16.3 A 23Mb/s 23pJ/b Fully Synthesized True-Random-Number Generator in 28nm and 65nm CMOS

Kaiyuan Yang, David Fick, Michael B. Henry, Yoonmyung Lee, David Blaauw, Dennis Sylvester

University of Michigan, Ann Arbor, MI

True random number generators (TRNGs) use physical randomness as entropy sources and are heavily used in cryptography and security [1]. Although hardware TRNGs provide excellent randomness, power consumption and design complexity are often high. Previous work has demonstrated TRNGs based on a resistor-amplifier-ADC chain [2], oscillator jitter [1], metastability [3-5] and other device noise [6-7]. However, analog designs suffer from variation and noise, making them difficult to integrate with digital circuits. Recent metastability-based methods [3-5] provide excellent performance but often require careful calibration to remove bias. SiN MOSFETs [6] exploit larger thermal noise but require post-processing to achieve sufficient randomness. An oxide breakdown-based TRNG [7] shows high entropy but suffers from low performance and high energy/bit. Ring oscillator (RO)-based TRNGs offer the advantage of design simplicity, but previous methods using a slow jittery clock to sample a fast clock provide low randomness [1] and are vulnerable to power supply attacks [8]. In addition, the majority of previous methods cannot pass all NIST randomness tests.

To simultaneously achieve ease of design, high randomness, good throughput and energy/bit, we present a TRNG based on 3-edge multimode RO synthesized entirely with standard cells (Fig. 16.3.1). A conventional RO injects 1 edge that propagates through the ring to form pulses. The proposed 3-edge RO has 3 input nodes that inject 3 edges into the ring simultaneously. Each edge propagates as in a conventional RO; the period of each edge is the same, but the three edges are 120° phase shifted and overall frequency is boosted by 3×. However, the 3 edges independently accumulate jitter from thermal noise, causing an increasing variation of the pulse width between two neighboring edges with each completed cycle. Given time, two neighboring edges will eventually collapse, forcing the RO back to its nominal 1× frequency mode. The time to collapse reflects the accumulation of jitter and is used as the entropy source for random number generation. Process variation is inherently cancelled, since all 3 edges pass through the same RO stages. The design was fabricated in 28nm and 65nm and consistently passes all NIST randomness tests.

Figure 16.3.2 shows the TRNG consisting of 2 ROs, a counter, and control logic. A conventional RO (RO_REF) with ~2/3rd as many stages as the 3-edge RO (RO_RNG) acts as a reference for the phase frequency detector (PFD) to determine the edge collapse event. Since the frequency change is large (3×), a conventional digital implementation of the PFD is used, which enables a fully synthesizable design. To avoid setup and hold-time violations in the sampling registers, a glitch removal stage and 2b shift register is added. This ensures that a collapse event is flagged only after two consecutive pulses. A 14b cycle counter triggered by the 3-edge RO records the number of cycles until collapse. An intermediate counter bit, COUNT[3], is used to prevent false triggers in the first few cycles. Random number generation is initiated by a master clock, which is set sufficiently slow to ensure that the vast majority of collapse events (e.g. >90% in the tested design) complete within the active phase duration. The TRNG throughput is determined by the master clock frequency and the number of random bits harvested from each collapse event. The capture register reads the cycle counter when triggered by the PFD. As expected, the collapse cycle count displays a log-normal distribution (Fig. 16.3.5). To transform this into a uniform distribution, the collapse cycle counter is truncated, retaining the lower *p* bits, while the LSB is dropped to eliminate sensitivity to mismatch in the counter sampling flip-flop.

All hardware TRNGs must cope with interference from a potentially noisy environment as well as dedicated attacks. ROs are known to be sensitive to frequency injection, which can introduce errors in RO-based TRNGs [8]. The proposed TRNG uses accumulated jitter rather than jitter at a specific time point, making it more robust to noise injection. We tested the sensitivity to a deliberate attack with off-chip noise sources and also created on-chip test structures to inject and measure noise (Fig. 16.3.3). A programmable noise generator controlled by an on-chip VCO introduces substantial noise on the TRNGs supply, locking the oscillation and impacting collapse event time. To measure noise amplitude on-chip, an asynchronous clock samples the supply voltage, compares it with an external reference voltage, and increments a counter accordingly. With sufficient samples (2^{14} here) the noise amplitude can be determined from the counter value. In addition, an RC filter with a 210MHz corner frequency was designed to mitigate the impact of supply noise (Fig. 16.3.3).

The TRNG is evaluated using two test chips: one in 28nm CMOS with 8 different rings, the other in 65nm CMOS with 48 different TRNGs. The NIST Pub 800-22 RNG testing suite is used to evaluate the randomness of generated bits with 112Mb in total across 15 tests. Both 28nm and 65nm TRNGs pass all 15 NIST tests as shown in Fig. 16.3.4. Shorter rings with higher frequency collapse faster but have a narrower distribution, reducing the number of random bits obtained per cycle (i.e. they require higher truncation). Longer rings provide more random bits but overall throughput is limited by the slower master clock.

Using an RF signal generator, up to 600mV$_{pp}$ noise is injected on the power supplies (after removing PCB decoupling caps) to test TRNG robustness against off-chip attack. The 65nm TRNGs retain randomness up to 360mV$_{pp}$ noise without filter and up to the 600mV$_{pp}$ generator limit with filter. To compensate for filter IR drop, TRNGs with filters operate at 5% increased supply voltage, incurring a slight power penalty. Since ROs in 28nm TRNGs operate at a higher frequency they are less sensitive to external attack; even unfiltered versions did not suffer randomness degradation at the generator limit. EMI emitted by an antenna also did not cause failure in any randomness tests.

Figure 16.3.5 shows the impact of supply noise on TRNG performance using on-chip noise generation. Even though a deliberate attacker will not have access to such a noise source, this test can demonstrate how readily a 3-edge TRNG can be integrated with noisy circuits on an SoC. TRNGs showed sensitivity to supply noise at frequencies near 1× and 4× nominal RO frequencies, reducing collapse-time mean and variance. Randomness degrades at >125mV noise amplitude and 4× frequency without a filter, but is recovered using a filter. Denial of service occurs when a TRNG cannot generate outputs due to external an influence. This is observed only in unprotected TRNGs with on-chip noise at exactly 3× nominal frequency since the ring locks to its 3× frequency mode, preventing collapse. In this case, yield (the % of master cycles that generate outputs bits) drops to 7.37%. Generated bits remain random (passing all tests). Fig. 16.3.6 summarizes measurement results with comparisons to prior work. In 28nm, the TRNG generates random bits at 23.16Mb/s, while consuming 0.54mW and 375μm^2. Constructed entirely using a standard cell library and conventional place and route tools, this design presents a 'soft IP' TRNG that passes all NIST randomness tests without post processing.

Acknowledgments:
The authors acknowledge STMicroelectronics for IC fabrication support.

References:
[1] M. Bucci, *et al.*, "A High Speed Oscillator Based True Random Number Generator for Cryptographic Applications on a Smart Card IC," *IEEE Trans. Computers*, vol. 52, no. 4, pp. 403-409, 2003.
[2] C. Petrie, *et al.*, "A Noise-Based IC Random Number Generator for Applications in Cryptography," *IEEE Trans. Circuits and Systems-I*, vol. 47, no. 5, pp. 615-621, 2000.
[3] R. Brederlow, *et al.*, "A Low-Power True Random Number Generator using Random Telegraph Noise of Single Oxide Traps," *ISSCC Dig. Tech. Papers*, pp. 536-537, 2006.
[4] C. Tokunaga, *et al.*, "True Random Number Generator with a Metastability-Based Quality Control," *ISSCC Dig. Tech. Papers*, pp. 404-405, 2007.
[5] S. Mathew, *et al.*, "2.4Gbps, 7mW All-Digital PVT-variation Tolerant True Random Number Generator for 45nm CMOS High-Performance Microprocessors", *IEEE J. Solid-State Circuits*, vol. 47, no. 11, pp. 2807-2821, 2012.
[6] M. Matsumoto, *et al.*, "1200μm^2 Physical Random-Number Generators Based on SiN MOSFET for Secure Smart-Card Application," *ISSCC Dig. Tech. Papers*, pp. 414-415, 2008.
[7] N. Liu, *et al.*, "A true random number generator using time-dependent dielectric breakdown," *IEEE Symp. VLSI Circuits*, pp. 203-204, 2010.
[8] A. Markettos, *et al.*, "The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators," *CHES*, pp. 317-331, 2009.

 978-1-4799-0920-9/14/$31.00

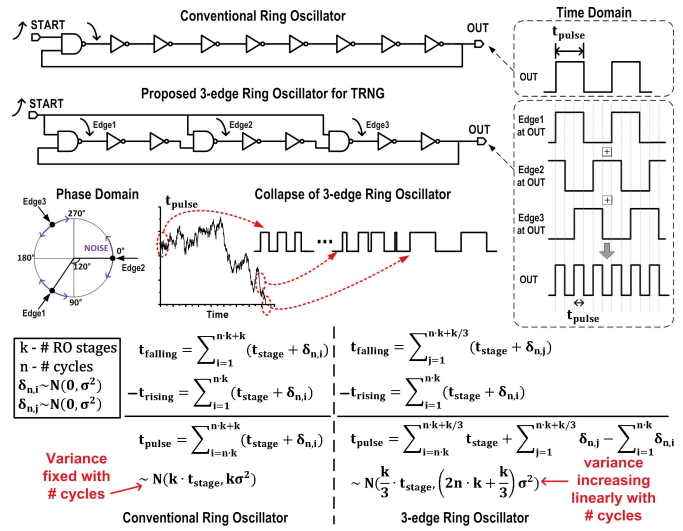


Figure 16.3.1: Frequency collapse in the 3-edge ring oscillator in time and phase domains.

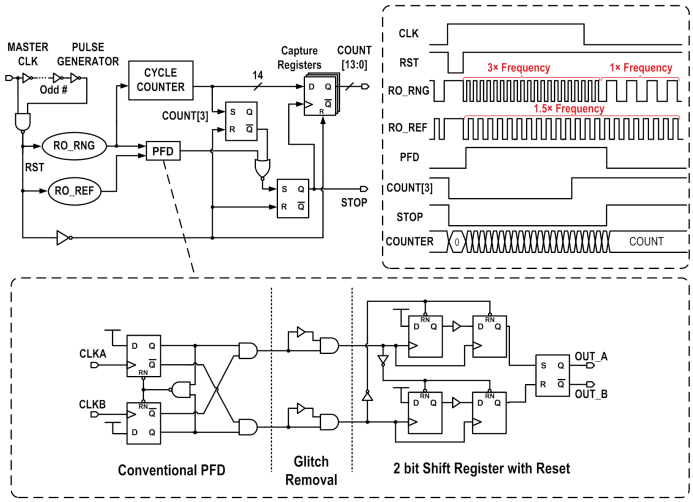


Figure 16.3.2: TRNG system block diagram and phase frequency detector (PFD) implementation.

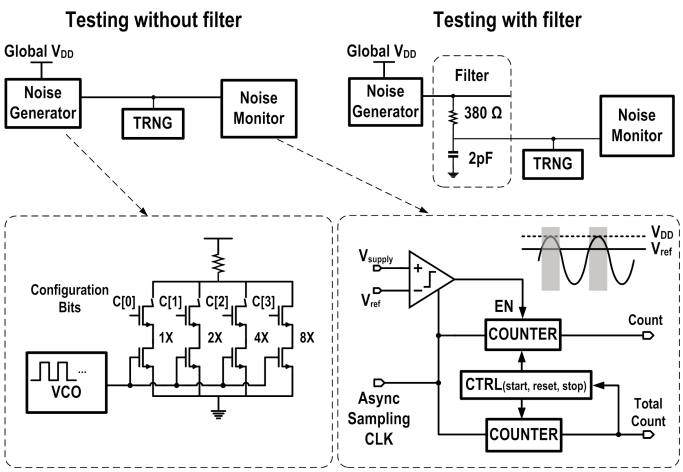


Figure 16.3.3: On-chip supply noise testing setups for protected and unprotected TRNGs.

NIST Pub 800-22, rev. 1a, 2010 Randomness Tests	65nm, 21 stage RO, 0.9V, 2.80Mb/s		28nm, 21 stage RO, 0.9V, 23.16Mb/s	
	P-value χ^2	Pass Rate	P-value χ^2	Pass Rate
Frequency	0.785562	296/300	0.872947	297/300
Block Frequency	0.082177	297/300	0.746572	297/300
Cumulativ Sum	0.462245	294/300	0.955835	296/300
Cumulativ Sum	0.942895	295/300	0.329332	294/300
Runs	0.220931	296/300	0.574903	297/300
Longest Runs	0.329332	296/300	0.81047	298/300
Matrix Rank	0.046668	294/300	0.000682	296/300
FFT	0.03013	295/300	0.224821	295/300
Non Overlapping Template	PASS*	PASS*	PASS*	PASS*
Overlapping Template	0.878107	297/300	0.329332	296/300
Linear Complexity	0.487885	297/300	0.304126	295/300
Universal	0.935716	98/100	0.719747	99/100
Random Excursions	PASS*	PASS*	PASS*	PASS*
Random Excursions Variant	PASS*	PASS*	PASS*	PASS*
Approximate Entropy	0.514124	100/100	0.275709	100/100
Serial	0.304126	99/100	0.897763	99/100
Serial	0.867692	99/100	0.595549	100/100

* "PASS" means all sub tests pass minimum requirement.
** Minimum p-value χ^2 is 0.0001. Minimum pass rate is 291/300 for first 10 tests (using 300 × 40K bits) and 96/100 for the other 5 tests (using 100 × 1M bits).

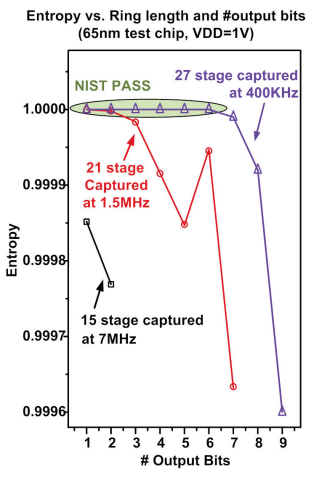


Figure 16.3.4: Measured NIST randomness test results and impacts of RO length and the number of harvested random bits on output data entropy.

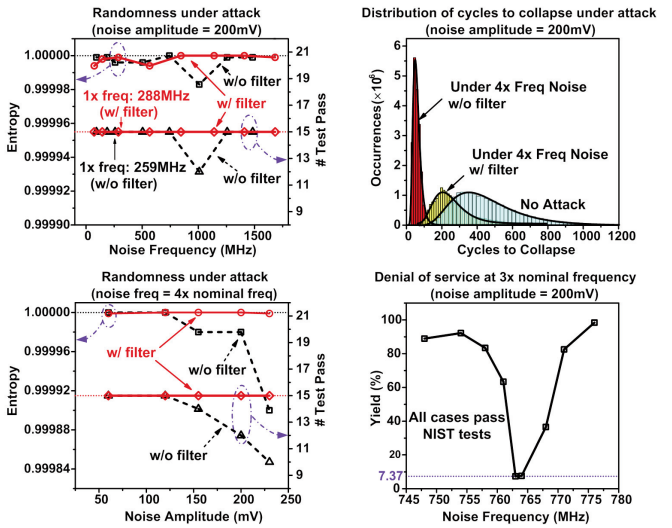


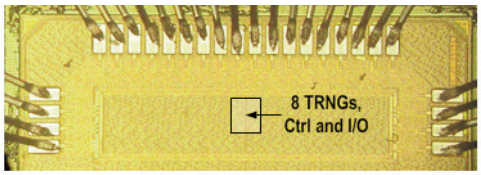
Figure 16.3.5: Measured impacts of on-chip noise frequency and amplitude on randomness of protected and unprotected TRNGs (65nm, 21-stage RO TRNG).

	This work (25°C, 0.9V core supply)		JSSC' 12 [5]	VLSI' 11 [7]	ISSCC' 08 [6]	ISSCC' 07 [4]	ISSCC' 06 [3]	Trans. Computers' 03 [1]
Technology	28nm	65nm	45nm	65nm	0.25μm	0.13μm	0.12μm	0.18μm
Entropy Source	Jitter in 3-edge RO		Metas-tability	Oxide breakdown	SiN MOS-FET Noise	Metas-tability	Metas-tability	Oscillator jitter
Bit Rate (Mb/s)	23.16	2.8	2400	0.011	2	0.2	0.2	10
NIST Pass	All	All	All	All	not reported[b]	5	not reported	not reported[b]
TRNG Core Area (μm²)	375	960 (1080[a])	4004	1200	1200	36300	9000	16000
Power (mW)	0.54	0.159	7	2	1.9	1	0.05	2.3
Efficiency (nJ/bit)	0.023	0.057	0.0029	181.81	0.95	5	0.25	0.23
Post Processing	No	No	No	No	Yes	No	Yes	no
Resistance to Attack	Yes	Yes	Not reported	Not reported	Not reported	Not reported	Not reported	No[c]

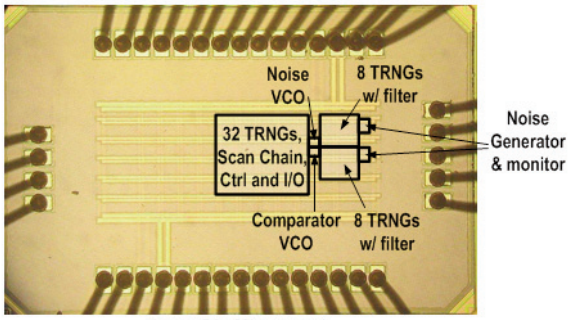
[a] Including 1/8th of filter area (MIM cap and poly resistor); 1 filter is shared by 8 TRNGs and MIM cap is placed above TRNGs.
[b] NIST FIPS 140-2 test result is provided, which is older, less rigorous than NIST Pub 800-22 with 4 tests and only 20,000 bits required.
[c] Commercial TRNG based on similar RO approach is successfully attacked in [8].

Figure 16.3.6: Summary of measurement results and a comparison with state-of-the-art hardware TRNG designs.

16



28nm Die Micrograph



65nm Die Micrograph

Figure 16.3.7: Die micrographs of 28nm and 65nm TRNG test chips.

978-1-4799-0920-9/14/$31.00