22.4 True Random Number Generator with a Metastability-Based Quality Control

Carlos Tokunaga, David Blaauw, Trevor Mudge

University of Michigan, Ann Arbor, MI

True random number generators (tRNG) use a physical source of randomness such as thermal noise, or telegraph noise to generate a random bit stream. However, they are sensitive to undesired deterministic noise, such as supply noise, process variations or deliberate attacks. In this paper, we introduce a metastability-based tRNG that is able to counteract such deterministic events and to qualify the output stream according to the actual randomness of the system.

A number of tRNG methods are presented [1,2] that use a so-called von Neumann corrector to eliminate long runs of 0s and 1s. However, such a corrector can only mask the fact that the initial bit stream is compromised and is unable to restore true randomness. The method in [3] uses metastability to amplify thermal noise, employs an XOR corrector and controls the metastable operation by biasing the system to generate equal number of 0s and 1s. However, this makes the system prone to generating correlated streams, such as alternating streams of 0s and 1s, which actually lack randomness.

The innovation of the proposed tRNG method is that control of the metastable operation is performed without observing the generated output bits. Instead, the resolution time of each metastable event is recorded, (regardless of the 0,1 outcome), which allows the system to determine the original noise level at the time of metastability and the randomness of the event. This allows the control to grade the quality of the output bits and to tune the system for maximum randomness. Furthermore, this method allows the user to tradeoff the quality of the bit stream with the bit production rate. The fully integrated tRNG is fabricated in a 0.13μm process in 0.036mm^2 and consumes 1mW. The metastability events take 20ns but the chip is operated at a bit production rate of 200kb/s due to external timing constraints. The generated bit streams achieve high entropy and pass NIST randomness tests without the aid of a corrector.

The proposed tRNG uses a latch operating near the metastable state where the final state is upset by thermal noise of the devices, giving rise to random output values. However, if the initial latch voltages are not at the exact metastable point, due to mismatch or external noise, the latch will have a deterministic output value. The key observation of our method is that the randomness of a metastable event can be determined by measuring the time it takes the latch output to resolve. The resolution time is modeled as $t_d = \tau_r \cdot \ln (K_f / \Delta V_i)$, where τ_r and K_f are device- and circuit-dependent constants and ΔV_i is the initial voltage difference from the metastable point. ΔV_i has two components: a deterministic voltage difference ΔV_d (e.g., external noise, power supply noise) and the thermal random noise V_n, $\Delta V_i = \Delta V_d + V_n$. By observing t_d, it is therefore possible to compute the original voltage differential ΔV_i. Given that the thermal noise in MOS semiconductor devices can be modeled as a normal random variable with zero mean and variance $\sigma^2 = 4kT\gamma g_m \Delta f$ [4], the probability that the final metastable outcome is dictated by thermal noise can be computed. This is illustrated in Fig. 22.4.1 where sets of simulations of a metastable system are performed for different values of ΔV_d. In each individual metastable event simulation, the magnitudes of ΔV_d and V_n are compared to establish which determined the final output resolution. When $\Delta V_d >> V_n$, the probability of random bit flips is low because the system is dominated by the deterministic noise and hence, the mean and variance of $\overline{t}_d$ (t_d and σt_d) are small. As ΔV_d is reduced, the probability of random outcomes, as well as $\overline{t_d}$ and σt_d, increases as the system becomes dominated by thermal noise. It is therefore possible to tune a latch to metastable operation by evaluating the statistics of t_d. In addition, the t_d values of *individual* metastability events can be used to filter the output stream when $\Delta V_d \approx V_n$. Increasing the t_d filtering threshold results in a higher probability of random bit flips at the expense of a reduced bit-production rate.

The control and grading system is shown in Fig. 22.4.2 and consists of two elements: cycle-to-cycle generation of output bits by the latch, which are graded and stored in memory, and calculation of resolution time statistics used in metastability control. The metastability latch, shown in Fig. 22.4.3, is reset by collapsing the supplies to half V_{dd} and equalizing the output nodes by asserting the *EQ*, *Bias* and *Start* signals. Following this, charge is induced on node *q* by the control module that tunes the latch into metastability. The charge-injection circuit consists of a capacitive coupling array ranging in value from 0.25 to 100fF, allowing the voltage on node *q* to be varied by 16mV with a resolution of 10μV. However, it is found in silicon that with a 120μV control resolution, the latch is brought into sufficiently metastable operation to obtain qualified random outputs when using t_d based filtering. After charge injection, the latch is activated by restoring the supplies to full V_{dd} and asserting *Start*. The latch output then resolves to its final state and the *Stop* signal is generated using a pair of complementary comparators as illustrated in Fig. 22.4.4.

A time-to-digital converter (TDC) is used to determine t_d (Fig. 22.4.3). It is composed of two parts: a fine counter that has a resolution of 50ps and a coarse counter that extends the range of the TDC to 20ns. The fine counter contains an array of flip-flops clocked by delayed versions of the *Start* signal that sample in discrete times the *Stop* signal producing a thermometer code.

To tune the latch into metastability, the control algorithm maximizes the mean value of t_d. Fig. 22.4.5 shows the measured distributions of t_d and the associated value of $\overline{t}_d$ for sets of 128 samples as the injected charge is swept. As expected, biasing the system below or above the metastability point (which fell at ~604.1mV) results in a small $\overline{t}_d$ and σt_d values and a biased bit stream of all 0s or 1s. As the system approaches metastability, $\overline{t}_d$ increases rapidly allowing for excellent control feedback. In addition, the spread of t_d also increases, as shown in the distribution plots, and the percentage of 0s and 1s in the output stream reaches 50%. The statistical behavior of t_d also tracks well with temperature for a measured range of 10 to 60°C.

Figure 22.4.6 shows the tuning algorithm operation for a fabricated die. The system locks into metastable operation in iterations 65 to 75 and then readjusts when the system is affected by power-supply noise in iterations 75 to 85. After the tRNG is tuned into metastable operation, the bits in the output stream are filtered based on their individual t_d values. Increasing the filtering threshold from 75 to 96 TDC-units results in a lower output bit rate while significantly increasing the entropy of the bit stream, confirming that metastable events with a longer resolution time have a higher probability that the bit was generated by random noise. As a result, the output bit stream was able to pass NIST [5] randomness tests without the use of a corrector using an efficiency of 40%, as shown in Fig. 22.4.6.

References:

[1] R. Brederlow, R. Prakash, C. Paulus, R. Thewes, “A Low-Power True Random Number Generator Using the Random Telegraph Noise of Single Oxide-Traps,” *ISSCC Dig. Tech. Papers*, pp. 536-537, Feb., 2006.

[2] B. Jun and P. Krocher, “The Intel Random Number Generator,” White Paper, http://www.cryptography.com/intelRNG.pdf, 1999.

[3] D. Kinniment and E. Chester, “Design of an On-Chip Random Number Generator using Metastability,” *Proc. European Solid-State Circuit Conf.*, pp. 595-598, Sep., 2002.

[4] P. Gray, P. Hurst, S. Lewis, R. Meyer, Analysis and Design of Analog Integrated Circuits, 4th Ed., pp. 759, John Wiley & Sons, Inc., 2000.

[5] National Institute of Standards and Technology, “A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications,” Pub 800-22, 2001.

1-4244-0852-0/07/$25.00 ©2007 IEEE.

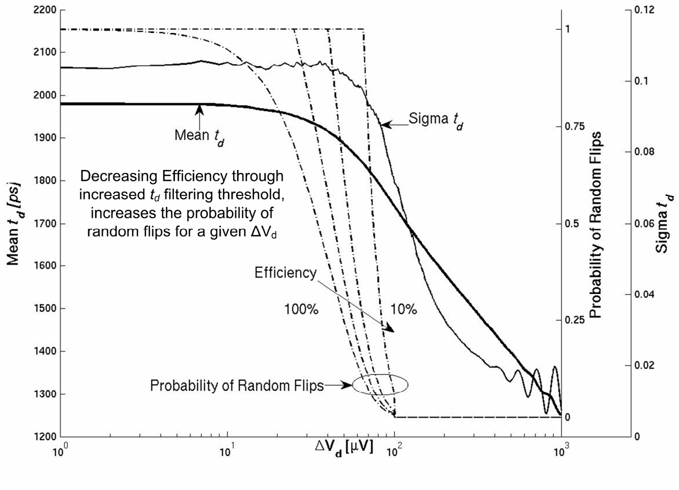


Figure 22.4.1: Statistical properties of the metastable resolution time t_d.

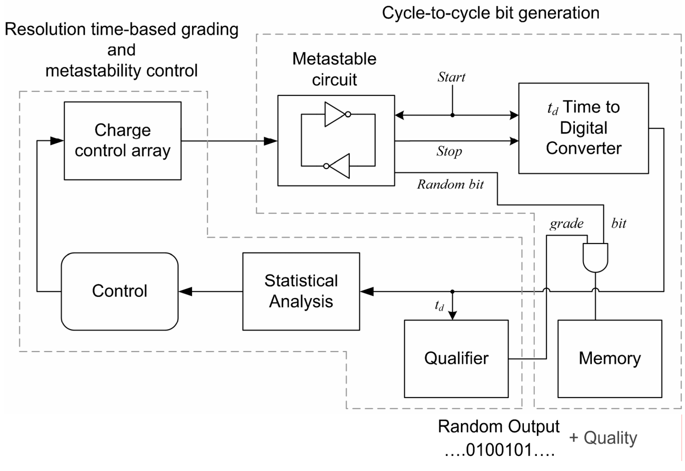


Figure 22.4.2: tRNG system block diagram.

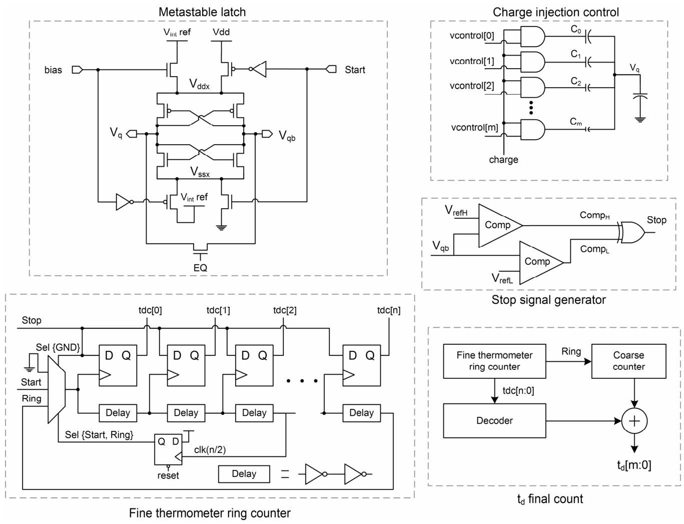


Figure 22.4.3: Metastable latch, Stop and TDC circuits.

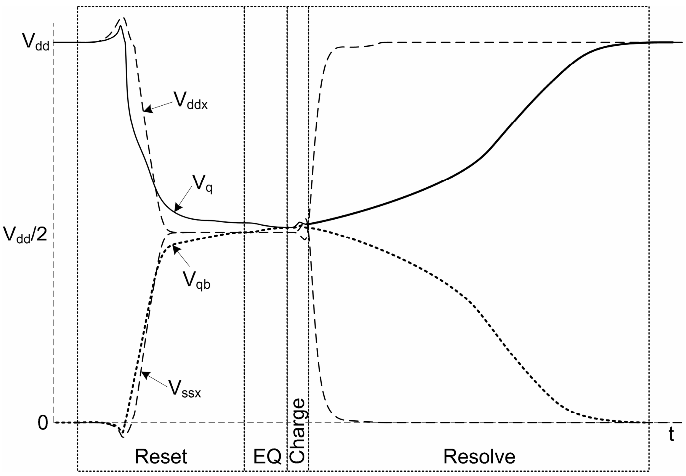


Figure 22.4.4: Simulation of a random bit generation cycle.

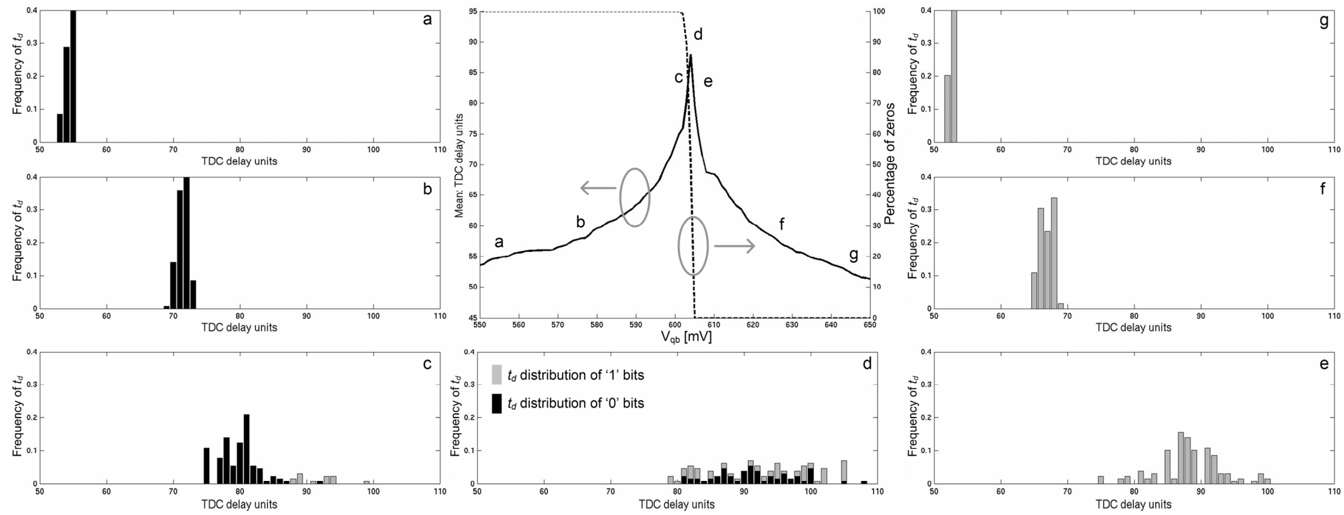
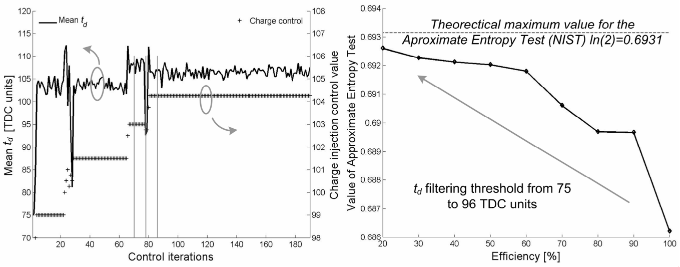


Figure 22.4.5: Measured statistics of t_d and random bit distributions.

Continued on Page 611



Efficiency	Random NIST Tests				
	Frequency	Block Frequency	Cumulative Sums	Runs	FFT
100%	fail	pass	fail	fail	pass
90%	fail	pass	pass	fail	pass
80%	fail	pass	fail	fail	pass
70%	fail	pass	fail	fail	pass
60%	pass	pass	pass	fail	pass
50%	pass	pass	pass	fail	pass
40%	pass	pass	pass	pass	pass
30%	pass	pass	pass	pass	pass
20%	pass	pass	pass	pass	pass

Figure 22.4.6: Metastability control, and randomness test results.

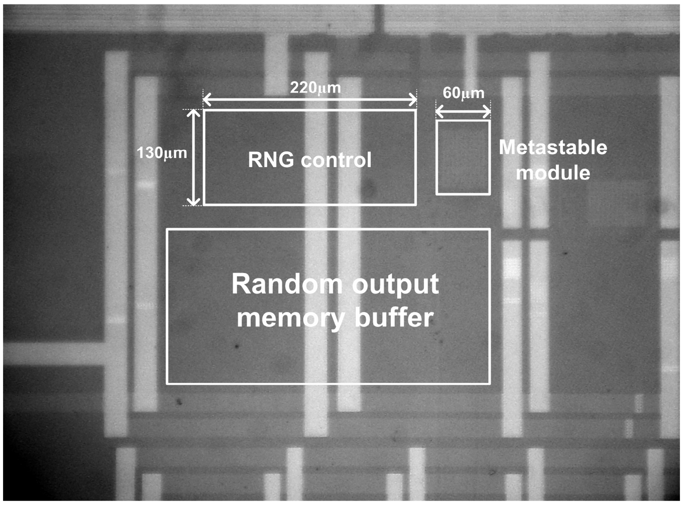


Figure 22.4.7: Die micrograph of tRNG with 8kb SRAM.