Advanced Electronic Materials

ADVANCED ELECTRONIC MATERIALS Open Access

www.advelectronicmat.de

RESEARCH ARTICLE OPEN ACCESS

RRAM Variability Harvesting for CIM-Integrated TRNG

Ankit Bende[1] | Gokulnath Rajendran[2] | Regina Dittmann[1] | Anupam Chattopadhyay[2] | Vikas Rana[1]

[1]Peter Grünberg Institute – 7 & 10, Forschungszentrum Jülich GmbH, Jülich, Germany | [2]College of Computing and Data Science, Nanyang Technological University, Singapore

Correspondence: Ankit Bende (a.bende@fz-juelich.de)

Received: 12 September 2025 | **Revised:** 1 December 2025 | **Accepted:** 22 December 2025

Keywords: CiM | entropy source | hardware security | RRAM | TRNG

ABSTRACT

True random number generators (TRNGs) are essential for hardware security in edge AI systems, yet conventional designs often incur large analog overhead and limited throughput imposed by standalone macros. We present a Compute-in-Memory (CiM)-compatible TRNG that directly exploits the intrinsic stochasticity of TaO_x-based 1T1R RRAM arrays, enabling entropy extraction within the memory fabric. Bit-rate is scaled by parallel column readout circuits consisting of a transimpedance amplifier (TIA) and an ADC. Our design achieves up to ∼270 Mbps throughput with TIA + 16-bit ADC per column. Furthermore, a lightweight shift-XOR post-processing stage permits reduction to 8-bit ADC resolution, lowering energy consumption to ∼51 pJ bit^{-1} without degrading randomness quality. Fully compatible with standard CiM read paths, the architecture introduces minimal hardware overhead and provides a scalable and energy-efficient foundation for secure random number generation in edge-AI applications.

1 | Introduction

Compute-in-Memory (CIM) has emerged as a promising architectural approach to overcome the von Neumann bottleneck by enabling computations directly within memory units [1]. This paradigm significantly reduces data movement and improves energy efficiency, making it well-suited for edge artificial intelligence (AI) applications. As CIM architectures gain traction in different applications, they bring unique security challenges. Unlike traditional processors, the CIM chips perform computation directly inside memory arrays, making sensitive data such as model parameters, cryptographic keys, and intermediate computations more vulnerable to extraction or tampering. Conventional security mechanisms at the system or software level are often insufficient, as attackers with sufficient computational power or through physical side-channel leakages can bypass these defenses and extract the sensitive data [2]. This underscores the need for the CIM systems to incorporate hardware-level security primitives. Such primitives draw entropy from stochastic physical processes that are inherently difficult to model, enabling functions such as True Random Number Generators (TRNGs) and Physically Unclonable Functions (PUFs). These primitives act as unique hardware fingerprints that can be used to authenticate devices, generate cryptographic keys, and encrypt data directly on-chip, ensuring that sensitive computations and stored information remain secure even under invasive probing. Consequently, the design of robust hardware entropy sources is fundamental to establishing strong hardware-based security.

Resistive RAM (RRAM) is a leading candidate for the CIM architecture due to its ability to support both in-situ computation and non-volatile data storage [3–5]. Beyond its in-memory computational advantages, RRAM also presents promising opportunities for hardware security. Its intrinsic device-to-device (D2D) and cycle-to-cycle (C2C) variations can be harnessed as natural entropy sources for the TRNGs [2, 6–10]. By enabling in-situ storage, computation, and encryption, RRAM-based TRNG systems provide a secure, robust, tamper-resistant, and low-overhead solution for next-generation edge AI applications.

Existing RRAM-based TRNG implementations are designed as standalone security blocks and rely on entropy extraction circuits such as multi-stage ring oscillators, comparators, or high-speed counters [11–17]. While effective, these approaches increase area, power, and design complexity, undermining the dense, low-overhead philosophy of the CiM arrays. Some recent studies have explored CiM-compatible TRNGs, they often require high-resolution ADCs, up to 16 bits or suffer from low throughput (< 25 Mbps), which are impractical for energy-constrained platforms [18–21]. This highlights the need for entropy sources that can operate effectively with low-resolution ADCs and minimal hardware overhead. Moreover, most existing designs generate random bits using a single device at a time, resulting in limited throughput due to the inherently low entropy generation rate. This creates a significant bottleneck for applications demanding high-speed and continuous randomness. Although combining multiple entropy sources in parallel could potentially enhance throughput, D2D variations introduced during fabrication have traditionally made such integration challenging, often degrading the statistical quality of the output. In this work, we propose a CiM-compatible, high-throughput TRNG architecture that overcomes these limitations by leveraging multiple entropy sources in parallel, while maintaining statistical robustness and energy efficiency of the system. Our design is tolerant to the D2D variability and addresses the throughput bottleneck without compromising compatibility with low-resolution ADCs and compact CiM readout circuits.

In the study, we demonstrate two intrinsic entropy sources in a typical RRAM-based CiM read path: (1) C2C resistance variability and (2) READ noise. Both sources are accessed through the CiM-compatible read circuit comprising a transimpedance amplifier and an ADC. The effectiveness of the proposed entropy sources for TRNG applications is first rigorously assessed through comprehensive statistical evaluations employing the NIST SP800-22 and SP800-90B tests. Subsequently, the minimum ADC resolution required to maintain high-entropy output is investigated. Experimental findings demonstrate that the C2C-based source attains high entropy at a reduced 10-bit ADC resolution, attributable to its intrinsically elevated variability. In contrast, the READ noise-based source, characterized by smaller fluctuations, requires a higher 12-bit ADC resolution to attain similar entropy levels. Although the READ noise-based source avoids energy-intensive switching operations in every cycle, its reliance on the high-resolution ADC offsets the energy savings, resulting in comparable overall energy consumption to the C2C-based source. Furthermore, by incorporating a simple XOR-based bit-mixing step, the required ADC resolution for the C2C-based source can further be reduced to 8 bits, offering additional benefits in terms of circuit complexity and area efficiency. The C2C-based TRNG also demonstrates temperature, spatial, and temporal robustness without compromising the statistical properties required for high-speed TRNG applications.

2 | Results and Discussion

2.1 | TRNG Architecture

To realize the CiM-compatible TRNG architecture, we fabricated and integrated a TaO_x-based 1T1R RRAM crossbar array with 180 nm CMOS technology. The optical image of the die containing the 31×16 1T1R array is shown in Figure 1a. The schematic layout of the proposed TRNG architecture, including the 1T1R array and column-wise readout circuitry, is presented in Figure 1b, where column-wise readout enables parallel TRNG operation. The read circuit comprises a transimpedance amplifier (TIA) for current amplification and current-to-voltage conversion, followed by an n-bit ADC for entropy digitization [19], as shown in Figure 1c. The 1T1R cell, depicted in Figure 1d, consists of an NMOS transistor with a width and length of 10 µm × 10 µm. The RRAM device consists of Pt/Ta/TaO_x/Pt stack and has lateral dimensions of 200 nm × 200 nm, as illustrated in the layer stack (Figure 1e) and the SEM image in Figure 1f. The DC *I-V* characteristics of the RRAM device with 100 consecutive switching cycles are shown in Figure 1g, demonstrating stable bipolar switching behavior with clearly distinguishable high-resistance state (HRS) and low-resistance state (LRS), confirming suitability for entropy extraction based on resistance variability.

For the TRNG implementation, we captured the randomness through two different entropy sources in the 1T1R RRAM devices: C2C resistance variability and READ noise-induced variability in the read current. To systematically evaluate their entropy generation capability, we used the readout circuit as depicted in Figure 1c to digitize the analog read current and analyzed the resulting bitstreams for statistical quality. The read current was experimentally measured using an FPGA based memory characterisation tool, ARC2 measurement board. The subsequent TIA and ADC quantization were emulated in Python for flexible resolution analysis. The output of the TIA can be obtained using Kirchhoff's law and is given by the following equation:

$$V_{\text{out}} = R_2 I_{\text{READ}} + \left(\frac{R_2}{R_1}\right)(V_{\text{READ}} - V_1) + V_{\text{READ}} \tag{1}$$

where R_1 and R_2 are the feedback resistors, in this work, they are chosen to be 10~$k\Omega$ and 30~$k\Omega$ respectively with $V_{\text{READ}} = 0.3\,\text{V}$ and $V_1 = 0.2\,\text{V}$. The output voltage is then digitized using a 16-bit analog-to-digital converter (ADC) with reference voltage $V_{\text{ref}} = 3.3\,\text{V}$. The 16-bit ADC output D is computed as:

$$\text{D} = \left\lfloor \frac{V_{\text{out}}}{V_{\text{ref}}} \times (2^n - 1) \right\rfloor \tag{2}$$

where $n = 16$ is the ADC resolution. The least significant bits (LSBs) of the ADC output reflect the variability in READ current and are extracted as random bits.

For evaluating the quality of randomness, we applied both NIST SP800-22 and SP800-90B test suites. The NIST SP800-22 test suite evaluates the statistical properties of binary sequences to ensure uniformity and independence, while NIST SP800-90B focuses on assessing the entropy content and the quality of entropy sources used in random number generation systems [22, 23]. Together, these tests provide comprehensive validation of TRNG output quality. We then investigated the impact of ADC resolution by progressively lowering the number of bits and identifying the minimum resolution that still maintains acceptable randomness quality. To further reduce the ADC requirements, we developed and implemented a lightweight post-processing technique that

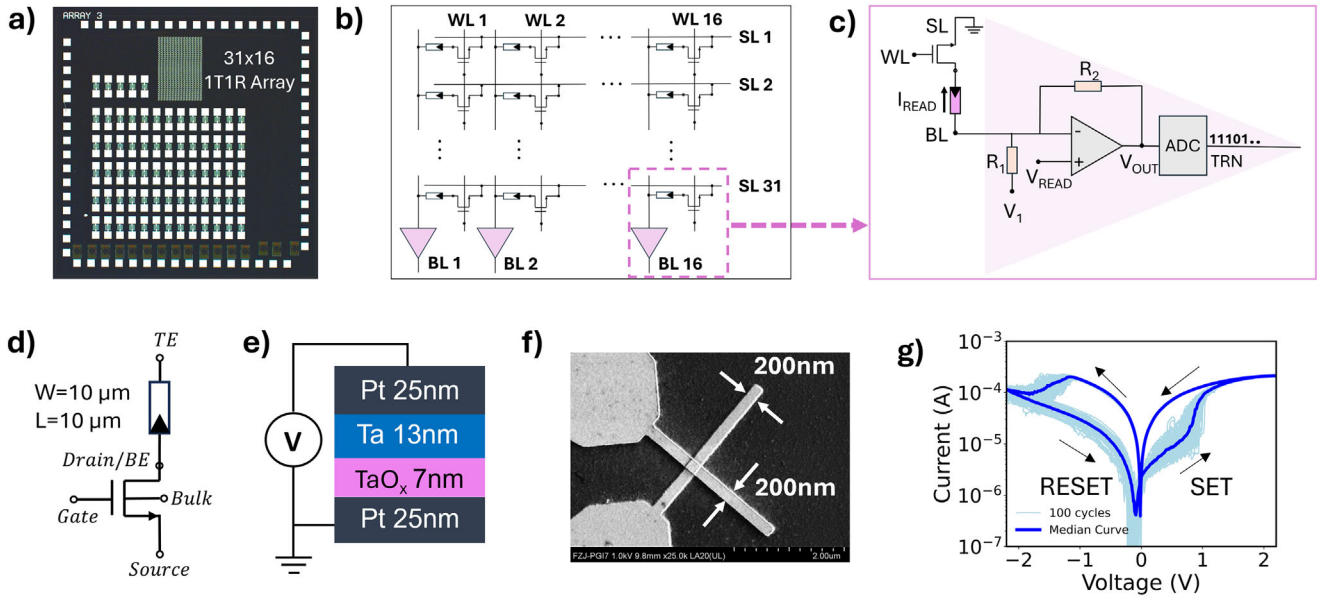

FIGURE 1 | TaO_x-based 1T1R RRAM array for Compute-in-Memory (CiM) compatible TRNG. (a) Die picture of the fabricated chip integrating a 31×16 1T1R RRAM array. (b) Schematic layout of the 1T1R array with column-wise readout circuitry. (c) Block diagram of the read circuit comprising a transimpedance amplifier and an analog-to-digital converter (ADC) used for TRNG operation. (d) Schematic of the 1T1R unit cell architecture. (e) Layer stack of the TaO_x-based RRAM device. (f) SEM image of a fabricated 1T1R cell. (g) DC I–V characteristics over 100 switching cycles.

compensates for entropy loss at lower resolutions. We first discuss the C2C variability as a TRNG entropy source in the next section.

2.2 | LRS C2C based Entropy Source

The C2C variability in LRS arises from the stochastic nature of conductive filament formation during the SET operation, which is governed by the valence change mechanism (VCM)[24–26]. Each SET event involves the migration and accumulation of oxygen vacancies that lead to the formation of one or more conductive filaments bridging the top and bottom electrodes. Due to the randomness in the nucleation site, growth direction, local defect density, and filament morphology, the resulting LRS resistance varies significantly from C2C, even under fixed programming conditions [27–30]. To harness the inherent randomness in the C2C resistance variations, we implement a repetitive sequence of parallel programming and serial readout operations across the 1T1R crossbar array. The randomness was extracted by combining multiple entropy sources, i.e., multiple 1T1R cells in the array, to generate long (>1~Mbit) random sequences. To ensure reliable operation, a 28×9 functional subarray was selected from the original 31×16 array by discarding rows and columns exhibiting stuck-at-"0" or stuck-at-"1" faults. Combining multiple entropy sources increases the overall throughput of the TRNG while reducing endurance stress on individual devices.

The algorithm for generating random bits is illustrated in Figure 2a. Initially, a parallel SET operation is performed on all devices in the array. During this step, all word lines (WLs) are biased at $V_{G,\,SET} = 2$ V, source lines (SLs) are grounded, and a SET voltage of $V_{SET} = 2.5$ V with a pulse width of 1 µs is applied to all bit lines (BLs). This biasing scheme ensures that all 252 devices in the array receive the programming voltage simultaneously, enabling parallel yet inherently stochastic switching due to device-level variability. Compared to serial programming, which would require $252 \times t_{SET}$ to program the array, the parallel SET step generates 252 LRS states within a single pulse interval, improving the entropy-generation rate by a factor of 252 and directly increasing throughput. Parallel programming also yields larger D2D variation in the resulting LRS states, as evident in Figure 2b, in contrast to the more uniform distribution observed after serial programming [Figure 2f]. We attribute this enhanced D2D variability to (i) the limited supply current being shared among all devices during parallel programming and (ii) small variations in the effective SET time across devices. Although a small fraction of cells may remain in the HRS due to intrinsic variability, these devices do not degrade the statistical quality of the generated random bits.

After programming, each device is read sequentially by applying $V_{READ} = 0.3$ V to the selected BL, $V_{G,\,READ} = 3.3$ V to the selected WL, and $V_{SL} = 0$ V to the selected SL. Figure 2b shows the read current distribution across the 28×9 array following a parallel SET. The spatial map clearly demonstrates the stochastic nature of the LRS states. Subsequently, a parallel RESET is performed using $V_{WL} = V_{G,\,RESET} = 3.3$ V, $V_{SL} = V_{RESET} = 2$ V, and $V_{BL} = 0$ V. This cycle of parallel SET, serial READ, and parallel RESET is repeated over multiple iterations to capture the full C2C variability in read current. The detailed parallel SET/RESET and serial READ methodology is described in Section 3.2

Figure 2c presents the distribution of the LRS states obtained from 252 devices over 5000 switching cycles. The broad spread in the SET-state resistances confirms the presence of substantial entropy suitable for TRNG. A representative 1-million-bit output is visualized in Figure 2d as a binary map, demonstrating the absence of spatial or temporal correlations. The random bits generated through C2C variations, using the readout circuit

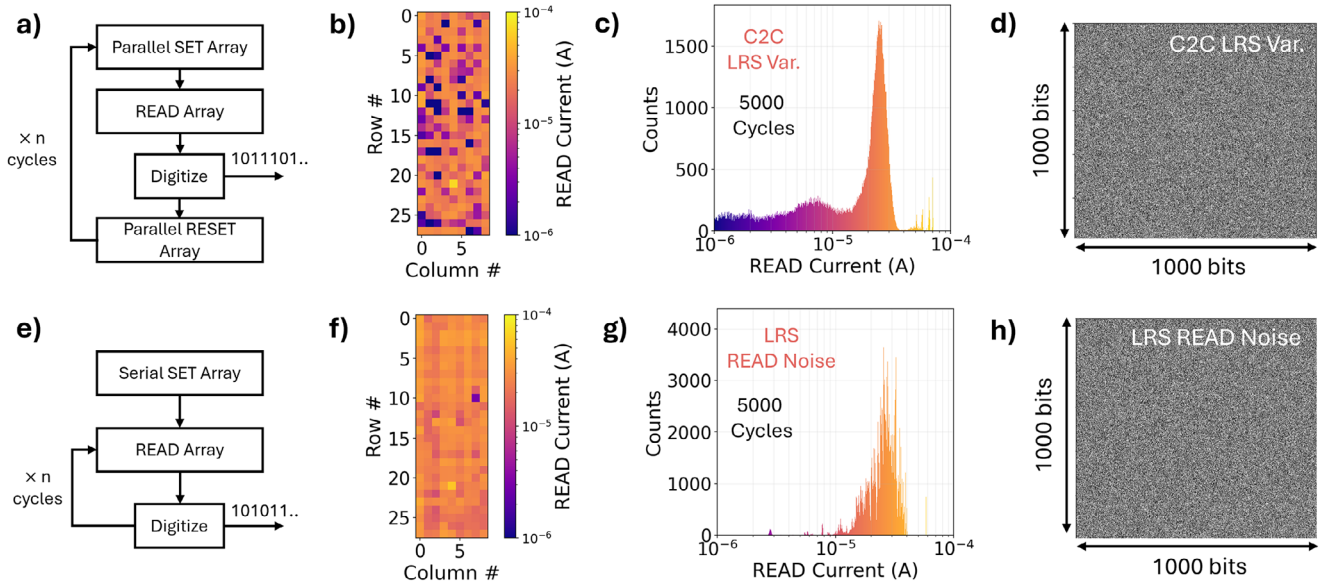

FIGURE 2 | Entropy sources for True Random Number Generation (TRNG). (a) Flowchart illustrating the TRNG methodology based on the C2C switching variations in read current. (b) Read current variation across devices in a 28×9 1T1R array following a parallel SET operation; this process is repeated over 5000 cycles to generate a random bitstream. (c) Histogram of C2C read current fluctuations after parallel SET operations. (d) Bit map of a 1-million-bit TRNG output generated by exploiting C2C variability. (e) Flowchart of the TRNG approach utilizing intrinsic READ noise. (f) Read current variation in the low resistance state (LRS) across the array. (g) Distribution of READ noise measured from 252 LRS devices over 5000 repeated read cycles. (h) Bit map of a 1-million-bit TRNG output generated by exploiting READ noise.

consisting of a 16-bit ADC and three least significant bits (LSBs) extracted per sample, were evaluated using the NIST SP800-22 and SP800-90B test suites. The results are summarized in Table 1 and Table 2. The bitstream passed all the tests in both suites, achieving a high estimated min-entropy of 0.996. These findings confirm that SET-state C2C variability serves as a robust and reliable entropy source for secure, CiM-compatible TRNG architectures.

2.3 | LRS READ Noise-Based Entropy Source

In TaO_x-based RRAM, stochastic fluctuations during READ operations arise from instabilities in the conductive filament (CF) and the trapping/de-trapping of carriers at oxygen vacancy sites [31–34]. Low-frequency-noise spectroscopy (LFNS) and random telegraph noise (RTN) studies have revealed a broad distribution of trap activation energies inside and around the CF [31]. Under READ bias, modulation of trap occupancy induces transient conductance changes and gradual resistance drift, which provide a source of entropy for TRNG applications. To extract this READ noise stochasticity, the 1T1R array was first deterministically and serially programmed (one device at a time) into the LRS using a high SET pulse of $V_{SET} = 2.5$ V. Subsequently, repeated READ operations were performed by serially accessing each device under the bias conditions $V_{READ} = 0.3$ V (BL), $V_{WL} = 3.3$ V (WL), and $V_{SL} = 0$ V (SL). As highlighted in detail in the Section 3.2, the READ biasing and readout circuitry are identical to those used in the C2C-based TRNG. In the READ-noise TRNG, a single LRS initialization is followed by repeated reads, whereas the C2C TRNG relies on a new SET/RESET cycle for each entropy sample. The overall READ-noise based random number generation procedure is illustrated in Figure 2e, and the current distribution following serial SET is shown in Figure 2f. Figure 2g presents the current fluctuations recorded over 5000 READ cycles. Compared to the C2C variability, the READ noise distribution exhibits a narrower spread with sharper peaks, reflecting smaller differences between consecutive cycles. A representative 1-million-bit sequence generated from this source is visualized as a bit map in Figure 2h, showing no spatial or temporal correlations. The statistical quality of the generated sequences was evaluated using the NIST SP800-22 and SP800-90B test suites (Tables 1 and 2). Using a 16-bit ADC and extracting two least significant bits (LSBs) per sample, the bitstreams passed all tests, with a measured minimum entropy of 0.995. These results confirm that READ noise can serve as a promising entropy source for CiM-compatible TRNGs. Although this approach avoids repeated SET/RESET cycling and therefore reduces endurance stress, its lower intrinsic variability requires higher ADC resolution to preserve randomness, as discussed in the following section.

2.4 | ADC Requirements for C2C- and READ Noise-Based TRNGs

As demonstrated in the previous sections, TaO_x-based 1T1R RRAM arrays can provide entropy through both C2C variability and READ noise mechanisms, using a readout circuit comprising a TIA and a 16-bit ADC. While parallel column readout can increase throughput, integrating multiple high-resolution ADCs is impractical for large-scale deployment due to their area overhead, circuit complexity, and high energy consumption. Moreover, the least significant bit (LSB) step size of the16-bit ADC lies in the μV range, as summarized in Table 3, making it impractical for large-scale, energy-efficient TRNG deployment.

TABLE 1 | NIST SP800-22 test results for TRNGs based on the C2C variability and READ noise with 16-bit ADC in the readout circuit.

S/No.	Test	C2C Variability		READ Noise	
		p-value	Result	p-value	Result
1	Approx. Entropy	0.418	PASS	0.053	PASS
2	Block Frequency	0.531	PASS	0.107	PASS
3	Cumulative Sum-1	0.298	PASS	0.611	PASS
	Cumulative Sum-2	0.207	PASS	0.703	PASS
4	FFT	0.304	PASS	0.737	PASS
5	Frequency	0.854	PASS	0.921	PASS
6	Linear Complexity	0.771	PASS	0.941	PASS
7	Long Runs	0.754	PASS	0.496	PASS
8	Non-overlapping	0.027	PASS	0.012	PASS
9	Overlapping	0.368	PASS	0.234	PASS
10	Random Excursions	0.014	PASS	0.020	PASS
11	Random Excursions Variant	0.138	PASS	0.094	PASS
12	Rank	0.284	PASS	0.556	PASS
13	Runs	0.643	PASS	0.239	PASS
14	Serial 1	0.017	PASS	0.690	PASS
	Serial 2	0.092	PASS	0.803	PASS
15	Universal	0.095	PASS	0.951	PASS

TABLE 2 | NIST SP800-90B test results for TRNGs based on the C2C variability and READ noise with 16-bit ADC in the readout circuit.

S/No.	Test	C2C Variability	READ Noise
1	IID Permutation	PASS	PASS
2	Chi-square Independence	PASS, Score = 2084, dof = 2046, p-value = 0.27	PASS, Score = 2056, dof = 2046, p-value = 0.43
3	Chi-square Goodness-of-fit	PASS, Score = 14.3, dof = 9, p-value = 0.11	PASS, Score = 12.8, dof = 9, p-value = 0.17
4	LRS Test	PASS, Pr(X $\geqslant$ 1): 0.973	PASS, Pr(X $\geqslant$ 1): 0.59
	Min-entropy	0.996	0.995

TABLE 3 | LSB voltage for different ADC resolutions at V_{ref} = 3.3 V.

V_{ref} (V)	ADC Resolution (bits)	LSB Voltage
3.3	16	50.35 μV
	14	201.42 μV
	12	805.86 μV
	10	3.22 mV
	8	12.89 mV
	4	206.25 mV

To determine the minimum ADC resolution required for practical operations, we digitally emulated the quantization of measured READ currents at different ADC resolutions and evaluated the resulting random bitstreams using the NIST test suites. This analysis yields the critical resolution thresholds at which acceptable entropy quality can still be achieved, enabling reduction of both circuit complexity and energy consumption. Figure 3a,b summarize the resolution-dependent NIST SP800-22 and SP800-90B test results for the C2C-based TRNG. The C2C approach maintains full compliance with all SP800-90B tests down to 10-bit resolution for both 1- and 2-LSB slices, indicating preserved entropy quality. In contrast, SP800-22 results at 10-bit resolution show 11/15 tests passing, suggesting some residual repetitive patterns. As noted in the NIST guidelines, SP800-22 only tests statistical randomness, whereas SP800-90B explicitly estimates entropy and is the authoritative reference for cryptographic validation [23, 35, 36]. Therefore, SP800-90B is given higher weight in this analysis.

For the READ noise-based TRNG, the entropy quality is preserved down to 12-bit resolution, where all SP800-90B tests are passed and 12/15 SP800-22 tests are passed. This is consistent with the narrower READ current distribution,

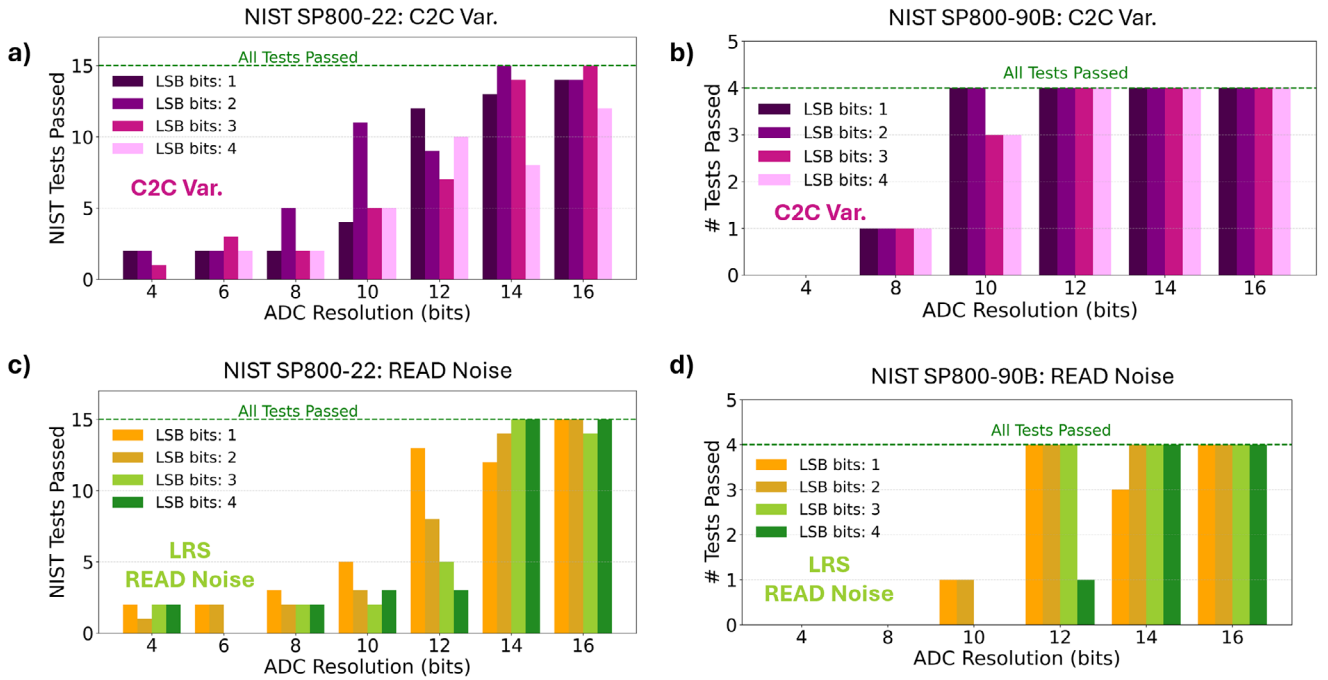

FIGURE 3 | ADC resolution requirement for TRNG randomness. ADC resolution dependence of NIST SP800-22 results for (a) C2C variability-based TRNG and (c) READ noise-based TRNG. ADC resolution dependence of NIST SP800-90B results for (b) C2C variability-based TRNG and (d) READ noise-based TRNG. The C2C read-based TRNG passes all tests at 12-bit and 10-bit ADC resolution for NIST SP800-22 and NIST SP800-90B, respectively. In contrast, the READ noise-based TRNG requires 14-bit and 12-bit ADC resolution to pass the NIST SP800-22 and NIST SP800-90B tests, respectively.

characterized by sharp peaks and smaller fluctuations between cycles, which require finer ADC granularity to resolve. In contrast, the broader current distribution in the C2C case allows sufficient variability to be captured even with lower-resolution ADCs. In summary, the minimum ADC resolution requirements are 10 bits for the C2C-based TRNG and 12 bits for the READ noise-based TRNG. While both represent a significant improvement over the baseline 16-bit ADC requirement, they still impose notable design and energy costs. To further reduce ADC resolution requirements without compromising entropy quality, a lightweight post-processing scheme based on bit shifting and XOR operations is introduced in the next section.

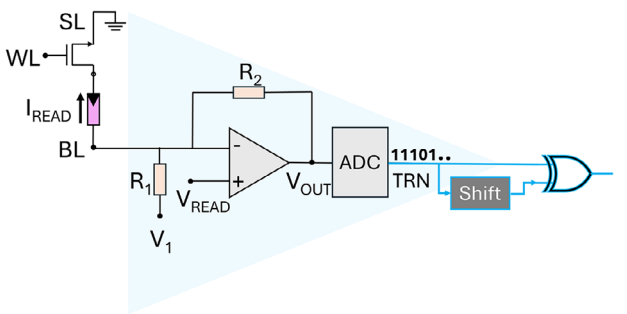

FIGURE 4 | READ circuit with shift and XOR technique to lower the ADC resolution requirement for the TRNG.

2.5 | Shift and XOR Post-Processing for Energy- and Complexity-Aware Design

To further reduce the ADC resolution requirement, we have implemented a lightweight shift and XOR post-processing scheme as shown in Figure 4. The principle of this approach is to decorrelate and uniformly redistribute the raw bit patterns by combining delayed versions of the same bitstream. Specifically, the raw sequence S is circularly shifted by a predetermined offset k bits to produce a shifted sequence S', and then XORed with the original:

$$S_{\text{out}} = S \oplus \text{Shift}(S, k) \tag{3}$$

where $\oplus$ denotes the bitwise XOR operation and Shift(S, k) performs a k-bit circular shift. In our experiments, k was empirically optimized to maximize entropy and NIST test performance while keeping implementation simple. This method helps in suppressing residual patterns arising from hardware biases or ADC quantization artifacts. The computational cost is negligible, as the operation can be integrated into peripheral control logic or firmware without requiring additional analog circuitry. Figure 5 presents the NIST evaluation results after applying shift-and-XOR post-processing with $k = 4$. With this step, the ADC resolution requirement for the C2C-based TRNG can further be relaxed up to 8-bit resolution, maintaining similar entropy quality as can be seen from NIST SP800-90B results in Figure 5b. However, for the READ noise-based TRNG, no ADC resolution reduction is possible because its smaller signal amplitude demands fine quantization that post-processing cannot replace. These results show that C2C-based TRNGs can exploit lightweight post-processing

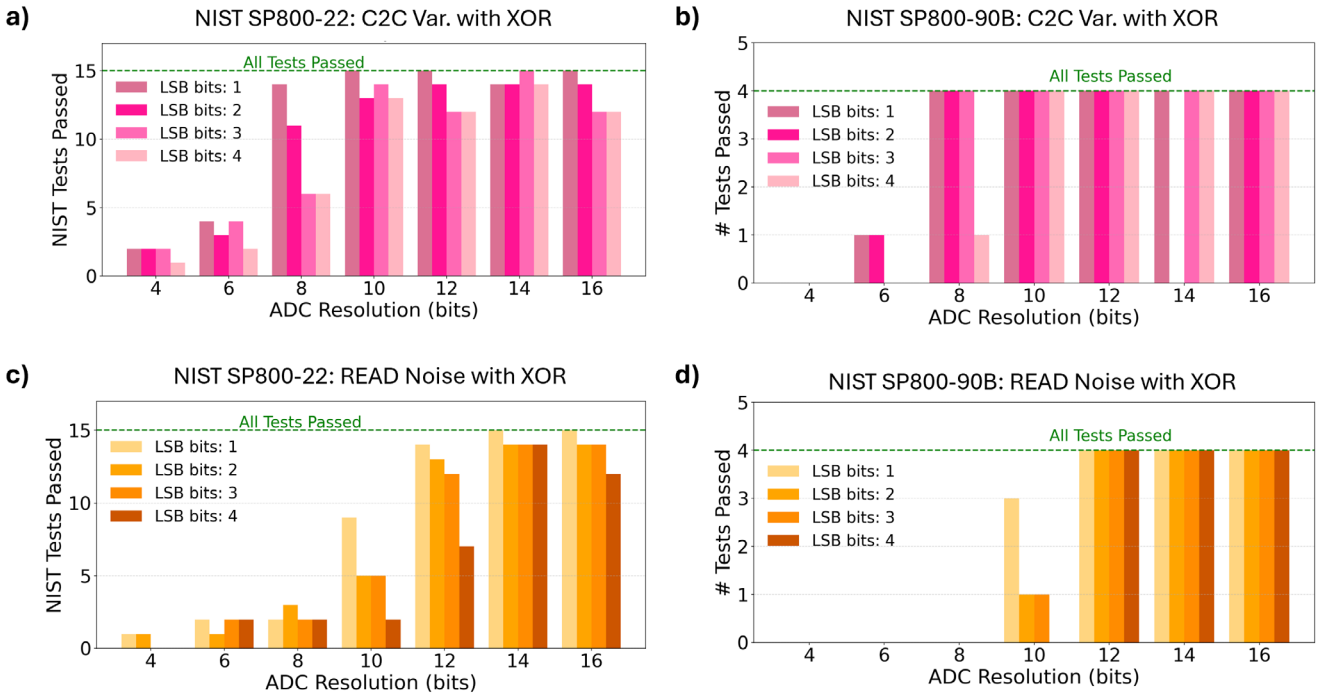

FIGURE 5 | Impact of shift-and-XOR post-processing on ADC resolution requirements. (a, b) ADC resolution dependence of NIST SP800-22 and SP800-90B test results for the C2C variability-based TRNG. (c, d) Corresponding results for the READ noise-based TRNG. The application of the shift-and-XOR technique allows for a reduction in the minimum ADC resolution required to meet NIST randomness criteria.

to enable low-resolution ADCs while maintaining efficiency and randomness.

2.6 | Performance Analysis of TRNG

2.6.1 | TRNG Energy Calculations

The energy consumption and throughput of the TRNG depend on both the entropy generation and the entropy extraction processes. To evaluate the two proposed techniques, we computed the energy contributions from both phases. In the readout stage, the ADC dominates energy consumption. The readout energy can be reduced by lowering the ADC resolution. We employed the Accelergy framework [37, 38] to model the resolution-dependent ADC conversion cost. This framework provides architecture-level energy estimation through analytical component models [37]. For the ADCs, its SAR-based plug-in [38] captures resolution-dependent scaling laws calibrated to circuit-level designs, enabling accurate and rapid exploration of energy–accuracy trade-offs. Figure 6a shows the modeled conversion energy trend for SAR ADC in 28 nm CMOS with the sampling rate of 500 Msamples/s, representative of typical ADC specifications in CiM systems. As the resolution decreases from 16 bits to 4 bits, the conversion energy drops exponentially.

During entropy generation phase, the C2C-based method requires active switching of the RRAM cells, whereas the READ noise-based method only involves repeated read operations of the LRS state. To calculate the switching energy, the 1T1R cells were cycled using the SET pulse of $V_{SET} = 2.5$ V and the RESET pulse of $V_{RESET} = 2$ V, each with the duration of $t_{pulse} = 100$ ns. The corresponding switching currents I_{SET} (during the SET) and I_{RESET} (during the RESET) were recorded, and the total switching energy was evaluated as:

$$E_{switch} = V_{SET} \times I_{SET} \times t_{pulse} + V_{RESET} \times I_{RESET} \times t_{pulse} \quad (4)$$

Under these conditions, the switching energy is estimated to be ~49.3 pJ, whereas a single LRS read operation consumes only ~0.6 pJ (for $t_{pulse} = 100$ ns and $V_{READ} = 0.3$ V), comparable to the cost of a 4-bit ADC conversion. In contrast, the conversion energy of a 12-bit ADC already approaches the magnitude of the switching energy.

The total per-bit TRNG energy consumption was computed as the sum of entropy generation and entropy extraction contributions, while the cost of the shift-and-XOR post-processing stage was neglected due to its negligible digital overhead. Figure 6b,c summarize the resolution-dependent energy versus randomness trade-off, and the detailed energy breakdown for representative operating points is provided in Table 4. At the 16-bit baseline, both TRNG variants pass all SP800-90B tests but require a high per-bit energy of ~7.5 nJ, dominated by ADC conversion. When the resolution is reduced, the C2C-based TRNG maintains entropy quality down to 8 bits, where the ADC energy drops to 1.3 pJ bit^{-1}, giving a total of ~51.2 pJ bit^{-1}, now dominated by switching. By contrast, the READ noise-based TRNG requires at least 12-bit resolution to remain compliant, resulting in a total of ~66.1 pJ bit^{-1}, where ADC conversion is still the main contributor. In addition to energy, the ADC resolution also impacts circuit footprint. According to Accelergy estimates, the 8-bit SAR ADC in 28 nm CMOS occupies ~4280 μm^2, whereas the 12-bit ADC requires ~13 723 μm^2. This threefold increase highlights the strong area overhead associated with higher-resolution converters.

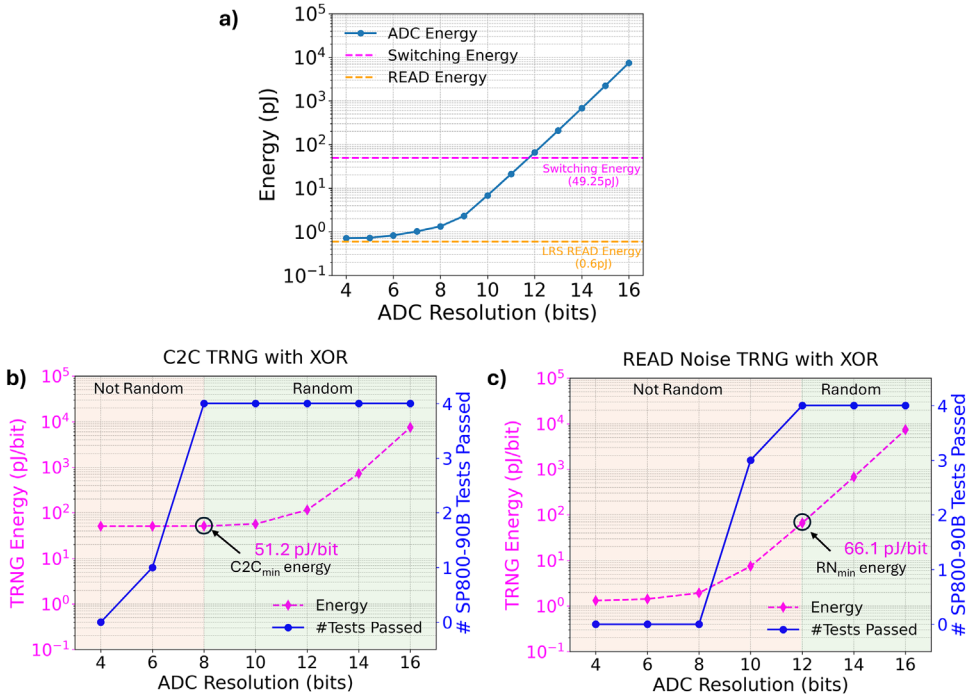

FIGURE 6 | Energy requirements of the entropy sources for TRNG. (a) Variation of ADC conversion energy as a function of ADC resolution evaluated using the Accelergy model. Trade-off between TRNG randomness (NIST SP800-90B tests passed) and energy consumption at different ADC resolutions for (b) C2C TRNG with XOR and (c) READ noise TRNG with XOR. The application of the shift-and-XOR technique reduces the ADC resolution requirement to 8 bits for the C2C variability-based TRNG, significantly lowering overall energy consumption. In contrast, the READ noise-based TRNG still requires the 12-bit ADC even with shift-and-XOR processing, resulting in comparable energy per bit despite the absence of energy-intensive switching operations.

TABLE 4 | Summary of energy components for the C2C- and the READ noise-based TRNGs at baseline (16-bit) and at the minimum ADC resolution required for NIST SP800-90B compliance with Shift-and-XOR post-processing.

TRNG Type	ADC Resolution	Energy Breakdown (pJ bit^{-1})	Total (pJ bit^{-1})
C2C variability	16-bit (baseline)	ADC: ~7,500 Switching: 49.3 Read: 0.6	~7,550
C2C variability	8-bit (with Shift & XOR)	ADC: 1.33 Switching: 49.3 Read: 0.6	51.2
READ noise	16-bit (baseline)	ADC: ~7,500 Switching: – Read: 0.6	~7,500
READ noise	12-bit (with Shift & XOR)	ADC: 65.5 Switching: – Read: 0.6	66.1

These results highlight a key trade-off: although the READ noise approach avoids energy-intensive switching, its dependence on high-resolution ADCs limits energy competitiveness. In contrast, the C2C method achieves similar per-bit energy with only an 8-bit ADC, reducing both circuit complexity and area overhead. With continuous process improvements, TaO_x-based RRAM endurance up to 10^{12} cycles has been reported [39–41], enabling generation of $\sim 2.5 \times 10^{14}$ random bits from a single array, sufficient for the lifetime requirements of typical CiM-based edge devices.

2.6.2 | TRNG Throughput Calculations

For the C2C-based TRNG, each cycle consists of a SET–READ–RESET sequence, where the SET and the RESET are applied in a one-step parallel manner and all 252 devices are read serially, requiring 252 serial READ cycles. The cycle time is therefore given by $t_{C2C,\,cycle} = t_{SET} + 252 \times t_{READ} + t_{RESET}$. With $t_{SET} = t_{RESET} = t_{READ} = 100$ ns and 3-bit slicing, each cycle produces $252 \times 3 = 756$ bits, corresponding to a serial throughput of ~29 Mbps. When parallel readout is enabled across all columns, the throughput scales linearly with the number of columns ($N_{col} = 9$ in our case), reaching ~267 Mbps. For the READ noise-based TRNG, a single SET operation initializes the array, after which repeated READs provide the entropy. Since the SET occurs only once, its contribution to average throughput is negligible. The effective cycle time is therefore $t_{READ,\,cycle} = 252 \times t_{READ}$, which for $t_{READ} = 100$ ns and 3-bit slicing yields $252 \times 3 = 756$ bits per cycle. This corresponds to a serial throughput of ~30 Mbps, which increases to ~270 Mbps with full column-level parallelism. The parallel mode, however, entails additional area overhead due to extra per-column readout circuits.

Overall, the energy and throughput characteristics of the two TRNG types are summarized in Table 5. The comparison

TABLE 5 | Comparison of C2C variability-based and READ noise-based TRNGs.

Aspect	C2C Variability TRNG	READ Noise TRNG
Entropy Source	C2C variability of LRS states	LRS read noise
RRAM Switching	Required every cycle	Not required
ADC Resolution (W/O shift & XOR)	10-bit	12-bit
ADC Resolution (With shift & XOR)	8-bit	12-bit
Energy Consumption	51.2 pJ bit^{-1}	66.1 pJ bit^{-1}
Throughput	Up to 267 Mbps	Up to 270 Mbps
TRNG Test Compliance	NIST SP800-22: 14/15 NIST SP800-90B: All	NIST SP800-22: All NIST SP800-90B: All
Variability in READ Current	High → needs lower ADC resolution)	Low → needs higher ADC resolution
Area Requirement (ADC)	Low (~4280 μm^2 for 8-bit)	High (~13723 μm^2, for 12-bit ~3 ×)
Best Use Case	Lower area & complexity with acceptable endurance limits	When device lifetime is more critical

highlights a fundamental trade-off between the two entropy sources: the C2C-based TRNG leverages high variability to allow low-resolution ADC operation (down to 8 bits with shift-and-XOR), thereby minimizing circuit complexity and area, but it incurs switching energy and endurance limitations due to repeated SET/RESET operations. Conversely, the READ noise-based TRNG eliminates switching overhead and offers very high endurance, yet its lower intrinsic variability requires a 12-bit ADC, which increases energy consumption and circuit overhead. Thus, C2C-based TRNGs are better suited when hardware simplicity and energy efficiency are priorities, whereas READ noise-based TRNGs are advantageous in applications where endurance is the primary constraint.

While the above analysis outlines the energy, throughput, and circuit-level trade-offs between the two TRNG architectures, the C2C-based TRNG presents a unique practical advantage: its inherently larger C2C variability enables the use of a significantly lower ADC resolution (down to 8 bits with shift-and-XOR). This approach significantly reduces readout complexity and area while retaining power consumption comparable to the read-noise-based TRNG. At the same time, it preserves the strong entropy source, making the C2C method highly appealing for embedded or resource-constrained security hardware. Nevertheless, ensuring stable statistical quality under environmental, spatial, and temporal variations is crucial. To this end, we conduct a comprehensive robustness analysis of the C2C-based TRNG and show that its variability-driven entropy generation remains consistently reliable across diverse operating conditions.

2.7 | Robust C2C Variability based TRNG

To evaluate the reliability and stability of the proposed C2C-based TRNG architecture, we performed a comprehensive robustness analysis covering thermal sensitivity, spatial consistency across the memory array, and temporal repeatability across multiple experimental runs. Since the TRNG performance must remain stable under environmental variations, we evaluated the C2C entropy source at elevated temperature. A 1-million-bit sequence was generated at 85 °C and the entropy is evaluated using NIST SP800-90B test suite. As represented in Table 6, the C2C variability based TRNG passes all the statistical tests at 85 °C with the estimated min-entropy of 0.996, confirming stable entropy generation under thermal stress.

To assess spatial robustness, we generated 1-million-bit sequences from five distinct regions of the 28×9 RRAM array. Four regions consisted of 50 devices and the fifth of 52 devices. For each region, we evaluated the min-entropy using NIST SP800-90B and verified that all tests were passed. As shown in Figure 7a,b, all sub-arrays exhibit consistent performance with min-entropy values greater than 0.99, demonstrating strong spatial consistency across different device clusters. Temporal repeatability was validated by generating ten independent 1-million-bit sequences from the same C2C TRNG architecture. All sequences passed the full NIST SP800-90B tests, with min-entropy consistently greater than 0.99, as shown in Figure 7c,d. These results confirm the stability of the entropy generation mechanism across repeated measurements. Overall, the C2C-based TRNG demonstrates robustness against temperature variations, spatial non-uniformity across sub-arrays, and temporal variations across repeated runs, validating its suitability for reliable hardware security applications.

Table 7 benchmarks proposed C2C based TRNG with prior RRAM-based TRNGs. Earlier designs often achieve high throughput or competitive energy efficiency [11–17], but they are not compatible with compute-in-memory (CiM) operation. These approaches typically rely on dedicated entropy-extraction circuits, such as ring oscillators, counters, or multi-stage logic blocks, which add area, complexity, and system overhead. CiM-compatible ADC-based TRNGs [19, 20] reduce such overhead but achieve only modest bit rates (1.5–23 Mb s^{-1}). Their throughput is also limited by the intrinsic entropy-generation rate of a single device or noise mechanism. Parallel entropy extraction is a natural strategy to increase throughput. However, the D2D variability in RRAM devices often leads to nonuniform entropy distributions and unstable statistical behavior when multiple cells are combined [13, 42]. In this work, we have addressed these limitations by designing the entropy-extraction architecture that is inherently invariant to D2D variability. Our approach simultaneously harvests both C2C and D2D fluctuations across many devices. This enables robust parallel readout without calibration or statistical imbalance and allows us to exceed the generation

TABLE 6 | NIST SP800-90B test results for the C2C variability TRNGs with 8-bit ADC (with shift and XOR) at 25 °C and 85 °C.

S/No.	Test	T=25 °C	T=85 °C
1	IID Permutation	PASS	PASS
2	Chi-square Independence	PASS, Score = 1979, dof = 2046, p-value = 0.27	PASS, Score = 1957, dof = 2046, p-value = 0.92
3	Chi-square Goodness-of-fit	PASS, Score = 10.44, dof = 9, p-value = 0.32	PASS, Score = 19.34, dof = 9, p-value = 0.02
4	LRS Test	PASS, Pr(X ⩾ 1): 0.0.60	PASS, Pr(X ⩾ 1): 0.59
	Min-entropy	0.995	0.996

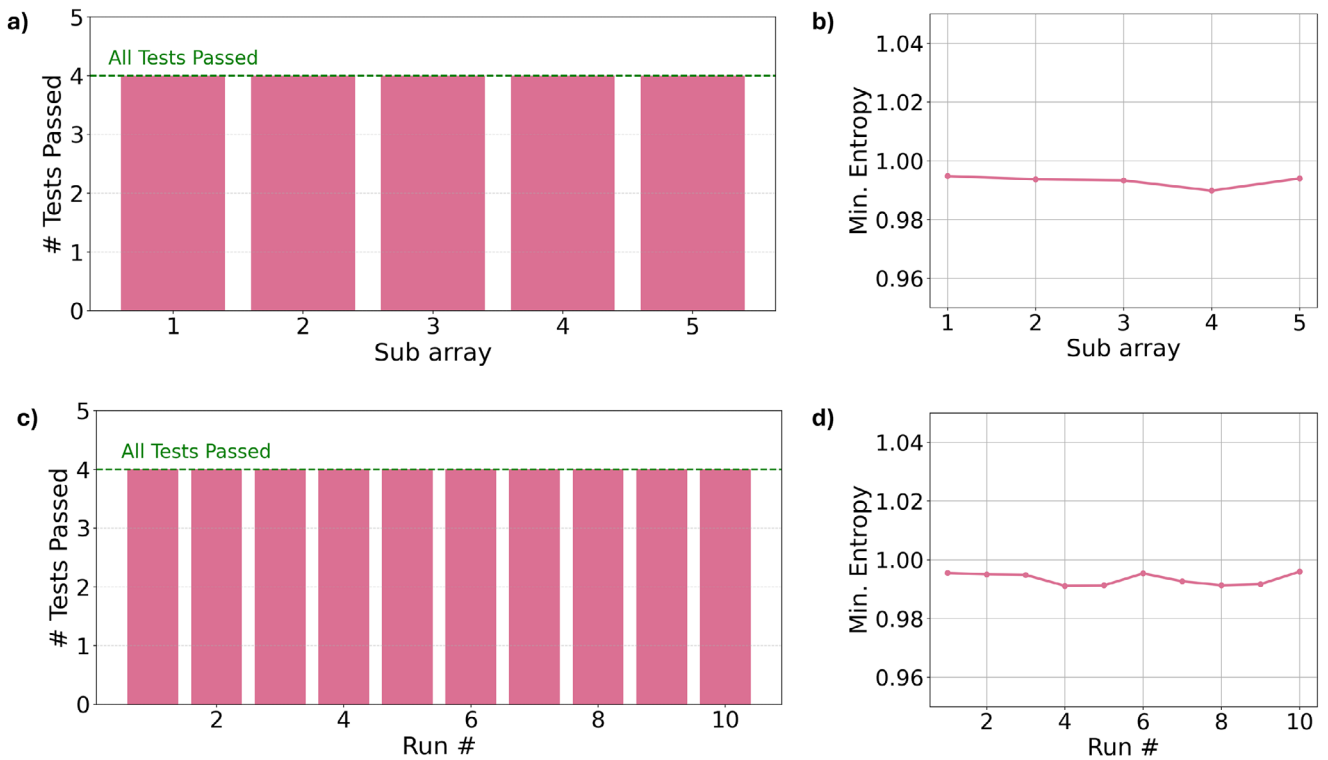

FIGURE 7 | Spatial and temporal robustness of the C2C-based TRNG: (a)–(b) NIST SP800-90B test results and estimated min-entropy for TRNG bitstreams generated from five distinct sub-array regions. (c)–(d) NIST SP800-90B test results and min-entropy for ten independent 1-million-bit sequences demonstrating temporal repeatability.

-rate limit imposed by any single entropy source. Consequently, our C2C-LRS-based TRNG achieves a throughput of 267 Mb s^{-1} with the energy consumption of 51.2 pJ bit^{-1} and maintains full NIST SP800-90B compliance over 25–85° C. These results establish our design as a fast, robust, and highly reliable CiM-compatible RRAM-based TRNG.

3 | Conclusion

In this work, we experimentally demonstrated and evaluated two CiM-compatible TRNG architectures based on TaO_x-based 1T1R RRAM arrays: one exploiting C2C variability of the LRS and the other leveraging LRS read noise. Both architectures integrate a column-wise readout circuit with a TIA and an *n*-bit ADC for entropy digitization. Comprehensive statistical evaluation using NIST SP800-22 and SP800-90B test suites confirmed the cryptographic quality of randomness for both entropy sources in the array. The comparative analysis, summarized in Table 5, reveals distinct trade-offs between the two approaches. The C2C-based TRNG benefits from higher intrinsic variability in the LRS READ current, enabling acceptable randomness down to 10-bit ADC resolution without post-processing, and down to 8-bit resolution with a lightweight shift-and-XOR step. This reduces circuit complexity, ADC area, and energy consumption, albeit at the cost of endurance due to repeated SET/RESET operations. In contrast, the READ noise-based TRNG avoids switching-induced wear, offering higher endurance and slightly higher throughput. However, its lower read current variability necessitates a higher ADC resolution (12 bits), which increases circuit complexity, area, and energy consumption. Energy and throughput analyses further show that, although both approaches can achieve similar per-bit energy in the range of 51–66 pJ bit^{-1}, the dominant contributor differs: ADC conversion energy for READ noise

TABLE 7 | Comparison of RRAM-based TRNGs and this work.

Ref[Year]	Entropy source	Device / Architecture	Bit rate (Mb/s)	Energy (pJ/bit)	NIST 90B	Test Temp.	CiM Compatible
[11][2020]	Resistance perturbation	1T1R RRAM + Capacitor + Counter	230	n/a	Yes	−40– 125°C	No
[12][2021]	Oscillation period fluctuation	1T1R RRAM + Comparator + Counter	n/a	0.75	Yes	25°C	No
[13][2023]	Threshold switching + RRAM switching	Selector-RRAM + T&D FF + XOR	>28	0.8	No	25°C	No
[14][2023]	Resistance fluctuations	Memristor + Ring Oscillator	1000	0.144	No	−40– 125°C	No
[15][2023]	Inter/intra device resistance variability	RRAM + T FF + Inverter + AND + DFF	25	1.3	No	25°C	No
[16][2023]	Intra-device switching variability	Memristor + Ring Osc. + D Flip-Flop	∼1	3.64	No	25°C	No
[18][2025]	Thermal noise + RTN	RRAM + CRSA	20	n/a	No	25– 75°C	Digital
[19][2022]	Read noise	1T1R RRAM Array + 16-bit ADC	1.5	n/a	Yes	−55– 125°C	Yes
[20][2025]	ADC-based entropy extraction	1T1R RRAM Array + 16-bit ADC	23.16	23	No	25°C	Yes
[21][2025]	D2D variation (PUF entropy)	1T1R ReRAM CiM/PUF (128×128)	n/a	n/a	Yes	−50– 125°C	Yes
This Work	C2C LRS variability	1T1R RRAM Array + 8-bit ADC	**267**	**51.2**	**Yes**	25 – 85°C	**Yes**

-based TRNGs versus switching energy for C2C-based TRNGs. Throughput scales with the degree of parallel readout, reaching up to ∼270 Mbps for READ noise and ∼267 Mbps for C2C variability in the 1T1R array implementation.

In summary, the choice between C2C-variability-based and READ-noise-based TRNGs depends on system-level priorities. While both architectures achieve comparable energy efficiency and throughput, the C2C-based TRNG offers a unique practical advantage: its inherently larger C2C variability enables operation with substantially lower ADC resolution. This reduces readout complexity, ADC area, and energy consumption, making it highly attractive for embedded or resource-constrained security hardware, provided that device endurance remains within acceptable limits. In contrast, the READ-noise-based TRNG is preferable in scenarios where endurance is the primary constraint, albeit at the cost of requiring a higher-resolution ADC (12 bits). Finally, we performed a comprehensive robustness analysis demonstrating that the C2C-based TRNG preserves its statistical quality across environmental, spatial, and temporal variations, confirming the reliability of its variability-driven entropy source for secure CiM and edge-computing applications.

Experimental Section

3.1 | RRAM Array Fabrication

For hardware realization of the CiM-compatible entropy source, TaO_x/Ta-based RRAM 1T1R arrays were monolithically integrated with 180 nm CMOS technology provided by XFAB. The integration process began by exposing the tungsten (W) contact plugs from the front end of line (FEOL) processed wafers. A 25 nm-thick platinum (Pt) layer was then deposited by DC sputtering to form the bottom electrode (BE), which was subsequently patterned using electron-beam lithography (EBL) followed by reactive ion etching (RIE). Next, a 7 nm-thick TaO_x switching layer was deposited via RF sputtering in an Ar/O_2 gas mixture (77%/23%) at 236 W RF power. A 13 nm-thick Ta layer was then deposited by DC sputtering to serve as an oxygen reservoir. Subsequently, a 25 nm-thick Pt top electrode (TE) was deposited by DC sputtering. The switching oxide and TE stack were patterned using the EBL and RIE-based back-etching to complete the device integration.

3.2 | RRAM Array Electrical Characterization

Array-level electrical characterization was performed using an FPGA-based memory controller platform (ARC2, ARC Instruments). The 31×16 array was accessed through a 64-pin probe card connected to the ARC2 interface, controlled via Python. The ARC2 board generated programmable voltage pulses with widths down to 1 μs, enabling repeated SET/RESET operations and read measurements for entropy extraction. For C2C-based TRNG operation, random bits were generated by performing parallel SET/RESET followed by serial READ operations. During the parallel SET step, all WLs were biased at $V_{G,\,SET} = 2$ V, SLs were grounded, and a SET voltage of $V_{SET} = 2.5$ V with a 1 μs pulse was applied to all BLs. This results in a one-step parallel programming of all the devices in the array. The resulting LRS states of all devices were then read serially, one device at a time, by applying $V_{READ} = 0.3$ V to the selected BL, $V_{G,\,READ} = 3.3$ V to the selected WL, and $V_{SL} = 0$ V to the selected SL. For all unselected lines, $V_{BL} = 0$ V, $V_{WL} = 0$ V, and $V_{SL} = V_{READ}$ were applied, ensuring that only the selected device experienced the read potential of 0.3 V. After reading, a parallel RESET step was performed by applying $V_{RESET} = 2$ V to all SLs, grounding all BLs, and biasing all WLs at $V_{G,\,RESET} = 3.3$ V, thereby reversing the device polarity.

For READ-noise-based TRNG operation, all 1T1R devices in the array were first programmed serially by applying $V_{SET} = 2.5$ V to the selected BL, $V_{G,\,SET} = 2$ V to the selected WL, and grounding the selected SL. The unselected BLs were grounded, unselected SLs were pulled up to $V_{SL} = V_{SET} = 2.5$ V, and unselected WLs were grounded. This serial programming step is performed only once at the beginning of the measurement. The stochasticity in the READ-noise-based TRNG is then extracted by performing repeated serial READ operations across all devices in the array. It is important to note that the READ current conditions used in the READ-noise-based TRNG are identical to those used for the C2C-variability-based TRNG. The key distinction is that, in the READ-noise-based TRNG, the entire array is first initialized into the LRS and then each device is read multiple times, whereas in the C2C-based TRNG all devices undergo repeated parallel SET/RESET cycling with intermediate LRS READ

For device-level energy analysis, individual 1T1R cells were characterized using a Keithley 4200 semiconductor parameter analyzer equipped with integrated pulse-and-measure units. This setup enabled the application of voltage pulses as short as 100 ns while simultaneously capturing transient current waveforms, allowing accurate estimation of SET, RESET, and READ energies. For evaluating the SET, RESET, and READ energy, the corresponding voltages were applied through four PMU channels to the selected WLs, BLs, and SLs, following the biasing schemes described in the previous section. Due to the limited number of available PMU channels, all unselected lines were left floating.

Acknowledgments

This work was supported in part by the Federal Ministry of Education and Research (BMBF, Germany) in the project NEUROTEC II under Project 16ME0398K, Project 16ME0399. The authors would like to thank Dr. Michael Schiek for his valuable management contributions to the NEUROTEC II project.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

1. A. Sebastian, M. Le Gallo, R. Khaddam-Aljameh, and E. Eleftheriou, "Memory Devices and Applications for In-Memory Computing,"*Nature Nanotechnology* 15, no. 7 (2020): 529–544.

2. G. Rajendran, W. Banerjee, A. Chattopadhyay, and M. M. S. Aly, "Application of Resistive Random Access Memory in Hardware Security: A Review," *Advanced Electronic Materials* 7, no. 12 (2021): 2100536.

3. F. Zahoor, A. Nisar, U. I. Bature, et al., "An Overview of Critical Applications of Resistive Random Access Memory," *Nanoscale Advance* 6 (2024): 4980–5006.

4. D. Ielmini and H.-S. P. Wong, "In-Memory Computing with Resistive Switching Devices," *Nature Electronics* 1, no. 6 (2018): 333–343.

5. A. Bende, S. Singh, C. K. Jha, et al., "Experimental Validation of Memristor-Aided Logic Using 1T1R TaOx RRAM Crossbar Array," (IEEE, 2024): 565–570.

6. C. Ding, Y. Ren, Z. Liu, and N. Wong, "Transforming Memristor Noises into Computational Innovations," *Communications Materials* 6, no. 1 (2025): 149.

7. W. Choi, O. Kwon, J. Lee, et al., "Volatile Threshold Switching Devices for Hardware Security Primitives: Exploiting Intrinsic Variability as an Entropy Source," *Applied Physics Reviews* 11, no. 2 (2024): 021323.

8. R. Carboni and D. Ielmini, "Stochastic Memory Devices for Security and Computing," *Advanced Electronic Materials* 5, no. 9 (2019): 1900198.

9. G. Rajendran, F. Zahoor, S. S. Thakker, et al., "Harnessing Entropy: RRAM Crossbar-based Unified PUF and RNG," (IEEE, 2024): 560–564.

10. Y. Pang, B. Gao, B. Lin, H. Qian, and H. Wu, "Memristors for Hardware Security Applications," *Advanced Electronic Materials* 5, no. 9 (2019): 1800872.

11. B. Lin, B. Gao, Y. Pang, et al., "A High-performance and Calibration-free True Random Number Generator Based on the Resistance Perturbation in RRAM Array," in *2020 IEEE International Electron Devices Meeting (IEDM)* (IEEE, 2020), 38.6.1–38.6.4.

12. Q. Ding, H. Jiang, J. Li, et al., "Unified 0.75pJ/Bit TRNG and Attack Resilient 2F2/Bit PUF for Robust Hardware Security Solutions with 4-layer Stacking 3D NbOx Threshold Switching Array," in *2021 IEEE International Electron Devices Meeting (IEDM)* (IEEE, 2020), 39.2.1–39.2.4.

13. Y. Qin, Z. Wang, Y. Yang, et al., "A High-Speed True Random Number Generator Based on Unified Selector-RRAM," *IEEE Electron Device Letters* 44, no. 12 (2023): 1967–1970.

14. X. Li, Y. Wang, Y. Yang, et al., "A 144-fJ/Bit Reliable and Compact TRNG Based on the Diffusive Resistance of 3-D Resistive Random Access Memory," *IEEE Transactions on Electron Devices* 70, no. 8 (2023): 4139–4144.

15. M. Akbari, S. Mirzakuchaki, D. Arumí, et al., "True Random Number Generator Based on the Variability of the High Resistance State of RRAMs," *IEEE Access* 11 (2023): 66682–66693.

16. D. Arumí, S. Manich, A. Gómez-Pau, R. Rodríguez-Montañés, M. B. González, and F. Campabadal, "True Random Number Generator Based on RRAM-Bias Current Starved Ring Oscillator," *IEEE Journal on Exploratory Solid-State Computational Devices and Circuits* 9, no. 2 (2023): 92–98.

17. J. Park, H. Kim, and H. Kim, "Bias-Independent True Random Number Generator Circuit using Memristor Noise Signals as Entropy Source," *Advanced Intelligent Systems* 7, no. 6 (2025): 2400648.

18. P. Hsiung Huang, R. Yang Lu, Y. Hsien Lin, H. Siang Su, and E. Ray Hsieh, "Filamentary Random Telegraph Noise-Based Multiple-Resistive-State True Random Number Generator for Probabilistic Hot/Cold Bits," *IEEE Transactions on Electron Devices* 72, no. 7 (2025): 3573–3581.

19. B. Gao, B. Lin, X. Li, J. Tang, H. Qian, and H. Wu, "A Unified PUF and TRNG Design Based on 40-nm RRAM With High Entropy and Robustness for IoT Security," *IEEE Transactions on Electron Devices* 69, no. 2 (Feb 2022): 536–542.

20. X. Li, B. Gao, Q. Qin, et al., "Federated Learning Using a Memristor Compute-in-Memory Chip with In Situ Physical Unclonable Function and True Random Number Generator," *Nature Electronics* 8, no. 6 (2025): 518–528.

21. W. Yue, K. Yu, Z. Li, et al., "Physical Unclonable In-Memory Computing for Simultaneously Protecting Private Data and Deep Learning Models," *Nature Communications* 16 (2025): 1031.

22. National Institute of Standards and Technology, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," (2010), NIST Special Publication 800-22 Rev. 1a.

23. National Institute of Standards and Technology, "Recommendation for the Entropy Sources Used for Random Bit Generation," (2018), NIST Special Publication 800-90B.

24. J. Yang, D. Strukov, and D. Stewart, "Memristive Devices for Computing," *Nature Nanotechnology* 3, no. 7 (2008): 429–433.

25. R. Waser, R. Dittmann, G. Staikov, and K. Szot, "Redox-Based Resistive Switching Memories—Nanoionic Mechanisms, Prospects, and Challenges," *Advanced Materials* 21, no. 25-26 (2009): 2632–2663.

26. A. Schönhals, R. Waser, and D. Wouters, "Experimental and Theoretical Study of Resistive Switching in TaO_x Memristive Devices for Neuromorphic Applications," *Nanotechnology* 28, no. 46 (2017): 465203.

27. P. Ravindra, M. Liehr, R. Mathkari, K. Beckmann, N. Tokranova, and N. Cady, "Intrinsic Variability in Oxide-Based Resistive Memories: Challenge or Opportunity for Hardware Security?," *Frontiers in Materials* 11 (2024): 1343076.

28. C. Bengel, A. Siemon, F. Cüppers, et al., "Compact Modeling of RRAM Devices With Filamentary Switching Including Cycle-to-Cycle and Device-to-Device Variability," *IEEE Transactions on Circuits and Systems I: Regular Papers* 67, no. 12 (2020): 4618–4631.

29. V. Ntinas, D. Patel, Y. Wang, et al., "A Simplified Variability-Aware VCM Memristor Model for Efficient Circuit Simulation," in *2023 19th International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD)*, (2023): 1–4, https://doi.org/10.1109/SMACD58065.2023.10192107.

30. A. Funck, S. Dirkmann, H. Mähne, and M. Salinga, "Barrier Layer Engineering for Cycle-to-Cycle Variability Reduction in Oxide-Based Memristors," *Advanced Intelligent Systems* 5, no. 3 (2023): 2300040.

31. K. Sugawara, H. Shima, M. Takahashi, Y. Naitoh, H. Suga, and H. Akinaga, "Low-Frequency-Noise Spectroscopy of TaOx-based Resistive Switching Memory," *Advanced Electronic Materials* 8, no. 8 (2022): 2100758.

32. Y. Pan, Y. Cai, Y. Liu, et al., "Microscopic Origin of Read Current Noise in TaO_x-Based Resistive Switching Memory by Ultra-Low-Temperature Measurement," *Applied Physics Letters* 108, no. 15 (2016): 153504.

33. K. Yamauchi, N. Misawa, H. Shima, et al., "Read Voltage Dependency of Random Telegraph Noise in the Intermediate State of TaOx-based ReRAM," (IEEE, 2025): 1–6.

34. B. Sánta, Z. Balogh, L. Pósa, et al., "Noise Tailoring in Memristive Filaments," *ACS Applied Materials & Interfaces* 13, no. 6 (2021): 7453–7460.

35. M.-J. O. Saarinen, "SP 800-22 and GM/T 0005-2012 Tests: Clearly Obsolete, Possibly Harmful," in *2022 IEEE European Symposium on Security and Privacy Workshops*, (IEEE, 2022): 31–37.

36. M. Aslan, A. Doğanaksoy, Z. Saygı, M. S. Turan, and F. Sulak, "Observations on NIST SP 800-90B entropy estimators," *Cryptography and Communications* (2025), https://doi.org/10.1007/s12095-025-00778-7.

37. Y. N. Wu, J. S. Emer, and V. Sze, "Accelergy: An Architecture-Level Energy Estimation Methodology for Accelerator Designs," in *2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)* (2019): 1–8, https://doi.org/10.1109/ICCAD45719.2019.8942149.

38. T. Andrulis, R. Chen, H.-S. Lee, J. S. Emer, and V. Sze, "Modeling Analog-Digital-Converter Energy and Area for Compute-In-Memory Accelerator Design," arXiv preprint arXiv:2404.06553 (2024), https://arxiv.org/abs/2404.06553.

39. M.-J. Lee, C. B. Lee, D. Lee, et al., "A Fast, High-Endurance, and Scalable Non-Volatile Memory Device Made from Asymmetric Ta_2O_{5-x}/TaO_{2-x} Bilayer Structures,"*Nature Materials* 10, no. 8 (2011): 625–630.

40. M. Hellenbrand, I. Teck, and J. L. MacManus-Driscoll, "Progress of Emerging Non-Volatile Memory Technologies in Industry,"*MRS Communications* 14, no. 6 (2024): 1099–1112.

41. F. Zahoor, T. Z. A. Zulkifli, and F. A. Khanday, "Resistive Random Access Memory (RRAM): an Overview of Materials, Switching Mechanism, Performance, Multilevel Cell (mlc) Storage, Modeling, and Applications,"*Nanoscale Research Letters* 15, no. 1 (2020): 90.

42. Z. Chai, W. Shao, W. Zhang, et al., "GeSe-Based Ovonic Threshold Switching Volatile True Random Number Generator,"*IEEE Electron Device Letters* 41, no. 2 (2020): 228–231.