A Robust -40 to 120°C All-Digital True Random Number Generator in 40nm CMOS

Kaiyuan Yang, David Blaauw, Dennis Sylvester
University of Michigan, Ann Arbor, MI E-mail: kaiyuan@umich.edu

Abstract

An all-digital True Random Number Generator (TRNG) harvesting entropy from the collapse of 2 edges injected into one even-stage ring is fabricated in 40nm CMOS. A configurable ring and tuning loop provides robustness across a wide range of temperature (-40 to 120°C), voltage (0.6 to 0.9V), process variation, and external attack. The dynamic tuning loop automatically configures the ring to meet a sufficient collapse time, thereby maximizing entropy. All dies pass all NIST randomness tests across all measured operating conditions and power supply attacks. The all-digital TRNG occupies only 836μm^2 and consumes 23pJ/bit at nominal 0.9V and 11pJ/bit at 0.6V.

Introduction

High entropy random numbers from physical sources are a critical component in authentication and encryption processes within secure systems. Digital TRNGs offer the advantages of easy integration and lower sensitivity to PVT variations over conventional analog designs [1]. For mobile and IoT applications, robustness to environmental variations becomes critical. Previous work has demonstrated digital TRNGs based on metastability [1-3], oscillator jitter [4-6], or other device noise (e.g., time to oxide breakdown [7]). Metastability-based methods provide excellent performance but often require extensive calibration to remove mismatch in devices [1-3] and are sensitive to environmental conditions. A soft oxide breakdown based TRNG [7] shows high entropy but suffers from low performance and efficiency. Ring oscillator (RO) based TRNGs offer design simplicity, but conventional methods provide relative low randomness [4] and are vulnerable to power supply attacks. Recent works employing a 3-edge RO [6] and beat frequency [5] provide good randomness and performance, but robustness was not verified across PVT conditions and could pose difficulties. This work proposes an all-digital TRNG based on the collapse time of two racing edges in an even-stage RO with automatic tuning loop, demonstrating extensive robustness to PVT variations and intentional power supply attacks.

All-Digital TRNG Implementation

Fig. 1 shows the basic concept of two-edge racing in an even-stage RO. Two edges (A, B) are injected into opposite nodes of an even-stage RO simultaneously. The two injected edges travel entirely different paths and hence accumulate device delay mismatch and noise, causing one edge to overtake the other and collapsing the oscillation. Therefore, the number of cycles until collapse depends on both systematic delay mismatch and random noise. The distribution of collapse time depends on the relative magnitude of these two factors. If systematic mismatch is small, noise will have a more significant impact, resulting in a longer, more random collapse time with a wider distribution. In this case, random bits can be obtained from the RO by recording the number of cycles to collapse. However, under large systematic mismatch, the RO will collapse in a few cycles with predictable behavior. This systematic behavior is unique for each die and can be used to produce a chip ID or PUF [8] but is not useful for extracting entropy. Typically systematic mismatch dominates in an even-stage RO and makes entropy extraction difficult. Hence, RO-based TRNGs have previously employed an odd-stage number RO where mismatch naturally cancels out [6]. However, in this paper we show that, in fact, the mismatch in an even-stage RO can be used as a natural source of tunability to enable a highly adaptive TRNG design that is robust to a wide range of environmental and other factors using an automatic tuning loop.

The proposed approach (Fig. 2) replaces each inverter stage with a set of identical inverters and a multiplexer to select one of the inverters for the RO path as specified by configuration bits. During startup, a simple control program on the host processor tunes the RO (Fig. 5) as follows: An LSFR generates a random configuration trial and collects 1000-5000 collapse times and their mean and max values. If the mean collapse time is too low, systematic variations are not properly canceled out and a new configuration trial is attempted. Mean and max collapse times that are out of range can also indicate intentional external attack as shown in the measured results. Once the mean collapse time is in the correct range the RO is properly tuned and random numbers are generated while the host processor continues to monitor collapse times to adapt to any environmental changes. In the worst-case it was found that 315 configurations trials were needed to properly tune the RO. Measurement results in Fig. 4 show that a larger average collapse count results in wider distributions that produce more high entropy bits via the counter LSBs.

The proposed TRNG was implemented using a 32-stage RO with 8 selectable inverters per stage, providing a total of $8^{32} \approx 7.8\times10^{28}$ possible RO configurations. Edge collapse automatically stops the counter, removing the need for extra phase/frequency detectors and other peripheral circuits as in [5-6], saving power and area. A 9b counter records the cycles to collapse (COUNT), which is read at the rising edge of the control clock (Fig. 3). Since TRNGs are typically co-located with a SoC processor, the control algorithm can run on the host-processor (off-chip in our tests) although its simplicity makes it suitable for hardware implementation.

Measurement Results

The randomness of the 40nm CMOS TRNG test chip is evaluated by NIST Pub 800-22 RNG testing suite (15 tests) with 100Mb data for each test. Fig. 6(a) shows throughput ranges from 300kbps to 2Mbps and efficiency from 8.7 to 37.2 pJ/b across 0.5 to 1V at 25°C. The TRNG is robust and passes all NIST tests across all combinations of voltage (0.6 to 0.9V in 100mV steps) and temperature (-40 to 120°C in 30°C steps) with a required mean-count range of 70 to 85 cycles. At lower temperature the spread (σ/μ) of collapse count is lower due to less thermal noise. The mean count range ensures sufficient quality of 3 LSBs at -40°C while enabling successful RO tuning within an acceptable number of configuration trials (Fig. 6). Table 1 shows NIST test results of 5 chips at worst-case conditions (0.6V, -40°C).

Supply noise injection is an effective attack technique to compromise TRNGs [6]. To test the robustness of the proposed TRNG to injection locking, we implement a noise injection circuit by coupling a sine wave to a DC voltage (Fig. 7). As shown in Fig. 8a, injection locking occurs at harmonics of the ring frequency (f_{RO}) and impacts both the collapse count and bit entropy. When directly applying such an attack to a single configuration of the TRNG it fails to pass NIST tests for injection amplitudes > 250mV (Fig. 8b). However, since the injection locking shifts the mean collapse count outside the specified range (Fig. 9), the control loop automatically reject the harvested bits. It then selects new configurations that provide slightly different oscillation frequencies, restoring the desired average count value and randomness. Hence, while operating the control loop all NIST tests are passed with injection amplitudes up to equipment limits (400mV) at the worst-case injection frequency of $3\times f_{RO}$.

Table 2 summarizes measurement results and compares to prior work. The TRNG generates high entropy random bits under PVT variations and intentional attacks with 836μm^2 and 11pJ/b at 0.6V.

Acknowledgements

The authors thank the TSMC University Shuttle Program for chip fabrication and NSF for research support

References

[1] S. Mathew, *IEEE JSSC*, Nov. 2012.
[2] C. Tokunaga, *ISSCC*, 2007.
[3] R. Brederlow, *ISSCC*, 2006.
[4] M. Bucci, *IEEE Trans. Computers*, April 2003.
[5] Q. Tang, *CICC*, 2014.
[6] K. Yang, *ISSCC*, 2014.
[7] N. Liu, *Symp. VLSI Circuits*, 2010.
[8] K. Yang, *ISSCC*, 2015, in press.

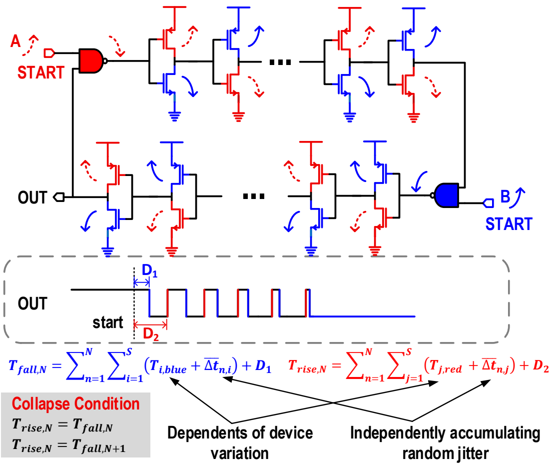

Fig. 1. Concept of TRNG based on collapse time of 2 edge RO.

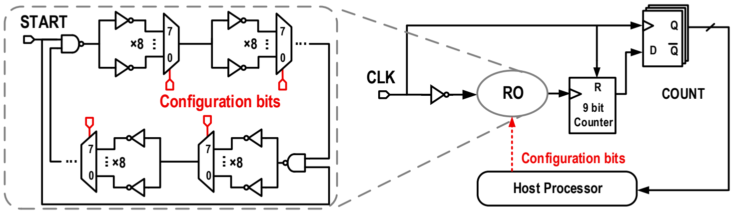

Fig. 2. TRNG block diagram and tunable RO with 8 inverters per stage.

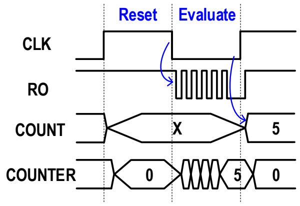

Fig. 3. Operating waveform of TRNG.

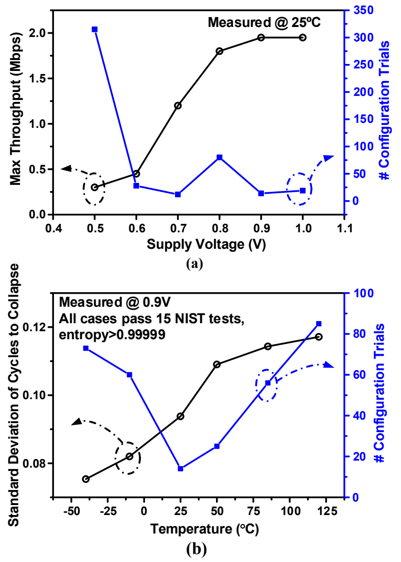

Fig. 6. Measured impacts of (a) supply voltage and (b) temperature on performance of TRNG.

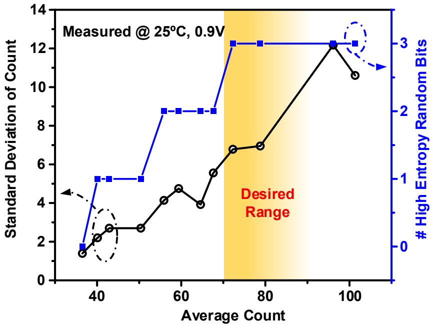

Fig. 4. Standard deviation of cycles to collapse and number of high entropy random LSBs vs. average collapse cycles.

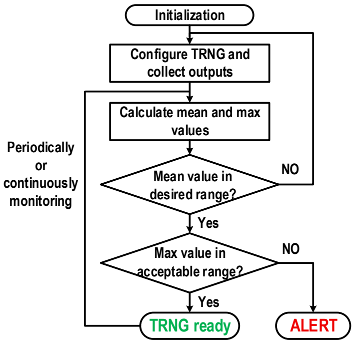

Fig. 5. Automatic tuning FSM of TRNG.

Table. 1. Measured NIST tests of 5 chips at worst condition (0.6V, -40°C)

NIST Pub 800-22, rev. 1a, 2010 Randomness Tests	Measured at -40°C, 0.6V, 450Kbps									
	Chip #1		Chip #2		Chip #3		Chip #4		Chip #5	
	P-value	Pass	P-value	Pass	P-value	Pass	P-value	Pass	P-value	Pass
Frequency	0.69	0.987	0.28	0.990	0.13	0.993	0.97	0.993	0.13	0.993
Block Frequency	0.12	0.983	0.03	0.983	0.43	0.993	0.45	0.987	0.20	0.987
Cumulativ Sum	0.57	0.983	0.09	0.990	0.55	0.987	0.02	0.993	0.25	0.993
Cumulativ Sum	0.69	0.993	0.69	0.990	0.28	0.990	0.36	0.990	0.60	0.990
Runs	0.16	0.990	0.90	0.987	0.63	0.997	0.40	0.977	0.28	0.983
Longest Runs	0.70	0.990	0.98	0.997	0.86	0.990	0.44	0.993	0.93	0.990
Matrix Rank	0.02	0.993	0.12	0.990	0.22	0.983	0.11	0.987	0.12	0.990
FFT	0.39	0.983	0.24	0.980	0.20	0.990	0.52	0.993	0.44	0.993
Serial	0.88	0.983	0.72	0.987	0.84	0.993	0.03	0.990	0.84	0.993
Serial	0.93	0.983	0.21	0.990	0.29	0.987	0.05	0.983	0.57	0.983
Linear Complexity	0.93	0.987	0.17	0.990	0.60	0.990	0.40	0.983	0.03	0.977
Non Overlapping Template	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Overlapping Template	0.19	1.000	0.63	0.980	0.65	0.980	0.57	0.970	0.83	0.980
Universal	0.21	0.990	0.38	0.970	0.26	0.980	0.70	0.960	0.49	0.990
Random Excursions	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Random Excursions Variant	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Approximate Entropy	0.03	0.960	0.35	0.970	0.26	0.980	0.43	0.990	0.55	1.000

* "PASS" means all sub tests pass minimum requirement.

** Minimum p-value χ^2 is 0.0001. Minimum pass rate is 0.97 for first 10 tests (using 300 × 40K bits) and 96/100 for the other 5 tests (using 100 × 1M bits).

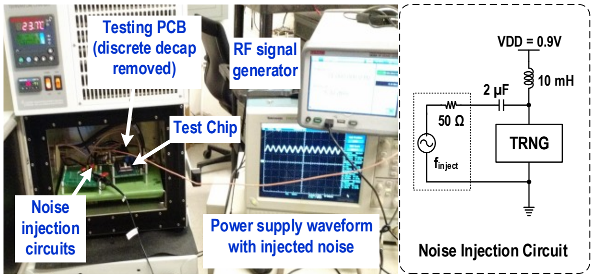

Fig. 7. Supply injection attack testing setup and schematic of noise injection circuits.

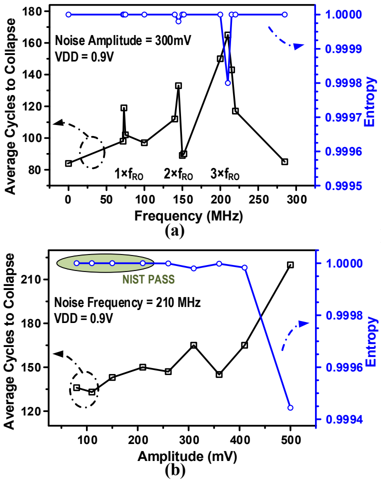

Fig. 8. Measured impacts of supply noise (a) frequency and (b) amplitude on randomness of the proposed TRNG.

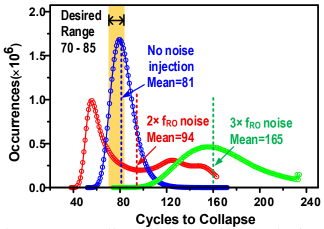

Fig. 9. Count distribution before and after supply noise injection of 300mV.

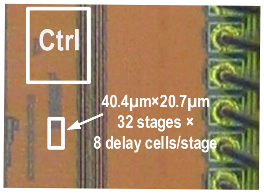

Fig. 10. Die micrograph of 40nm test chip.

	This work		CICC' 14 [5]	ISSCC' 14 [6]	JSSC' 12 [1]	VLSI' 11 [7]	ISSCC' 07 [2]	ISSCC' 06 [3]
	0.9V	0.6V						
Technology	40nm		65nm	28nm	45nm	65nm	130nm	120nm
Entropy Source	Jitter in oscillator		Jitter in oscillator	Jitter in oscillator	Metastability	Time to oxide breakdown	Metastability	Metastability
Bit Rate (Mb/s)	2	0.45	2	23.16	2400	0.011	0.2	0.2
NIST Pass	All		All	All	All	All	5	-
Area (µm^2)	836		6000	375	4004	1200	36300	9000
Power (mW)	0.046	0.005	0.13	0.54	7	2	1	0.05
Efficiency (nJ/bit)	0.023	0.011	0.066	0.023	0.0029	181.81	5	0.25
Post Processing	No		No	No	No	No	No	Yes
External Frequency Attack Robustness	Yes (up to 400mV)		N/A	Yes (filter)	N/A	N/A	N/A	N/A
Tested Operating Conditions	0.6 to 1V -40 to 120 °C		0.8 to 1.2V	N/A	0.28 to 1.35V	N/A	N/A	N/A

Table. 2. Summary of measurement results and a comparison with state-of-the-art CMOS TRNG designs.