SCIENCE CHINA
Information Sciences

• LETTER •

September 2026, Vol. 69, Iss. 9, 199403:1–199403:2
https://doi.org/10.1007/s11432-025-4824-y

A 250 Mbps 6.5375 Mb/s/μm² PVT-robust TRNG with charge-trap programming (CTP)-based dynamic 0/1 bias cancellation

Ye LIN[1], Junjie SHEN[1], Anying JIANG[1], Yuan DU[1,2*] & Li DU[2,3*]

[1]*School of Electronic Science and Engineering, Nanjing University, Nanjing 210023, China*
[2]*Interdisciplinary Research Center for Future Intelligent Chips (Chip-X), Nanjing University, Suzhou 215163, China*
[3]*School of Integrated Circuits, Nanjing University, Suzhou 215163, China*

Received 6 August 2025/Revised 11 December 2025/Accepted 2 March 2026/Published online 13 August 2026

Citation Lin Y, Shen J J, Jiang A Y, et al. A 250 Mbps 6.5375 Mb/s/μm² PVT-robust TRNG with charge-trap programming (CTP)-based dynamic 0/1 bias cancellation. Sci China Inf Sci, 2026, 69(9): 199403, https://doi.org/10.1007/s11432-025-4824-y

The demand for securing sensitive data is increasing exponentially in Internet of Things (IoT) devices. As a key component of security systems, random number generators (RNGs) are divided into pseudo RNGs (PRNGs) and true RNGs (TRNGs). Although PRNGs offer good statistical properties for highly secure systems, the random numbers become predictable once the seed is exposed, thereby reducing the level of security. Hardware TRNGs extracting entropy from physical noise are reported across various cryptographic applications. It can be categorized into jitter-based and metastability-based designs. Although jitter-based TRNGs have the advantages of design simplicity and a small area overhead, which typically harvest entropy through timing jitter, they remain vulnerable to power supply attacks, suffer from low speed, and have high power consumption. On the other hand, metastability-based TRNGs are prone to process variations, requiring complex calibration circuits to suppress bias; furthermore, a complex post-processing circuit is required to achieve sufficient randomness, introducing significant area overhead.

To overcome the above-mentioned TRNGs limitation, we proposed an area-efficient PVT-robust TRNG circuitry utilizing the charge-trap programming (CTP) method to correct 0/1 bias, where a StrongARM comparator is designed as the entropy source (ES). When a comparator is used as an ES, its output 0/1 bias must be canceled to a specific level. Conventional 0/1 bias cancellation methods, such as capacitor-based and binary-weighted device-based 0/1 bias cancellation, are volatile and require generating multiple-bit codes to correct 0/1 bias, which leads to additional area overhead and power consumption [1, 2]. In contrast, the CTP-based 0/1 bias cancellation method is demonstrated as an excellent nonvolatile cancellation method for bias cancellation without introducing additional area overhead and power consumption [3]. To address the volatility, increased design complexity, and additional power consumption associated with traditional 0/1 bias cancellation methods, we propose a CTP-based ES architecture, as shown in Figure 1(a). The proposed ES with minimum-sized transistors consumes a much smaller area compared to the previous binary-weighted trimming ES design [1], which utilizes 8-bit binary-weighted device arrays. In the proposed ES, the threshold voltage (VTH) of M3 and M4 is adjusted using the CTP method to achieve a low input voltage offset, which determines the ES offset [4]. SAE is the clock signal for the ES, while SAQ and SAQB represent differential outputs. CH and CHB are the programming enable signals, and HV_CHB is used to control the ES inputs, determining whether the ES operates in entropy sampling mode or 0/1 bias cancellation mode.

In 0/1 bias cancellation mode, charge trapping requires establishing a current path through the charge trap transistor (CTT). This is achieved by setting the CH signal to 0.9 V, thereby enabling current flow, as shown in Figure 1(b). Simultaneously, the HV_CHB signal is set to 1.8 V to disable transistors M1 and M2. An external programming voltage pulse is then applied to nodes P1 or P2 via the HV_CH switches according to the current 0/1 bias. Additionally, the body terminals of M3 and M4 are externally controllable, allowing support for light erase operations.

In entropy sampling mode, the CH and HV_CHB signals are set to 0 V, turning on both M1 and M2. The common-mode voltage VCOMP is then applied to the ES input, forcing the ES into a metastable state. The result is sampled and output when the SAE signal rises from 0 to 0.9 V, as shown in Figure 1(c).

After the 0/1 bias cancellation process, the comparator can generate random numbers with an approximately 50% 0/1 bias as an ES for post-processing. Four trimmed ESs are combined through an XOR chain-based post-processing circuit to eliminate statistical deviations and correlations between raw bits, and von Neumann post-processing (VN2) is applied to further remove residual bias, as shown in Figure 1(d).

During the cancellation process, using a constant programming voltage and duration often results in inefficient VTH increments, requiring more programming iterations and potentially causing bias reversal [5]. This makes it challenging to bring the bias within the target range. To address this issue, we propose a CTP-based dynamical 0/1 bias cancellation strategy that dynamically adjusts the programming strength based on the 0/1 bias.

Based on the extent of the deviation between the probability of

* Corresponding author (email: yuandu@nju.edu.cn, ldu@nju.edu.cn)

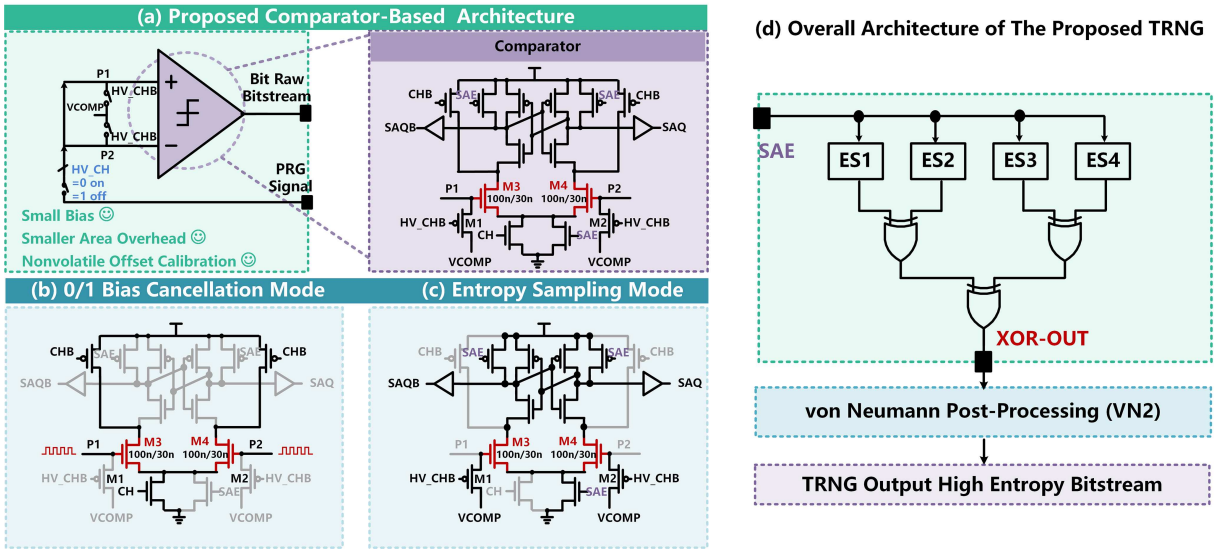

Figure 1 (Color online) (a) Proposed CTP-based ES; (b) 0/1 bias cancellation mode; (c) entropy sampling mode; (d) the overall architecture of the proposed TRNG with XOR-chain-based post-processing circuit.

1 (p_1) and the target value of 50%, we divide the calibration into three ranges: a large deviation region where $|p_1 - 50\%| > 30\%$, a moderate deviation region where $10\% < |p_1 - 50\%| \leqslant 30\%$, and a small deviation region where $5\% < |p_1 - 50\%| \leqslant 10\%$. When the deviation exceeds 30%, indicating a significant mismatch in the ES, a strong programming pulse is required to rapidly reduce the bias. In this case, we apply a programming pulse of 2 V for 5 ms, which has been experimentally shown to rapidly reduce large deviations. For the moderate deviation region, a 1.8 V pulse with a duration of 3 ms is used. Finally, when the deviation approaches the target (i.e., p_1 is close to 50%), a high programming voltage may cause bias reversal. Therefore, we reduce the programming voltage to 1.6 V while keeping the duration at 1 ms, enabling the 0/1 bias of each ES to gradually converge toward the target range.

In addition, a light erase operation is introduced to accelerate the 0/1 bias cancellation process. After programming, the VTH of the CTT initially increases significantly, followed by a slight relaxation phase before stabilizing. This transient behavior complicates 0/1 bias correction and potentially introduces additional 0/1 bias. After applying a light erase operation, the relaxation phase is skipped, which marginally lowers the VTH without fully reverting it to the pre-programmed state, thereby allowing the TRNG output to stabilize more rapidly and facilitating expedited calibration based on output bias.

The above cancellation procedure is applied to a single ES. In the proposed TRNG, four independent ES units are integrated, and their outputs are combined through an XOR-chain circuit. During operation, each ES must be sequentially canceled using the CTP-based dynamic 0/1 bias cancellation method to ensure that 0/1 bias falls within the target range. After applying the XOR-chain-based post-processing, the final TRNG output achieves a near 50% 0/1 bias.

A 6.5375 Mb/s/μm^2 PVT-robust TRNG with a CTP-based dynamic 0/1 bias cancellation method is proposed. The ES with a minimum-sized transistor achieves a low area overhead while the bias is efficiently calibrated within the target range by dynamically adjusting the programming strength based on the 0/1 bias. Additionally, the calibration circuit is eliminated due to the nonvolatile nature of CTP, further reducing the area overhead. The four trimmed ESs are combined through an XOR chain-based post-processing circuit to suppress statistical deviations and correlations between raw bits. A light erase operation is proposed to accelerate the 0/1 bias cancellation process by skipping the relaxation phase. The TRNG design is fabricated in 28-nm standard CMOS technology. All test items of NIST SP 800-22 and 800-90B are passed under four different supply voltage and temperature conditions. The Shannon entropy and Min entropy consistently exceed 0.999973909 and 0.983831 across ten chips, respectively. By trimming bias, the proposed TRNG achieves the lowest area overhead and the highlight area efficiency of 6.5375 Mb/s/μm^2. The throughput and energy efficiency are 250 Mb/s and 0.692 pJ/bit, respectively, making it suitable for area-constrained IoT applications.

Acknowledgements This work was supported in part by National Key Research and Development Program of China (Grant No. 2022YFB4400900), Strategic Industries and Key Technologies Project of Jiangsu Province (Grant No. BE2023020-3), and Basic Research Program of Jiangsu Province (Grant No. BK20243042).

Supporting information Appendixes A–D. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Kim J, Chae H. A 10-Gbps, 0.121-pj/bit, all-digital true random-number generator using middle square method. In: Proceedings of IEEE Asian Solid-State Circuits Conference (A-SSCC), 2022. 1–3
2 Zhang R, Wang X, Liu K, et al. A 0.186-pJ per bit latch-based true random number generator featuring mismatch compensation and random noise enhancement. IEEE J Solid-State Circ, 2022, 57: 2498–2508
3 Lin Y, Jiang A, Lv J, et al. An offset-cancellation technique using charge-trap transistors and asynchronous programming scheme. IEEE Trans Circuits Syst II, 2024, 71: 4638–4642
4 Shah J S, Nairn D, Sachdev M. An energy-efficient offset-cancelling sense amplifier. IEEE Trans Circ Syst II, 2013, 60: 477–481
5 Randriamihaja Y M, McMahon W, Kerber A, et al. MTPM ramped programming optimization methodology. In: Proceedings of IEEE International Reliability Physics Symposium (IRPS), 2017