was also used to improve performance in StyleGAN2-based image generation, suggesting that transistor-based TRNGs may find roles not only in secure

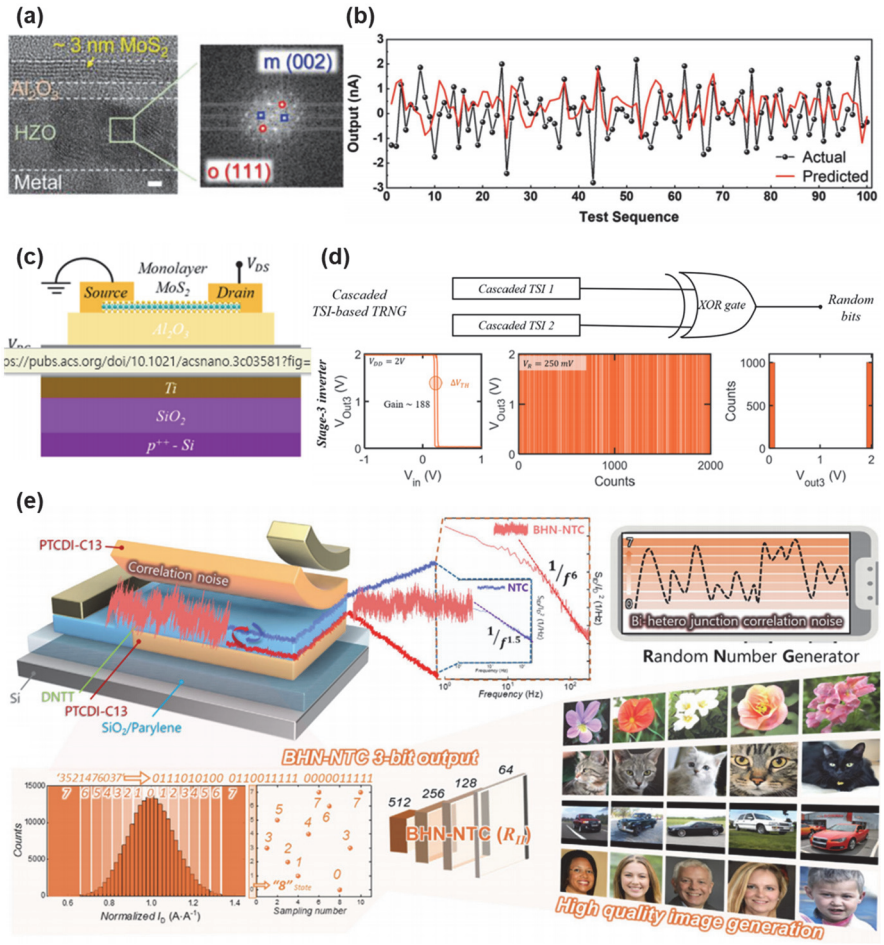

Fig. 4. (a) Cross-sectional HRTEM image and corresponding FFT analysis of MoS_2 ferroelectric field-effect transistors. (b) Actual and prediction results for output patterns obtained using a long short-term memory (LSTM)-based machine learning model. (Reprinted with permission from Ref. [31]. Copyright 2023 American Chemical Society) (c) Schematic illustration of a monolayer MoS_2 FET device. (d) Schematic of a cascaded TSI-based TRNG composed of two cascaded TSIs and an XOR gate. (Reprinted from Ref. [30].) (e) Overall schematic of a TRNG based on a BHN-NTC transistor and its application to high-quality image generation (Reprinted from Ref. [32].)

electronics but also in probabilistic computing and stochastic AI hardware.

In summary, transistor-based TRNGs are evolving beyond simple trap-fluctuation-driven random-number generators toward highly integrated, high-entropy, and application-oriented hardware-security platforms, with recent work increasingly incorporating operation-induced carrier dynamics and correlated noise amplification. As a result, transistor-based TRNGs occupy an important position between conventional CMOS circuit-based TRNGs and single emerging-material stochastic devices.

3.2 Threshold-Switching-Device-Based TRNGs

As outlined in the previous section, stochastic switching delay and relaxation represent the most characteristic entropy mechanisms in threshold-switching (TS) devices. In TS-device-based TRNGs, the essential source of randomness lies in the fact that, even under the same operating conditions, the turn-on delay, relaxation time, oscillation period, and timing of firing events exhibit slight cycle-to-cycle variations. This temporal indeterminacy is directly converted into random bits. In addition, unlike nonvolatile memories, volatile threshold-switching devices return spontaneously to their initial state without a separate RESET process, making them particularly attractive for compact, reset-free entropy hardware. For these reasons, TS-device-based TRNGs may be regarded as one of the most mature and rapidly advancing classes within the broader field of emerging-device TRNGs. The key performance characteristics of recently reported TS-device-based TRNGs are summarized in Table 2.

Jiang et al. reported the Ag:SiO_2 diffusive memristor TRNG in Nature Communications in 2017 [13]. As illustrated in Figs. 5(a) and 5(b), the authors converted stochastic delay time into digital random bits by combining the device with a comparator, an AND gate, and a counter. The resulting TRNG achieved a bit-generation rate of 6 kb/s and passed all 15 NIST tests without post-processing.

Table 2. Summary of the performance of recently reported TS-device-based TRNGs

Ref.	Device type	Material	Entropy sources	Bit rate	Energy per bit	Validation
[13]	Diffusive memristor	Ag:SiO_2	Stochastic delay time	6 kb/s	NR	all 15 NIST tests
[12]	Volatile memristor	HfO_2	Delay / relaxation time	16 kb/s	NR	NIST test suite
[33]	Diffusive memristor	$Cu_{0.1}Te_{0.9}$ HfO_2	Stochastic delay + relaxation times	32 kb/s	NR	all 15 NIST tests
[14]	Mott device	NbO_x	Thermal fluctuation	at least 40 kb/s	5.23 nJ/bit	all NIST tests
[25]	Diffusive memristor	$HfO_x/HfO_y/HfO_x$	Random integrate-and-fire process	≈108 kb/s	NR	NIST test suite
[26]	Double TS[1] memristor	Ag:i-carrageenan	Stochastic relaxation time	NR	NR	all 15 NIST tests
[36]	Diffusive memristor	FF MR[2]	Randomly distributed current response	NR	NR	NIST test suite
[34]	OTS[3]	$GeTe_x$	Random oscillation	2.22 Mb/s	NR	12 executable NIST tests
[35]	Mott device	NbO_x	Enhanced Johnson–Nyquist noise	100 kb/s	0.68 μJ/bit	NIST test suite
[37]	2D TS memristor	multilayer h-BN	Spike amplitude stochasticity	NR	NR	11 NIST tests

[1] Threshold switching

[2] Phenylalanine dipeptide microrod

[3] Ovonic threshold switch

Building on this concept, Woo et al. proposed in 2020 a high-speed-encryption-oriented architecture that combined a Pt/HfO_2/TiN volatile memristor with a nonlinear-feedback shift register [12]. In 2021, they further reported a diffusive memristor TRNG based on $Cu_{0.1}Te_{0.9}$/HfO_2/Pt, in which both stochastic delay time and relaxation time were used as entropy sources [33]. That device reached a bit-generation rate of 32 kb/s, while 55 independent sequences of 106 bits each passed all 15 NIST tests without post-processing. Stable operation was also maintained at 80°C.

TS-device-based TRNGs have not remained limited to delay-time harvesting, but have also expanded toward the direct use of oscillatory dynamics. Kim et al. reported in 2021 a self-clocking TRNG based on stochastic oscillation in an NbOx Mott memristor, as shown in Fig. 5(c) [14]. This architecture achieved at least 40

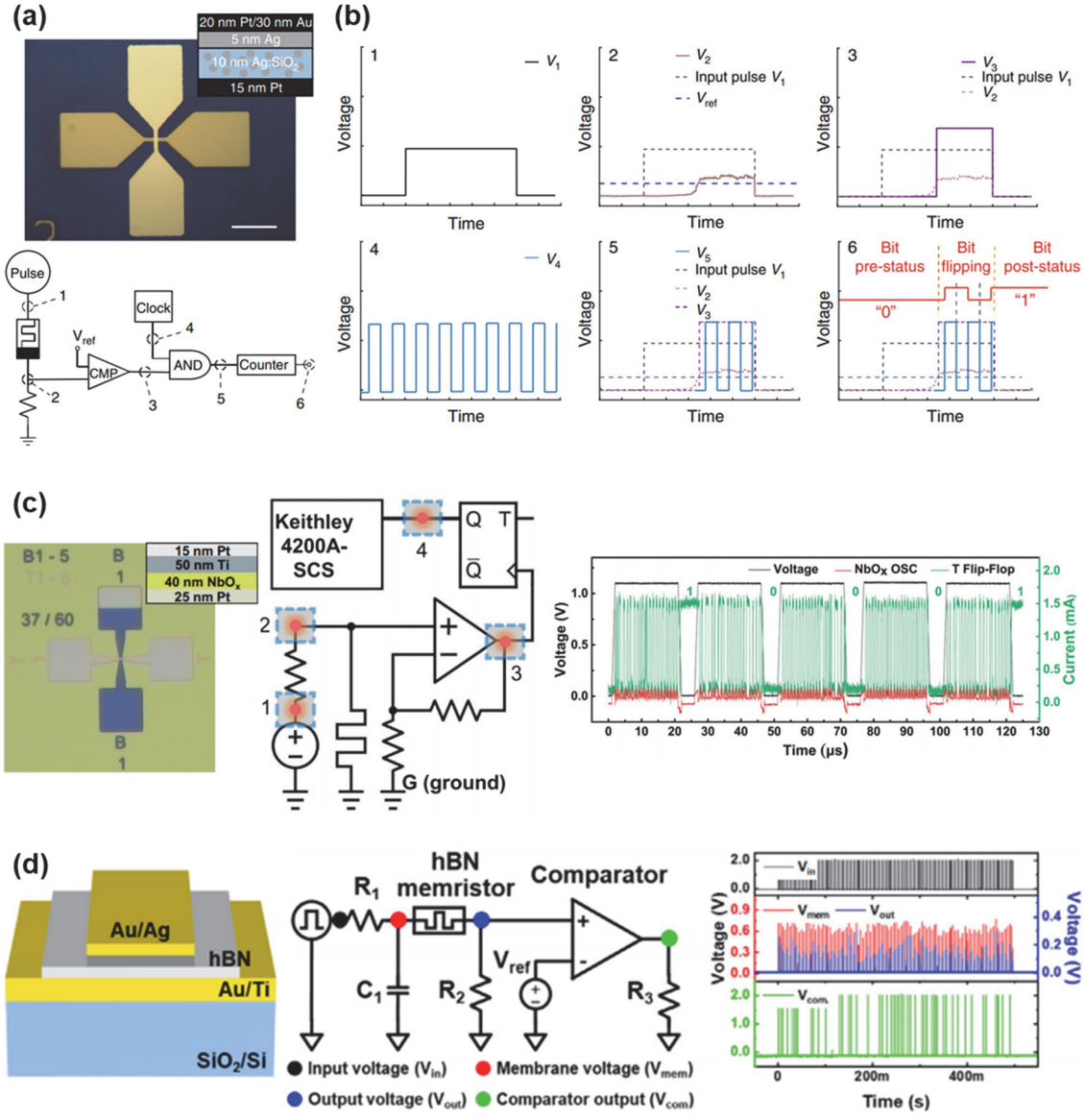

Fig. 5. (a) Schematic illustration of an Ag:SiO_2-based diffusive memristor device and the corresponding TRNG circuit diagram. (b) Schematic pulse waveforms at each stage of the TRNG circuit. (Reprinted from Ref. [13].) (c) Optical microscope image of an NbO_x-based two-terminal device, together with the corresponding TRNG circuit diagram and measured TRNG characteristics. (Reprinted from Ref. [14].) (d) Schematic of an h-BN-based TS memristor device, along with the corresponding TRNG circuit diagram and measured results (Reprinted from Ref. [37].)

kb/s without the need for an external clock. The authors argued that thermal fluctuation accumulates during oscillation and gives rise to variations in peak interval time. Using 130 Mbits of data, they showed that the generated output passed all NIST tests. The device also exhibited strong tolerance to temperature variation between 300 and 390 K and to device-to-device variation, while the self-clocking design eliminated the need for an additional clock generator. This oscillatory TS-TRNG approach was subsequently pushed toward higher speed. Fu et al. reported in 2023 an ovonic threshold-switching memristor based on GeTex, which achieved a throughput of 2.22 Mb/s per cell together with an endurance of 2 × 10^9 bits and successful completion of 12 executable NIST tests.[34] More recently, Kim et al. introduced a cell-integrated heater into an NbO_x Mott memristor architecture and deliberately enhanced Johnson–Nyquist noise, reporting 100 kb/s and 0.68 μJ/bit [35]. These studies demonstrate that TS-device-based TRNGs are improving both throughput and robustness by making more active use of temporal stochasticity.

Entropy extraction from diffusive memristors has itself become more diverse. Lu et al. reported in 2022 a calibration-free self-clocking TRNG based on an Ag/TiN/HfO_x/HfO_y/HfO_x/Pt multilayer structure that exploited a random integrate-and-fire process [25]. Instead of comparing delay time or threshold voltage against a reference value, this method classified the number of firing spikes within an excitation period as odd or even, thereby avoiding calibration problems arising from parameter drift. The authors reported a theoretical throughput of approximately 108 kb/s based on a switching time of 60 ns and a relaxation time of 500 ns. Although the raw 1,000-bit data could complete only nine executable NIST tests, an LFSR-assisted 1-Mbit stream passed all 15 NIST tests. This work underscores that, in TS-device TRNGs, performance is shaped not only by device speed but also by how stochastic events are digitized. Subsequent work has explored modified TS-device structures and more specialized entropy sources in order to broaden application possibilities. Bian et al. reported a double threshold-switching memristor with an Au/Ag:i-carrageenan/Pt structure, using stochastic relaxation time as the entropy source [26]. They attributed reliable bitstream formation to the gradual dissolution of Ag conductive channels together with double-TS synergy. Nineteen megabits of data passed all 15 NIST tests without post-processing, and the resulting true random keys were used for XNOR-based image encryption and decryption. The authors further showed that decryption remained functional up to a certain level of added Gaussian noise. Xing et al. took a different approach by using the randomly distributed current response of a diffusive memristor as the entropy source rather than stochastic delay or relaxation time [36]. In an Ag/phenylalanine dipeptide microrod/Ag device, the response current under input pulses was probabilistically distributed, and the probability of generating bit "0" or "1" could be tuned through the comparator and reference-voltage setting. A notable feature of this design is that ideal 50% uniformity could be approached by adjusting the reference voltage, and XOR-based image encryption was demonstrated using a key of 256 × 256 × 8 bits. This indicates that TS-device TRNGs are expanding beyond switching time to include current-amplitude distributions as usable entropy sources. Most recently, TRNGs based on 2D-material TS memristors have begun to emerge. Jo et al. reported in 2026 a multilayer h-BN volatile memristor-based TRNG in which a spike generator was constructed and spike amplitude was binarized with a comparator, as shown in Fig. 5(d) [37]. The device operated under 2.0 V, 200 μs pulse width, and 5 ms period conditions, with an average turn-on rate of 50.04 ± 3.60%. The generated bitstream passed 11 NIST tests without post-processing, and XOR-based encryption/decryption of both black-and-white and grayscale images was successfully demonstrated.

Overall, TS-device-based TRNGs are developing in a direction that simultaneously improves throughput, robustness, and self-clocking capability through increasingly sophisticated combinations of device physics and circuit design. The fact that the scope of usable entropy sources now includes stochastic delay, relaxation, oscillation, integrate-and-fire dynamics, and current-response distributions clearly reflects the broad versatility of this class. TS-device platforms can therefore be regarded as one of the central and still rapidly advancing pillars of emerging-device TRNG research.

3.3 Other Emerging-Device/Platform TRNGs

Whereas the two previous subsections are each tied relatively closely to a particular entropy mechanism, some recently reported TRNG platforms cannot be reduced to a single device category. In practice, a growing number of TRNG studies involve hybrid platforms that are difficult to classify simply as transistor-based structures or threshold-switching memristors. What these systems share is that they realize entropy sources through either material-specific physical phenomena or system-level circuit integration. For this reason, such platforms are treated here as a separate category in order to highlight how rapidly the scope of TRNG research is expanding. The main performance metrics of recently reported emerging-device/platform TRNGs are summarized in Table 3.

Liu et al. reported in 2022 an ACS Nano paper on a TRNG based on a Bi_2O_2Se memristor [20]. This work exploited the high carrier

Table 3. Summary of the performance of recently reported other emerging-device/platform TRNGs

Ref.	Device type	Material	Entropy sources	Bit rate	Energy per bit	Validation
[20]	2D memristive TRNG	Bi_2O_2Se	RTN + switching probability distribution	NR	NR	HD[1]/Hamming weight ML resilience
[38]	Hardware-integrated RTN TRNG	h-BN	RTN	30 kb/s practical, up to ~7.8 Mb/s max	~3.3 nJ/bit at 30 kb/s ~1.28 pJ/bit at max throughput	all 15 NIST tests
[10]	Correlated-oxide TRNG	$LaCoO_3$	self-oscillation in spin crossover	50 kb/s	NR	all 15 NIST criteria
[39]	Hybrid chaotic TRNG	SnS_2	electron trapping/detrapping + chaotic modulation	10 kb/s	4.3 μJ/bit	NIST test suite
[40]	Physical entropy noise TRNG	1T′-$MoTe_2$	conductance noise	>1 Mb/s secure random numbers	NR	NIST test suite
[41]	Stochastic photoresponse TRNG	PLGA[2] -$MAPbI_3$	trap-assisted stochastic photoresponse / photovoltage fluctuation	10 kb/s	NR	NIST test suite
[42]	Light-induced TRNG	SnO_2 QDs[3], F8BT[4]	competing positive/negative photocurrent	2 kb/s in main demo, enhanced circuit 10 kb/s	NR	all 15 NIST criteria

[1] Hamming distance

[2] Poly-L-glutamic acidmonosodium salt

[3] Quantum dots

[4] Poly(9,9-dioctylfluorene-alt-benzothiadiazole

mobility, air stability, low thermal conductivity, and vertical surface resistive-switching characteristics of Bi_2O_2Se to implement a bimodal analogue/digital TRNG. In analogue mode, amplitude-controllable RTN was used to encrypt and decrypt human voice data, whereas in digital mode, a broadly distributed set voltage was used to produce a random bitstream for a Diffie–Hellman key-exchange demonstration. The study also showed that the intra-Hamming distance was distributed near the ideal value of 50%, and it discussed resistance to machine-learning prediction using LSTM analysis and Shapley value visualization. A closely related but more hardware-oriented example was reported by Pazos et al. in Nanoscale in 2023 [38]. As shown in Figs. 6(a–c), they extended a 2D-material TRNG to a stand-alone hardware platform by using an Ag/h-BN/Ag memristor that generated stable RTN at low voltage, in combination with a transimpedance amplifier, an Arduino microcontroller, and a 19-bit NLFSR. The RTN signal was sampled at 15 Hz and used as a seed, after which the NLFSR produced continuous random output. The system was designed to continue operating even if the RTN signal disappeared for as long as 20s, and more than 5 Mbits of output passed all 15 NIST tests. The average energy consumption was estimated to be about 3.3 nJ/bit at 30 kb/s and as low as 1.28 pJ/bit at a maximum throughput of about 7.8 Mb/s.

Correlated oxides and hybrid systems also point to directions that cannot be neatly folded into conventional categories. Woo et al. proposed a TRNG based on $LaCoO_3$ biased in its spin-crossover regime so as to induce self-oscillation [10]. They argued that phase-transition-based TRNGs are often difficult to control because of their narrow operating windows and abrupt transition behavior, whereas spin crossover in $LaCoO_3$ provides a broader and more gradual operating range that is more favorable for true stochasticity. The device passed standard stochasticity tests and reportedly required only about half as many circuit components as earlier TRNGs. The same stochastic source was also used for

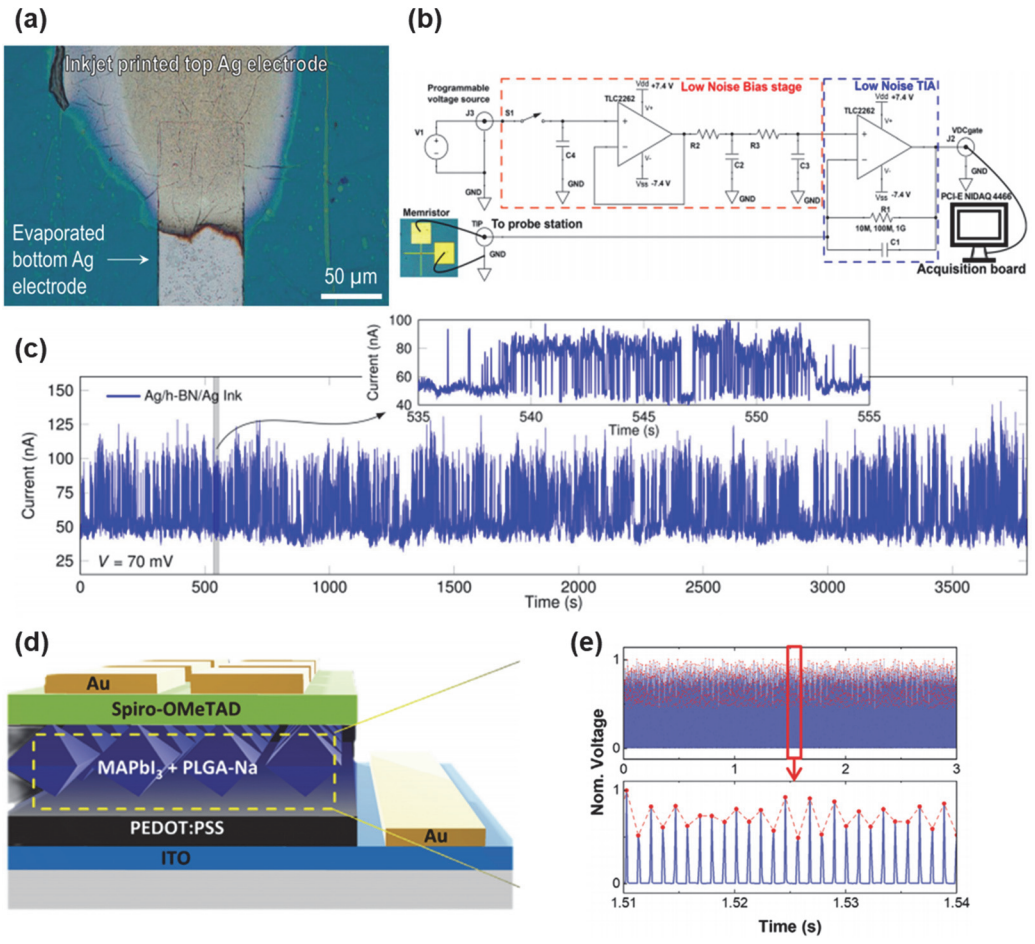

Fig. 6. (a) Optical microscope image of an Ag/h-BN/Ag memristor device. (b) Schematic of the measurement circuit used to acquire low-frequency noise and RTN signals from the h-BN-based device, and (c) the corresponding measurement results. (Reprinted from Ref. [38].) (d) Schematic of a polymer-blended MAPbI3 perovskite device, and (e) measured voltage variation of the device (Reprinted from Ref. [41].)

probabilistic max-cut problem solving, yielding solution quality superior to that obtained with software-generated randomness. Rehman et al. proposed a hybrid platform combining a memtransistor with a chaotic circuit [39]. In this work, cycle-to-cycle variability arising from electron trapping and detrapping in an SnS_2 memtransistor served as the base entropy source, which was then injected into an energy-efficient analog Lorenz chaotic circuit to transform it from a pseudo-chaotic system into a more truly random-like one. The resulting system achieved a throughput of 10 kb/s and an energy consumption of 4.3 μJ/bit, while device endurance exceeded 10^8 cycles. This result suggests that combining single-device stochasticity with system-level chaotic dynamics can improve both randomness quality and functional flexibility. Liu et al. also reported in 2024 a Nano Letters study showing TRNG operation based on conductance noise in structurally metastable 1T′-$MoTe_2$ [40]. They found that the noise followed Poisson statistics and remained a robust physical entropy source even at low and cryogenic temperatures. Their analysis further suggested that the phenomenon may be related to variations in ferroelectric dipole polarization within 1T′-$MoTe_2$. The generated random numbers were used as seeds for a secure random number generator that produced secure random streams above 1 Mb/s, and the work also demonstrated an application in masking biometric information in neural networks.

Optically driven platforms have also begun to emerge rapidly in recent years. Figure 6(d) presents a schematic of the TRNG reported by Ahn et al. in Advanced Science in 2025, which was based on an anionic polymer/perovskite hybrid photodetector [41].

In that system, stochastic photoresponse was used as the entropy source, yielding random numbers at 10 kb/s and a 10-Mbit sequence subjected to NIST evaluation. The authors also demonstrated image encryption using a 480,000-bit random sequence, showed that the device remained functional when light was transmitted through pork skin, and examined the retention of photovoltage generation under changes in vibration, temperature, and humidity. These results suggest that optically responsive devices may be extended beyond TRNGs toward wearable or implantable security platforms. Park et al. proposed another photonic route in a 2025 Advanced Materials paper, where the entropy mechanism did not rely on electrical noise or memristive switching but on polarity competition under optical excitation [42]. Their light-induced TRNG combined polychromatic light generated by arc discharge with a bipolar photoresponsive photodetector that produced photocurrents of opposite polarity under DUV and blue light. The system retained stability after storage at 100°C for 180 days and demonstrated wireless security-code generation at 2 kb/s using a custom readout circuit. An expanded circuit was also examined for 10 kb/s operation, and the resulting bitstream passed all 15 NIST criteria. These findings show that optical platforms can provide entropy sources through mechanisms fundamentally different from those of electronic switching devices.

In summary, other emerging-device/platform TRNGs reveal how the entropy categories discussed earlier are expanding beyond the conventional frameworks of transistors and threshold-switching devices. In particular, 2D-material memristive platforms, correlated oxides, structurally metastable 2D materials, hybrid chaotic systems, and photoresponsive devices all point to directions that are not easily captured by existing classification schemes. This category should therefore not be regarded as a collection of exceptional cases, but rather as an important indicator of how emerging-material-based TRNG research may expand toward new materials, new physical mechanisms, and new system architectures.

4 Randomness Validation and Benchmarking

The performance of a true random number generator cannot be assessed solely by asking whether it produces a bitstream that appears random. For emerging-device-based TRNGs in particular, evaluation must extend beyond the statistical properties of the output bitstream to include how unpredictable the underlying physical entropy source actually is, whether its characteristics remain stable over prolonged operation, and whether it satisfies functional requirements such as online testing and fault detection. For this reason, TRNG evaluation has gradually moved beyond a simple pass/fail perspective toward a multi-layered framework that considers the statistical randomness of the output bitstream, the min-entropy and health of the entropy source, and the functional reliability required for practical system deployment.

The criterion most widely used to assess the quality of random numbers generated by emerging-material-based TRNGs is NIST SP 800-22 [43]. This standard evaluates whether an output bitstream exhibits statistically random behavior through a range of tests, including frequency, runs, longest run, binary matrix rank, spectral test, template matching, and linear complexity. Accordingly, it has served as the most common randomness-evaluation tool in the majority of reported emerging-device TRNG studies. However, SP 800-22 is fundamentally a standard for determining whether an output bitstream exhibits random-like patterns; it does not directly quantify the unpredictability of the entropy source that produced that bitstream. Thus, although a reported “pass” in NIST SP 800-22 is clearly an important first indicator, it is not sufficient on its own to conclude that the underlying entropy source is robust and secure.

To address this limitation, NIST SP 800-90B provides a framework more specifically focused on entropy-source validation [44]. In SP 800-90B, an entropy source is described in terms of a noise source, a conditioning component, and health tests. Min-entropy is treated as the central metric, and the validation procedure includes IID/non-IID assessment, restart tests, repetition count tests, and adaptive proportion tests. In other words, whereas SP 800-22 is primarily concerned with the statistical randomness of the output bitstream, SP 800-90B is intended to evaluate, in a more conservative manner, how much unpredictability the entropy source itself actually provides. At the same time, the estimators used in SP 800-90B have also been subject to critical examination in recent studies. Some reports have shown that the collision and compression estimators may substantially underestimate min-entropy for non-IID entropy sources, whereas certain other estimators may overestimate entropy for biased distributions [11,45]. It has also been pointed out that strong correlations may exist among different estimators. These observations suggest that SP 800-90B results should not be interpreted as absolute values based on a single estimate, but rather in light of the IID or non-IID nature of the data and the possible bias of the estimator being used.

From a more certification-oriented perspective, BSI AIS 20/31 is also an important reference [46]. The revised 2024 version

distinguishes deterministic RNGs, physical true RNGs, and non-physical true RNGs, and defines functionality classes such as PTG.2 and PTG.3 specifically for physical TRNGs. Unlike a purely statistical black-box test, this framework requires a more systematic evaluation that includes a stochastic model, online testing, total failure testing, and start-up testing. Although most emerging-material-based TRNG studies do not yet satisfy the full set of these certification requirements, AIS 20/31 is nonetheless useful because it indicates which additional elements will be needed if current device demonstrations are to evolve into practical security hardware. Accordingly, the validation of emerging-material-based TRNGs should be understood not simply in terms of whether a device passes an NIST test, but in terms of a broader assessment that includes the statistical randomness of the output bitstream, the min-entropy and health of the entropy source, and the potential for certification based on long-term and functional reliability.

5 Toward Wearable and Flexible TRNGs

As research on TRNGs based on emerging materials has matured, recent work has increasingly moved beyond the demonstration of new devices with high randomness quality and toward their extension into wearable and flexible electronics [47,48]. This development has proceeded along two main directions. One is the realization of flexible hardware TRNGs that operate directly on mechanically compliant substrates. The other is the use of biosignal- or sensor-derived entropy obtained from the human body or from user activity as a cryptographic entropy source. The former emphasizes the mechanical flexibility, compactness, and low-power characteristics of material-based devices and circuits, whereas the latter treats the wearable device itself as an entropy-harvesting platform that remains close to the user at all times. Both directions arise from the same practical demand in IoT and edge-computing environments: security hardware that is lightweight, compact, low-power, and physically close to the point of use.

From the standpoint of flexible hardware, a representative example is the natively flexible IGZO-circuit-based TRNG reported by Gołofit et al. in 2023. In that work, a TRNG was implemented by combining a chaotic circuit with the metastable oscillation of an RS flip-flop using metal-oxide TFT technology [49]. The device produced a constant bitstream of 66.7 kb/s with a power consumption of 200 μW in an area of 0.3 mm^2. Importantly, this architecture was not obtained by simply thinning a rigid CMOS circuit, but was instead specifically designed for one-type-only TFT-based flexible integrated circuits and their associated constraints. The authors further showed, through area and power comparisons with a flexible 32-bit ARM microprocessor, that the proposed TRNG could be integrated into flexible electronic systems without imposing a substantial burden. More recently, there have also been attempts to combine storage and TRNG functionality within a single flexible memristive device. Wang et al., in a 2025 Nano Energy paper, proposed a low-voltage, forming-free, multifunctional flexible memristor based on a Ti_3C_2 MXene-doped PEI composite [50]. In that study, MXene doping was used not only to stabilize filament formation by tuning the local electric field and ion-migration pathways, but also to induce statistically distributed switching delay under the same voltage stimulus, thereby enabling the device to function as a high-entropy physical source. The device was fabricated on a flexible polyimide substrate and was proposed as a platform capable of performing both nonvolatile memory and TRNG functions within a single hardware element. These works suggest that future flexible edge devices may integrate storage, computation, and security functions on a common mechanically compliant platform.

Another direction in wearable TRNGs involves the use of physiological or sensor signals derived from the human body or from user activity as entropy sources. Yu and Kim proposed a TRNG that used values from a PPG sensor embedded in a wearable device as a physical random source [51]. Their system combined a 16-bit LFSR with PPG-based physiological signals and performed random-number generation on an FPGA, with the resulting bitstream evaluated using the NIST test suite. This study suggested that a wearable device could serve not as a display or sensing platform, but also as a security platform that directly utilizes human physiological signals as an entropy source. Camara et al. later developed this idea more systematically from the perspective of body sensor networks [52]. GSR signals measured from sensors attached to the human body, as shown in Fig. 7(a), were used as the entropy source for a TRNG. After analyzing both the entropy source and the generated output, they concluded that the output behaved as if it had been produced by a random variable. More recently, commercial smartwatches have begun to be considered as stand-alone entropy-harvesting platforms. Švarcmajer et al. evaluated whether motion, physiological, and environmental sensor data collected from a Wear OS-based commercial smartwatch could be used for local cryptographic key generation [53]. As shown in Fig. 7(b), they compared still and shake modes and implemented the entire pipeline—from sensor-data acquisition

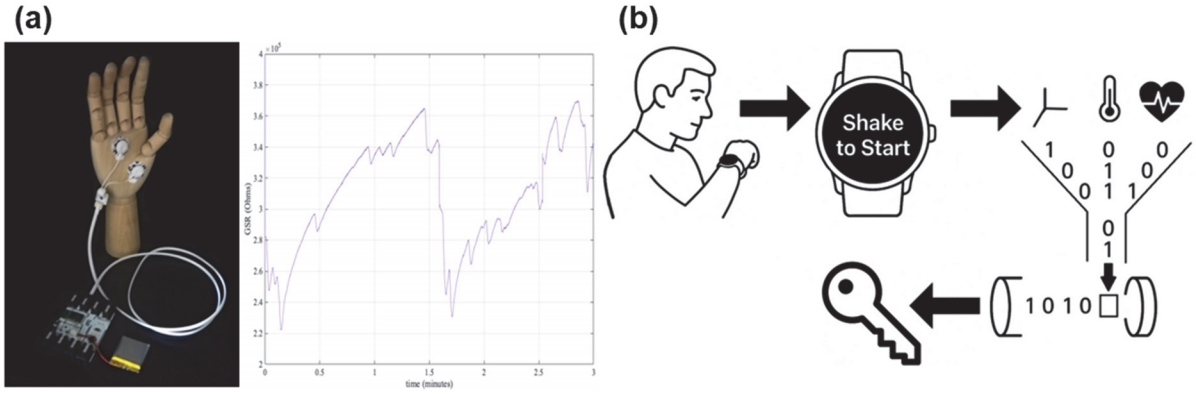

Fig. 7. (a) Electrode configuration for galvanic skin response (GSR) signal measurement and the corresponding measured signal (Reprinted from Ref. [52].) (b) illustration of the entropy generation process using a smartwatch (Reprinted from Ref. [53].)

to vectorization, 8-bit discretization, and SHA-256 hashing—fully offline, without relying on external hardware or cloud infrastructure. Their results indicate that, although the entropy level may be lower than that of a dedicated TRNG, a commercial wearable device can still function as a user-friendly local entropy source when accompanied by appropriate post-processing.

At the same time, not all assessments of wearable sensor-derived entropy have been optimistic. In 2025, Shepherd and Hurley examined the entropy available in mobile sensor data more critically and showed that, even when multiple sensor modalities are combined, the worst-case min-entropy may remain much lower than expected [54]. They reported that the min-entropy of a single sensor can be only about 3.4–4.5 bits, and that even the combination of more than twenty sensing modalities may yield a joint min-entropy of no more than roughly 22 bits. Their findings caution against the assumption that simply adding more sensors will automatically provide high security. This suggests that, while wearable biosignal- or sensor-based entropy is an intriguing direction, it is more realistic to interpret it not as a stand-alone cryptographic entropy source, but rather in conjunction with suitable post-processing, auxiliary entropy sources, or dedicated hardware TRNGs.

Overall, wearable and flexible TRNGs remain at an early stage, but they already represent one of the most important routes by which emerging-material-based TRNGs are being extended toward practical operating environments. Flexible hardware TRNGs point to the feasibility of mechanically compliant security circuits, while biosignal- and sensor-derived entropy points toward user-coupled security platforms. Future research will likely benefit from combining these two approaches in complementary ways, with the goal of realizing lightweight, low-power, and highly reliable personalized security hardware.

6 Conclusion

This review has examined TRNG research based on emerging material-based semiconductor devices from the perspectives of entropy sources, device structures, randomness validation, and wearable/flexible extensions. The overall direction of recent work shows that emerging-material-based TRNGs are moving beyond the simple use of new materials for random-number generation and toward a more deliberate identification of the physical origins of stochasticity, followed by their implementation in practical hardware-security platforms. In particular, stochastic programming/charge fluctuation, stochastic switching delay/relaxation, and random telegraph noise have emerged as the most representative entropy sources, and these have been realized through transistor-based platforms, threshold-switching devices, and a range of hybrid architectures. At the same time, the evaluation of emerging-material-based TRNGs must be interpreted using criteria that go beyond a simple pass under NIST SP 800-22 and instead include more refined measures such as min-entropy, health tests, and robustness. Recent efforts in wearable and flexible systems further suggest that these TRNGs may be extended toward edge computing, IoT, and personalized security hardware. Future work will therefore need to focus on device platforms capable of delivering both high entropy quality and high throughput, the establishment of more reliable validation frameworks, and the integration of these TRNGs into practical system-level environments.

ORCID

Daniel Juhyung Joe https://orcid.org/0000-0002-1945-8236
Joon Young Kwak https://orcid.org/0000-0002-7799-8812

Acknowledgement

This work was supported by the National Research Foundation of Korea (NRF) (Grant nos. RS-2023-00262880, RS-2024-00468995, and RS-2025-00517637). This research was also supported by the Development of advanced bio and medical measurement technology funded by Korea Research Institute of Standards and Science (KRISS–2026–GP2026–0007).

Conflict of Interest

The authors have no conflicts of interest to declare.

Author Contributions

Yooyeon Jo: Conceptualization, Investigation, Writing - Original Draft, Visualization.
Daniel Juhyung Joe: Conceptualization, Writing - Review & Editing, Supervision, Project administration, Funding acquisition.
Joon Young Kwak: Conceptualization, Writing - Review & Editing, Supervision, Project administration, Funding acquisition.

Data Availability

Data sharing not applicable – no new data generated

References

[1] G. Cao, P. Meng, J. Chen, H. Liu, R. Bian, C. Zhu, F. Liu, and Z. Liu, *Adv. Funct. Mater*., **31**, 2005443 (2021). doi: https://doi.org/10.1002/adfm.202005443
[2] A. Mehonic and A. J. Kenyon, *Nature*, **604**, 255 (2022). doi: https://doi.org/10.1038/s41586-021-04362-w
[3] H. Xiang, Y. C. Chien, Y. Shi, and K. W. Ang, *Small Struct*., **3**, 2200060 (2022). doi: https://doi.org/10.1002/sstr.202200060
[4] A. Wali and S. Das, *Adv. Mater*., **35** 2205365 (2023). doi: https://doi.org/10.1002/adma.202205365
[5] A. Wali, H. Ravichandran, and S. Das, *Adv. Mater*., **36**, 2400661 (2024). doi: https://doi.org/10.1002/adma.202400661
[6] C. Ezekannagha, A. Becker, D. Heider, and G. Hattab, *Mater. Today Bio*, **15**, 100306 (2022). doi: https://doi.org/10.1016/j.mtbio.2022.100306
[7] A. Doricchi, C. M. Platnich, A. Gimpel, F. Horn, M. Earle, G. Lanzavecchia, A. L. Cortajarena, L. M. Liz-Marzán, N. Liu, R. Heckel, R. N. Grass, R. Krahne, U. F. Keyser, and D. Garoli, *ACS Nano*, **16**, 17552 (2022). doi: https://doi.org/10.1021/acsnano.2c06748
[8] Y. Qin, Z. Wang, Y. Yang, L. Shan, Q. Wang, L. Bao, J. Robertson, Y. Cai, and R. Huang, *IEEE Electron Device Lett*., **44**, 1967 (2023). doi: https://doi.org/10.1109/LED.2023.3322992
[9] M. S. Equbal, T. Ketkar, and S. Sahay, *IEEE Trans. Electron Devices*, **70**, 1061 (2023). doi: https://doi.org/10.1109/TED.2023.3241122
[10] K. S. Woo, A. Zhang, A. Arabelo, T. D. Brown, M. Park, A. A. Talin, E. J. Fuller, R. S. Bisht, X. Qian, R. Arroyave, S. Ramanathan, L. Thomas, R. S. Williams, and S. Kumar, *Nat. Commun*., **15**, 4656 (2024). doi: https://doi.org/10.1038/s41467-024-49149-5
[11] S. Zhu, Y. Ma, T. Chen, J. Lin, and J. Jing, *IACR Trans. Symmetric Cryptol*., **2017**, 151 (2017). doi: https://doi.org/10.46586/tosc.v2017.i3.151-168
[12] K. S. Woo, Y. Wang, Y. Kim, J. Kim, W. Kim, and C. S. Hwang, *Adv. Electron. Mater*., **6**, 1901117 (2020). doi: https://doi.org/10.1002/aelm.201901117
[13] H. Jiang, D. Belkin, S. E. Savel'ev, S. Lin, Z. Wang, Y. Li, S. Joshi, R. Midya, C. Li, M. Rao, M. Barnell, Q. Wu, J. J. Yang, and Q. Xia, *Nat. Commun*., **8**, 882 (2017). doi: https://doi.org/10.1038/s41467-017-00869-x
[14] G. Kim, J. H. In, Y. S. Kim, H. Rhee, W. Park, H. Song, J. Park, and K. M. Kim, *Nat. Commun*., **12**, 2906 (2021). doi: https://doi.org/10.1038/s41467-021-23184-y
[15] M. S. Song, T. H. Kim, H. Hwang, S. Ahn, H. Nili, and H. Kim, *Adv. Intell. Syst*., **5**, 2200358 (2023). doi: https://doi.org/10.1002/aisy.202200358
[16] S. I. Kim, H. J. You, M. S. Kim, U. S. An, M. S. Kim, D. H. Lee, S. T. Ryu, and Y. K. Choi, *Sci. Adv.*, **10**, eadk6042 (2024). doi: https://doi.org/10.1126/sciadv.adk6042
[17] Y. Pang, B. Gao, B. Lin, H. Qian, and H. Wu, *Adv. Electron. Mater*., **5**, 1800872 (2019). doi: https://doi.org/10.1002/aelm.201800872
[18] S. Misra, L. C. Bland, S. G. Cardwell, J. A. C. Incorvia, C. D. James, A. D. Kent, C. D. Schuman, J. D. Smith, and J. B.

Aimone, *Adv. Mater*., **35**, 2204569 (2023).
doi: https://doi.org/10.1002/adma.202204569
[19] W. Choi, O. Kwon, J. Lee, S. Oh, S. Heo, S. Ban, Y. Seo, D. Kim, and H. Hwang, *Appl. Phys. Rev*., **11**, 021323 (2024).
doi: https://doi.org/10.1063/5.0183292
[20] B. Liu, Y. F. Chang, J. Li, X. Liu, L. A. Wang, D. Verma, H. Liang, H. Zhu, Y. Zhao, L. J. Li, T. H. Hou, and C. S. Lai, *ACS Nano*, **16**, 6847 (2022).
doi: https://doi.org/10.1021/acsnano.2c01784
[21] C. Wen, X. Li, T. Zanotti, F. M. Puglisi, Y. Shi, F. Saiz, A. Antidormi, S. Roche, W. Zheng, X. Liang, J. Hu, S. Duhm, J. B. Roldan, T. Wu, V. Chen, E. Pop, B. Garrido, K. Zhu, F. Hui, and M. Lanza, *Adv. Mater*., **33**, 2100185 (2021).
doi: https://doi.org/10.1002/adma.202100185
[22] A. Wali, H. Ravichandran, and S. Das, *ACS Nano*, **15**, 17804 (2021).
doi: https://doi.org/10.1021/acsnano.1c05984
[23] N. Abraham, K. Watanabe, T. Taniguchi, and K. Majumdar, *ACS Nano*, **16**, 5898 (2022).
doi: https://doi.org/10.1021/acsnano.1c11084
[24] J. Jeon, Y. Shin, H. Heo, J. Son, S. Ryu, K. Cho, and S. Kim, *Sci. China Inf. Sci*., **68**, 162401 (2025).
doi: https://doi.org/10.1007/s11432-024-4317-6
[25] Y. F. Lu, H. Y. Li, Y. Li, L. H. Li, T. Q. Wan, L. Yang, W. B. Zuo, K. H. Xue, and X. S. Miao, *Adv. Electron. Mater*., **8**, 2200202 (2022).
doi: https://doi.org/10.1002/aelm.202200202
[26] J. Bian, Y. Tao, Z. Wang, Y. Dong, Z. Li, X. Zhao, Y. Lin, H. Xu, and Y. Liu, *Appl. Phys. Lett*., **122**, 193502 (2023).
doi: https://doi.org/10.1063/5.0145875
[27] J. Brown, J. F. Zhang, B. Zhou, M. Mehedi, P. Freitas, J. Marsland, and Z. Ji, *Sci. Rep*., **10**, 17210 (2020).
doi: https://doi.org/10.1038/s41598-020-74351-y
[28] X. Li, T. Zanotti, T. Wang, K. Zhu, F. M. Puglisi, and M. Lanza, *Adv. Funct. Mater*., **31**, 2102172 (2021).
doi: https://doi.org/10.1002/adfm.202102172
[29] D. Yu, S. Ahn, S. Youn, J. Park, and H. Kim, *Chaos Solitons Fractals*, **189**, 115708 (2024).
doi: https://doi.org/10.1016/j.chaos.2024.115708
[30] Y. C. Chien, H. Xiang, J. Wang, Y. Shi, X. Fong, and K. W. Ang, *Small*, **19**, 2302842 (2023).
doi: https://doi.org/10.1002/smll.202302842
[31] H. Ravichandran, D. Sen, A. Wali, T. F. Schranghamer, N. Trainor, J. M. Redwing, B. Ray, and S. Das, *ACS Nano*, **17**, 16817 (2023).
doi: https://doi.org/10.1021/acsnano.3c03581
[32] Y. Han, R. H. Koo, J. Song, C. H. Kim, E. K. Lee, W. Shin, and H. Yoo, *Adv. Mater*., **37**, 2505150 (2025).
doi: https://doi.org/10.1002/adma.202505150
[33] K. S. Woo, J. Kim, J. Han, J. M. Choi, W. Kim, and C. S. Hwang, *Adv. Intell. Syst*., **3**, 2100062 (2021).
doi: https://doi.org/10.1002/aisy.202100062
[34] Y. Fu, J. Wen, L. Wang, L. Yang, Q. Zhu, W. Zuo, P. Zhang, Y. Li, H. Tong, G. Ma, H. Wang, and X. Miao, *IEEE Electron. Dev. Lett*., **44**, 853 (2023).
doi: https://doi.org/10.1109/LED.2023.3259000
[35] G. Kim, J. H. In, H. Rhee, W. Park, H. Song, and K. M. Kim, *npj Unconv. Comput*., **2**, 12 (2025).
doi: https://doi.org/10.1038/s44335-025-00027-3
[36] X. Xing, S. Huang, Y. Gong, J. Wang, Z. Lv, Y. Zhou, X. Zhao, J. Hao, and S. T. Han, *Mater. Today Nano*, **22**, 100315 (2023).
doi: https://doi.org/10.1016/j.mtnano.2023.100315
[37] Y. Jo, G. Noh, E. Park, D. K. Lee, H. Wi, and J. Y. Kwak, *Adv. Funct. Mater*., **36** 2522597 (2026).
doi: https://doi.org/10.1002/adfm.202522597
[38] S. Pazos, W. Zheng, T. Zanotti, F. Aguirre, T. Becker, Y. Shen, K. Zhu, Y. Yuan, G. Wirth, F. M. Puglisi, J. B. Roldán, F. Palumbo, and M. Lanza, *Nanoscale*, **15**, 2171 (2023).
doi: https://doi.org/10.1039/d2nr06222d
[39] S. Rehman, M. S. Kim, M. F. Khan, and S. Kim, *Nano Energy*, **127**, 109764 (2024).
doi: https://doi.org/10.1016/j.nanoen.2024.109764
[40] Y. Liu, P. Liu, Y. Wen, Z. Liang, S. Liu, L. Song, J. Pei, X. Fan, T. Ma, G. Wang, S. Gao, K. P. Pun, X. Chen, and G. Hu, *Nano Lett*., **24**, 14315 (2024).
doi: https://doi.org/10.1021/acs.nanolett.4c03957
[41] D. Ahn, M. Lee, W. Kim, Y. K. Lee, J. Y. Lee, G. Y. Jung, H. Choi, Y. Yoon, H. S. Song, H. Lee, M. Seo, J. Min, and Y. Pak, *Adv. Sci*., **12**, 2412139 (2025).
doi: https://doi.org/10.1002/advs.202412139
[42] T. Park, J. Seo, N. Kim, C. Kim, Y. J. Kim, H. Kim, H. H. Kim, S. Oh, D. C. Kim, D. Son, J. Hur, Y. J. Kim, B. C. Jang, and H. Yoo, *Adv. Mater*., **37**, 2419579 (2025).
doi: https://doi.org/10.1002/adma.202419579
[43] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo, *Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, NIST Special Publication 800-22 Rev. 1a (National Institute of Standards and Technology, Gaithersburg, MD, 2010).
doi: https://doi.org/10.6028/NIST.SP.800-22r1a
[44] M. S. Turan, E. Barker, J. Kelsey, K. A. McKay, M. L. Baish, and M. Boyle, *Recommendation for the Entropy Sources Used for Random Bit Generation*, NIST Special Publication 800-90B (National Institute of Standards and Technology, Gaithersburg, MD, 2018).
doi: https://doi.org/10.6028/NIST.SP.800-90B
[45] M. Aslan, A. Doğanaksoy, Z. Saygı, M. Sönmez Turan, and F. Sulak, *Cryptography Commun*., **18**, 63 (2026).
doi: https://doi.org/10.1007/s12095-025-00778-7
[46] M. Peter and W. Schindler, *A Proposal for Functionality*

Classes for Random Number Generators, Version 3.0 (Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, Germany, 2024).

[47] K. Zhu, G. Vescio, S. González-Torres, J. López-Vidrier, J. L. Frieiro, S. Pazos, X. Jing, X. Gao, S. D. Wang, J. Ascorbe-Muruzábal, J. A. Ruiz-Fuentes, A. Cirera, B. Garrido, and M. Lanza, *Nanoscale*, **15**, 9985 (2023).
doi: https://doi.org/10.1039/D3NR00030C

[48] L. Liao, E. Kovalska, J. Regner, Q. Song, and Z. Sofer, *Small*, **20**, 2303638 (2024).
doi: https://doi.org/10.1002/smll.202303638

[49] K. Gołofit, P. Z. Wieczorek, and M. Pilarz, *AEU - Int. J. Electron. Commun*., **170**, 154835 (2023).
doi: https://doi.org/10.1016/j.aeue.2023.154835

[50] X. Wang, H. Wang, D. Yang, Y. Lin, R. Bie, R. Xu, and L. Sun, *Nano Energy*, **142**, 111225 (2025).
doi: https://doi.org/10.1016/j.nanoen.2025.111225

[51] H. Yu and Y. Kim, *Proc. 2018 International SoC Design Conference (ISOCC)* (IEEE, Daegu, Korea, 2018), pp. 231.
doi: https://doi.org/10.1109/ISOCC.2018.8649804

[52] C. Camara, H. Martín, P. Peris-Lopez, and M. Aldalaien, *Sensors*, **19**, 2033 (2019).
doi: https://doi.org/10.3390/s19092033

[53] M. Švarcmajer, M. Köhler, Z. Krpić, and I. Lukić, *Sensors*, **25**, 5298 (2025).
doi: https://doi.org/10.3390/s25175298

[54] C. Shepherd and E. A. J. Hurley, *J. Inf. Security Appl*., **95**, 104272 (2025).
doi: https://doi.org/10.1016/j.jisa.2025.104272