True Random Number Generator Circuits Based on Single- and Multi-Phase Beat Frequency Detection

Qianying Tang, Bongjin Kim, Yingjie Lao, Keshab K. Parhi, and Chris H. Kim
University of Minnesota, Minneapolis, MN 55455 USA

Abstract- **A fully-digital True Random Number Generator (TRNG) measures the frequency difference between two free-running ring oscillators, or in other words the beat frequency, to extract random frequency jitter. For generating a continuous stream of random bits with a high entropy level, the lower significant bits meeting the NIST randomness criteria are concatenated. The generation efficiency is further improved by utilizing a multi-phase structure. The proposed circuit fabricated in 65nm achieves an energy efficiency of 15.1Mb/mW at 0.8V. Experimental data collected from eight TRNG test chips passed all 15 NIST tests without the use of any feedback or tracking scheme.**

I. INTRODUCTION

True Random Number Generators (TRNGs) are used for authentication and encryption purposes in systems requiring a high level of security. On-chip TRNGs typically harvest randomness from a circuit that converts transistor level noise such as thermal noise, flicker noise, or random telegraph noise (RTN) [1-4] into a voltage or delay signal. For example, a popular type of TRNG utilizes an inverter pair that is initialized to a metastable state to amplify the thermal noise [2,3]. A recent work of metastability based TRNG features the time variation for a non-conventional oscillator circuit collapse from unstable state to stablized state [4]. Conventional delay based TRNGs employ oscillator circuits that are highly sensitive to device noise so that sufficient randomness can be achieved within a short sampling period. However, these schemes involve extensive analog components for amplifying the device noise and coupling it to the oscillator's bias voltage, making them less amenable to product level integration [5]. In this work, we demonstrate a fully-digital TRNG circuit based on standard digital logic in which the subtle frequency difference between two identical free-running ROSCs is measured using standard digital logic.

II. PROPOSED BEAT FREQUENCY BASED TRNG

The basic concept for capturing the frequency difference between two ROSCs is illustrated in Fig. 1 [6]. The faster signal A passes, catches up and overtakes the slower signal B repeatedly at intervals determined by the frequency differences of the two ROSCs, namely the beat frequency or Δf. This pattern is recorded by a standard D-flip-flop where the output of ROSC A is continuously sampled by that of ROSC B. The counter output (N in Fig. 1) increments every ROSC period until it reaches the beat frequency interval after which the count is sampled and reset. For better illustration, let's consider an example in which the average frequency difference between the ROSC pair is 1% and the maximum frequency difference due to random jitter is 0.01%. Under this condition, the average counter output is 100 while the maximum and minimum counts are 101 and 99, respectively. In this scenario, we can take the least significant bit (LSB) of the output count as the TRNG output. Now suppose the average frequency difference is reduced to 0.5% by adjusting the frequency difference, while the random jitter remains the same at 0.01%. Then, the output count will fluctuate between 196 and 204, thereby providing up to three random bits (1st, 2nd, and 3rd LSBs) per output count and at the same time increasing the randomness of the lower bits. By making the frequencies even closer using fine grain trimming circuits, we could generate more random bits from a larger count at the expense of a longer sampling time.

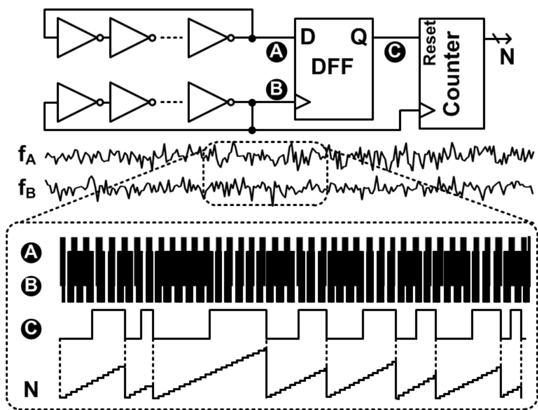

Fig. 1. Basic principle of the proposed beat frequency based TRNG circuit.

	Conventional Metastability TRNG [3]	This Work
Schematic	Digitizer; Fine and Coarse Tuning	D Q; Counter
Description	Inverter pair driven to metastable state	Beat frequency (i.e. Δf) detection
Calibration	Continuous monitoring and calibrating required	One-time calibration during initial start up
Output Sensitivity (VDD=0.8~1.2V, pre-calibration)	P(0)=33-49%	P(0)=50.0-50.0% (1st LSB) P(0)=49.9-50.0% (2nd LSB)
Area	Large overhead for compensation scheme	Small (no feedback or compensation scheme)

Fig. 2. Comparison between conventional and proposed designs.

Fig. 2 compares the proposed work with the conventional TRNG based on a cross-coupled inverter pair. In this previous design, the two output nodes of the inverter pairs are initialized to the same voltage. The switches are then turned off causing the outputs to resolve to either '1' or '0' depending on the random device noise. The main drawback of this circuit

is that the meta-stable point is extremely sensitive to the inverter pair's voltage offset. More specifically, it has been shown that randomness can only be guaranteed when the voltage offset is below $\pm 0.24\sigma_{noise}$. Here, σ_{noise} is the standard deviation of the noise [3]. In contrast, the proposed beat frequency detection scheme can produce LSBs with good randomness for an average frequency difference corresponding to up to $5.0\sigma_{noise}$, making it more tolerant under process skew. Furthermore, unless a tracking loop is used for de-biasing the random bits, the previous design suffers from a large drop in the output '0' probability (i.e. 49% to 33%) as the supply voltage is increased from 0.8V to 1.2V. The proposed beat frequency detection scheme, on the other hand, provides good randomness for the 1st and 2nd LSBs with only a 0.1% drop in that probability (see Fig. 2). This allows the proposed circuit to operate reliably without a compensation loop, enabling a simpler TRNG design with a smaller area and lower power consumption.

III. TRNG Test Chip Design and Measured Data

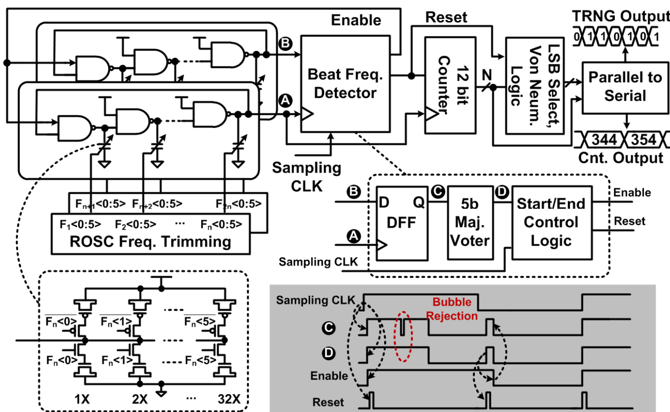

Fig. 3. TRNG circuit with trimming caps and power saving mode.

A 65nm test chip was designed to experimentally verify the proposed TRNG circuit. A block diagram of the main circuit blocks is shown in Fig. 3. A trimming capacitor bank is connected to each ROSC stage for tuning the initial frequencies of the two ROSCS to ensure beat frequency counts are in the desired range. A 5 bit majority voter circuit is used in the beat frequency detector to prevent functional errors due to logic bubbles (e.g. lone 0 in a string of 1). This may occur when the two ROSC signal edges are about to cross each other. To reduce unnecessary switching power consumption, a start/end control logic is implemented to automatically shut down the ROSCs once the beat frequency has been successfully sampled. Finally, the lower LSBs are serialized to produce the final TRNG output bit stream.

A. Serializing Random Bits

Fig. 4 shows the measured beat frequency count under different trimming capacitor settings. The average count increases from 191 to 3040 as the ROSC frequencies are brought closer together. Injection locking between the two ROSCs was not observed in any of the tests owing to the good isolation between the two ROSCs. This can be attributed to the modest amount of decoupling capacitors placed between the ROSCs as can be seen in the layout diagram in Fig. 16. Fig. 5 shows that for an average count of 352, the percentage of 1's and 0's are almost equal for the first 4 LSBs, implying good randomness for these bits. Fig. 6 illustrates the procedure for generating the final random bit sequence from the measured beat frequency counts. The first 3 LSBs can be directly concatenated and streamed out without any post-processing. Although the 4th LSB appears to be unbiased, NIST test results in Fig. 7 reveal that further de-biasing is necessary. To improve the throughput, von Neumann correction is applied on 4th LSB as shown in Fig. 6. This popular algorithm takes two consecutive bits from the original data and encodes '01' into an output '0' and '10' into an output '1'. The two other combinations (i.e. '00' and '11') are simply dropped. In our implementation, a group of four 4th LSBs from the original sequence generates a single corrected output bit that is buffered and inserted into the final bit sequence. The efficiency is increased from 3 bits per count to 3.25 bits per count using the von Neumann method with almost no additional power consumption.

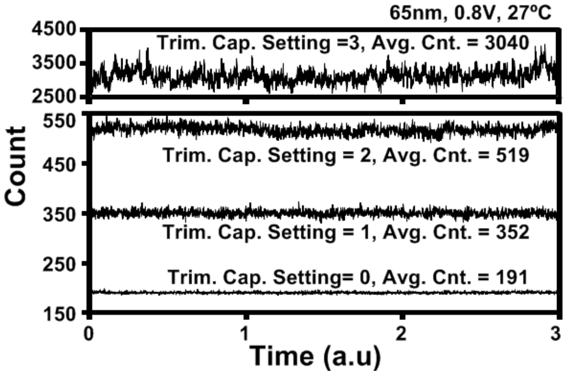

Fig. 4. Measured beat frequency count for different trim capacitor settings.

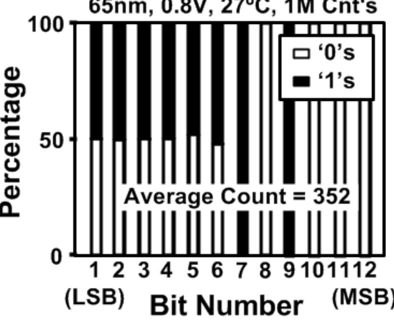

Fig. 5. Percentage of '1's and '0's for each bit of the beat frequency count output. The lower significant bits (e.g. bits 1, 2, 3) have better randomness compared to the higher bits.

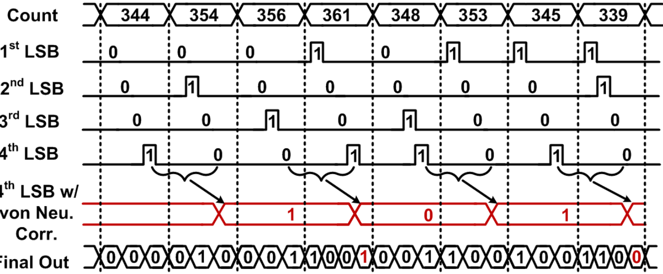

Fig. 6. Concatenating LSBs to generate the final TRNG output bit stream. 4th LSB can be used after von Neumann correction.

B. NIST Randomness Test Result

NIST test results performed using measured data from the proposed TRNG are summarized in Fig. 7. For a beat frequency output with an average count of 352, the first 3 LSBs passed all 15 NIST tests (P-value χ^2 >0.01, Proportion>0.949751) without requiring any post-processing steps. The final sequence with the insertion of the 4th LSB after von Neumann correct also passed all NIST tests.

	1st LSB		2nd LSB		3rd LSB		4th LSB		**Final Output	
P-Val / Proportion	P-Val	Prop.	P-Val	Prop.	P-Val	Prop.	P-Val	Prop.	P-Val	Prop.
Frequency	0.679	0.9818	0.091	0.9818	0.514	1.0000	Fail	Fail	0.514	1.0000
Block Frequency	0.130	1.0000	0.760	1.0000	0.063	0.9818	Fail	Fail	0.946	0.9818
*Cumulative Sums	0.554	0.9818	0.367	0.9818	0.475	1.0000	Fail	Fail	0.437	1.0000
Runs	0.596	1.0000	0.182	1.0000	0.225	0.9818	Fail	Fail	0.720	1.0000
Longest Run	0.049	0.9818	0.760	0.9818	0.596	1.0000	Fail	Fail	0.475	1.0000
Rank	0.305	0.9818	0.335	0.9636	0.305	1.0000	0.596	0.9636	0.055	0.9636
FFT	0.305	1.0000	0.010	1.0000	0.514	0.9818	Fail	Fail	0.103	1.0000
*Nonoverlapping Temp.	0.437	1.0000	0.596	1.0000	0.679	1.0000	Fail	Fail	0.679	1.0000
Overlapping Template	0.249	0.9818	0.249	1.0000	0.798	0.9818	Fail	Fail	0.182	0.9818
Universal	0.868	1.0000	0.475	0.9818	0.071	1.0000	Fail	Fail	0.063	1.0000
Approximate Entropy	0.554	1.0000	0.043	1.0000	0.103	1.0000	Fail	Fail	0.600	1.0000
*Random Excursions	0.672	1.0000	0.740	1.0000	0.500	1.0000	Fail	Fail	0.637	1.0000
*Rand. Excursions Var.	0.740	1.0000	0.602	1.0000	0.637	0.9679	Fail	Fail	0.876	1.0000
Serial	0.637	1.0000	0.401	1.0000	0.637	0.9818	Fail	Fail	0.304	0.9818
Linear Compelxity	0.401	1.0000	0.072	0.9818	0.063	0.9818	0.163	0.9818	0.868	0.9636

** Tests with 2 or more subtest, P-val and Prop shown here are the smaller or median values*
*** Concatenate 1st~3rd LSBs and 4th LSB after von Neumann correction ***Avg. count = 352*

Fig. 7. NIST test results for 1st~4th LSB and final bit sequence.

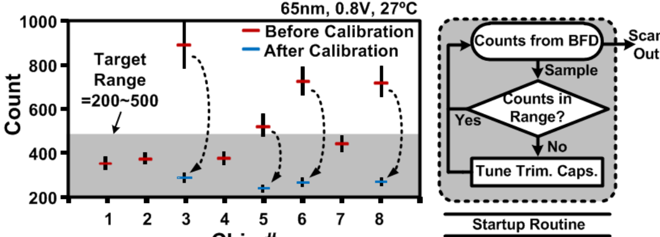

Fig. 8. One-time calibration of average count during start up.

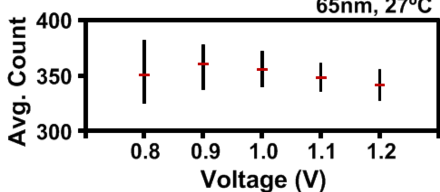

Fig. 9. Measured count under different voltages.

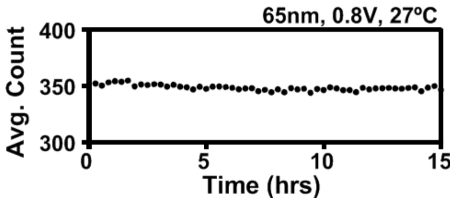

Fig. 10. Stability under continuous operation.

C. TRNG Robustness

The initial count measured from different chips ranges from 200 to 1000 when using the same trimming capacitor setting. Through extensive testing, we found that a count range of 200 to 500 provides a reasonable trade-off between speed and bit efficiency. This count range corresponds to a ROSC frequency difference of 0.5% to 0.2%, respectively. A simple one-time calibration step shown in Fig. 8 can be used to guarantee that the initial count is in the desired range (200 to 500) across the different TRNG chips. This can be readily achieved within a few beat frequency periods using minimal hardware overhead during the initial startup. The measured count values are relatively consistent for a supply voltage range of 0.8V to 1.2V as shown in Fig. 9 suggesting a wide operation range and good tolerance against environmental effects such as supply voltage and temperature variation. The slightly wider count range at 0.8V can be attributed to the larger device noise and higher delay sensitivity. Stability of average count was verified through a continuous 15 hour operation test (Fig. 10).

IV. Simulation and Modeling

For better insight into the beat frequency based TRNG circuit, Monte Carlo simulations were performed using a statistical delay model. Here, the oscillation periods of the two ROSC circuits were formulated as independent Gaussian random variables $N(\mu_A, \sigma_A^2)$ and $N(\mu_A, \sigma_A^2)$. Standard deviations of the ROSC periods (σ_A and σ_B) are assumed to be identical since intrinsic device noise under a given operating condition shows the same characteristics. The average values of the two ROSC periods (μ_A and μ_B) on the other hand, can be tuned during initial startup using different trimming capacitor settings for a desired beat frequency count N. We can estimate the average period values based on the measurement results as shown in Fig. 11. Simulation results from our model using fitting parameters μ_B-μ_A = 0.0028 and σ_A=σ_B=0.0006 show excellent agreement with the measured data.

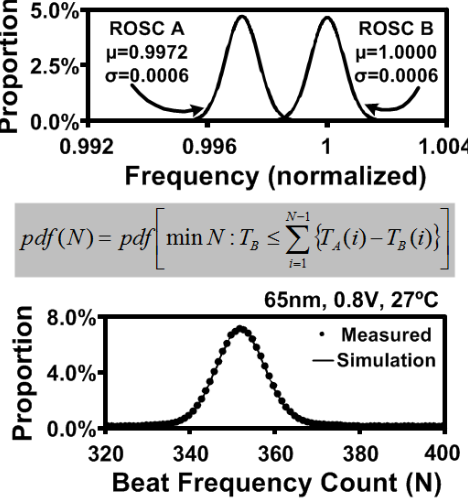

Fig. 11. (Upper) Individual ROSC frequency distributions estimated using statistical model and measured data. (Lower) Measured count distribution shows good agreement with simulated data.

V. Multi-phase Implementation

A multi-phase TRNG capable of sampling the beat frequency from each ROSC stage was implemented in another 65nm test chip. This new design can maximize the number of random bits generated from a single ROSC pair without increasing the measurement time. The simplified block diagram of the multi-phase TRNG is illustrated in Fig. 12. As

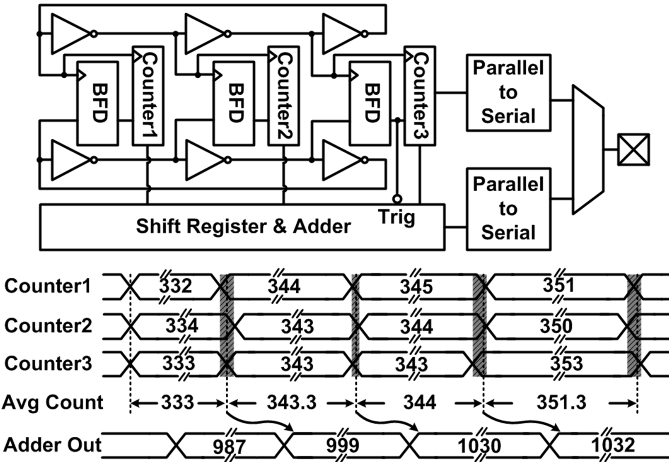

Fig. 12. Multi-phase TRNG implementation (3 phase example). The number of LSBs with good randomness increases under the same sampling time as compared to the single-phase version.

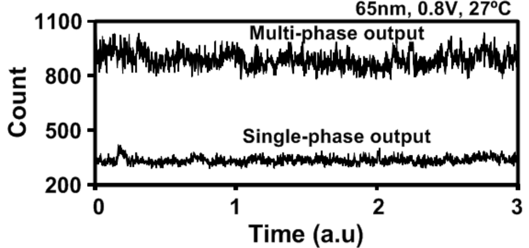

Fig. 13. Measured count output from single-phase and multi-phase TRNGs

	3 stage ROSC		31 stage ROSC	
	Single phase	Multi phase	Single phase	Multi phase
# of bits passing NIST	2	3	3	8
Efficiency (Mbits/mW)	13.341	15.114	2.0342	3.176

Fig. 14. The number of random bits per output that passes all NIST test as well as the TRNG generation efficiency improves using the proposed multi-phase structure.

shown in the figure, beat frequency detectors in each ROSC stage sample the frequency difference between the top and bottom ROSCs. Under an ideal condition where no device noise is present, the ROSC signal is simply delayed from one stage to the next by a fixed amount. The multi-phase design in this case does not provide any benefit over the single-phase version as the beat frequency measured from each stage will be identical. In the presence of device noise however, each ROSC stage will introduce a slightly different delay and hence each beat frequency count will be different. This noise effect can be captured using simple logic blocks to increase the number of random bits. The counter values are stored in the shift registers and summed up together during the subsequent beat frequency period (i.e. falling edge of next beat signal). Fig. 13 compares the measured beat frequency counts from a single-phase and multi-phase TRNG implemented in the same test chip. A larger fluctuation in the count value can be observed for the multi-phase design. Therefore, for the same sampling period, the multi-phase TRNG can provide a higher number of random bits that pass all NIST tests. The number of additional random bits obtained from a multi-phase TRNG has a logarithmic dependency on the number of phases. For example, as shown in Fig. 14, a multi-phase TRNG using a 3 stage ROSC generates one more random bit while five more bits are generated using a 31 stage ROSC. Even though the power consumption slightly increases due to the extra beat frequency detectors, the overall efficiency still increases due to the improved throughput. Fig. 15 compares the TRNG performance measured from various single-phase and multi-phase TRNG circuits. A TRNG with fewer ROSC stages achieves a higher bit rate which can be attributed to the higher ROSC frequency. As a result, the TRNG efficiency increases from 2.2 Mbits/mW to 15.1 Mbits/mW as the number of ROSC stages is reduced from 31 to 3. Die microphotographs of the two TRNG test chips are shown in Fig. 16.

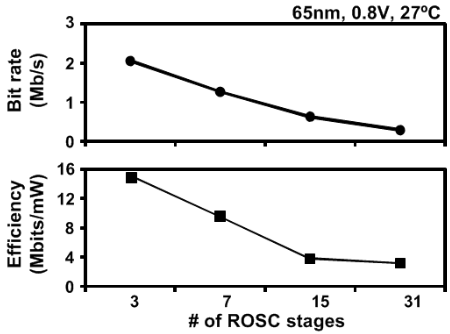

Fig. 15. Bit rate and efficiency vs. # of ROSC stage in TRNG.

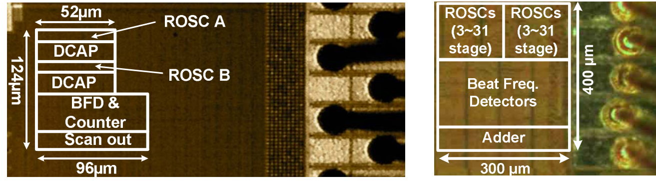

Fig. 16. Single-phase (left) and multi-phase (right) TRNG chips in 65nm.

VI. Conclusion

ROSC based TRNG circuits utilizing a novel beat frequency detection technique have been demonstrated in two 65nm test chips. The random bits generated using the proposed circuit pass all 15 NIST tests under a wide supply voltage range without any feedback scheme. Long-term (>15 hours) tests were performed to confirm good TRNG output under continuous operation. A one-time calibration scheme ensures that ROSC frequency mismatch across different chips is cancelled out. To further improve the efficiency, a multi-phase TRNG was demonstrated that captures phase noise in each ROSC stage. Experimental data shows a TRNG efficiency of 15.1Mbits/mW for a 3 stage multi-phase design.

[1] R. Brederlow, et al., “A Low-Power True Random Number Generator using Random Telegraph Noise of Single Oxide-Traps,” ISSCC, Feb. 2006. [2] C. Tokunaga, et al., “True Random Number Generator With a Metastability-Based Quality Control,” JSSC, Jan. 2008. [3] S. Srinivasan, et al., “2.4GHz 7mW All-Digital PVT-Variation Tolerant True Random Number Generator in 45nm CMOS,” VLSI Symp. Jun. 2010. [4] K. Yang, et al., “A 23Mb/s 23pJ/b Fully Synthesized True-Random-Number Generator in 28nm and 65nm CMOS,” ISSCC, Feb. 2014.[5] M. Bucci, et al., “A High-Speed Oscillator-Based Truly Random Number Source for Cryptographic Applications on a Smart Card IC,” IEEE Tran. on Computers, Apr. 2003. [6] T. Kim, et al., “Silicon Odometer: An On-Chip Reliability Monitor for Measuring Frequency Degradation of Digital Circuits", JSSC, Apr. 2008.