2023 18th Conference on Ph.D Research in Microelectronics and Electronics (PRIME) | 979-8-3503-0320-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/PRIME58259.2023.10161842

Design Space Exploration of TRNG Latches for Improved Entropy and Efficiency

Samuel Ellicott, Michael Kines, Waleed Khalil
Department of Electrical and Computer Engineering
Ohio State University
Columbus, Ohio
ellicott.4@osu.edu, kines.1@osu.edu, khalil.18@osu.edu

***Abstract*—True Random Number Generators (TRNGs) are a key building block in cryptography. In order to obtain random outputs, the TRNG must produce sufficient noise such that the probability of overcoming any offsets caused by on-die variations between devices, which are inescapable in CMOS processes, is high. In this paper, we analyze the metastable latch based TRNG design with regards to relative device strength, type, and size to determine the tradeoffs in robustness to offsets, bit-rate, and power.**

***Index Terms*—True Random Number Generator (TRNG), entropy, random noise, metastability**

I. Introduction

Data encryption and internet security relies on the generation digital true random bit streams for algorithms. With the proliferation of Internet-of-Things (IoT) devices, there exists a need for efficient generation of random numbers for battery powered or energy harvesting systems. These random number generators must produce a sequence of digital bits which, on average, have equal number of 1's and 0's. Additionally, each bit in the sequence should not be influenced by any preceding outputs. Furthermore, for the design to be robust, the statistics of the TRNG output must maintain this behavior over process, voltage, and temperature (PVT) variations. TRNGs are evaluated for the performance metrics of bit-rate and power; typically using energy/bit at a particular bit-rate as a figure-of-merit. It is desirable for the energy/bit to be low and the bit-rate to be high.

The purpose of this paper is to present an evaluation of the tradeoffs made when designing a latch for a TRNG. This study is deemed necessary, since the majority of prior work has not taken into account the impact of device sizing and/or type on the TRNG performance [1]–[3]. The remainder of the paper is organized as follows. Section II provides background information on the metastable latch TRNG design. Section III analyzes the circuit parameters of a metastable latch for TRNG operation. Section IV shows simulation results for latch evaluation-time, power, and sensitivity to offsets while varying circuit parameters of relative device strength, type, and size. Finally, section V concludes the paper.

II. Background

A metastable latch circuit is a common TRNG topology due to it's simple design, small area, high-bitrate and low-power [1]–[4]. In this topology, a latch amplifies noise present in the circuit using positive feedback, resulting in a random bit stream at the output. Figure 1a shows a simplified schematic for the TRNG latch, while Fig. 1b a representative evaluation cycle. As shown in Fig. 1b, the large amplification pushes the outputs (V_1 and V_2) to opposite supply rails, resulting in a digital output value. To generate a random bit, the outputs are initially reset to equal voltages around mid-supply by the equalization transistor (EQ in Fig. 1a). The transistor pulls both V_1 and V_2 to the same voltage when the EQ signal is asserted as shown in Fig. 1b. Then, once the latch is allowed to evaluate (EQ signal is low) thermal noise from the inverters provides a small voltage difference on the input/output nodes, which is amplified by inverters. At this point, amplification from positive feedback forces the outputs to the supply rails, producing a random bit. After a bit is generated, the system is reset back into metastability to produce the next bit in the sequence.

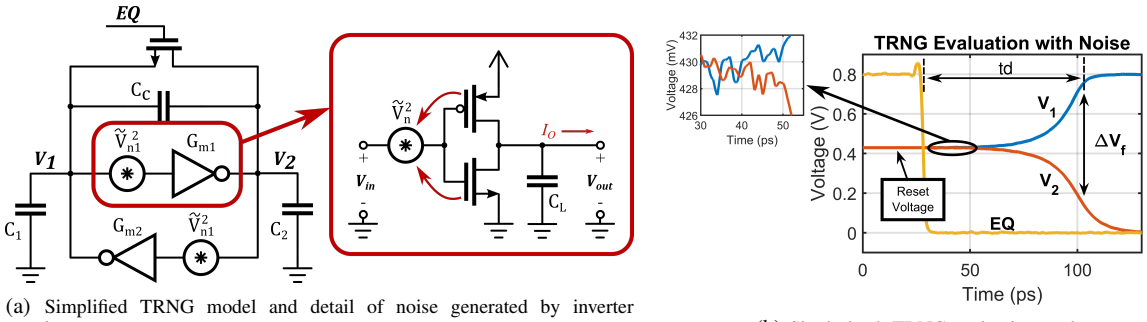
Generating random bits using a latch has several benefits. First, the high gain afforded by the latch provides a high output bitrate with relatively low power consumption when compared to other amplification methods [1]. Designs of this type have been demonstrated with bit-rates exceeding 1 Gbps and energy efficiencies exceeding 3 pJ/bit [1], [4]. Second, since metastable latches do not rely on traditional analog circuits, such as high-gain/bandwidth amplifiers which require large device area, the TRNG can benefit from process scaling to reduce both area and power, while maintaining other performance metrics [1], [4].

III. The Metastable Latch as a TRNG

A. Latch Model

In order to produce a random bit-stream, the noise present in the TRNG must have a high likelihood of overcoming any bias present in the system. In the ideal case where there are no offsets, any small amount of noise will result in a perfectly random output bit-stream. However, variations among transistors and parasitics introduce offsets, influencing the TRNG to favor one output state over the other, leading to biased outputs [1]–[3]. These variations are typically compensated using a per-die calibration. However, any calibration has a finite precision, and sufficient noise must be present to overcome remaining offsets with a high probability. In general, for a latch with low-probability of random outputs, robustness against PVT variation can be obtained by reducing offsets with precise

979-8-3503-0320-9/23/$31.00 ©2023 IEEE



(a) Simplified TRNG model and detail of noise generated by inverter transistors.

(b) Single latch TRNG evaluation cycle

Fig. 1: 1a shows a dynamic latch TRNG. A positive feedback loop is formed by two back-to-back inverters. $C1$, $C2$, and C_c are parasitic capacitors from the inverter transistors and following logic stages. The detail in 1a shows noise generated by each transistor in the inverter circuit. The channel thermal noise from each transistor is combined and input referred using the the G_m of the inverter. In 1b a single bit evaluation cycle is shown. At the start of the cycle, the latch is reset using the equalization transistor to a mid-supply reset voltage. Then, once equalization is removed (EQ goes low), thermal noise forces a voltage difference between V_1 and V_2 which is amplified until the outputs reach the supply rails. Evaluation time of the latch (t_d) is measured between the transition of the EQ signal and ΔV_f which is chosen to be $Vdd/3$.

calibration until the random outputs are sufficiently probable. Alternatively, the same result may be reached by increasing the noise power through device sizing. Since calibration takes time, impacting throughput, relaxing calibration requirements can improve TRNG bit rate. In this paper, we will primarily focus on analyzing and optimizing the latch circuit with the goal of increasing its random noise contribution.

In the following section we describe a model for the TRNG latch that we will use to perform this. Next, this model will be used to choose a reset voltage for the latch to minimize a specific class of offsets. Finally, the noise generated by the transistors will be considered in relation to relevant circuit parameters.

Our model for the latch is based on [5] where each inverter is modeled as shown in Fig. 1a. In this model, the inverter is linearized around the input voltage (V_{in}) where the current from the PMOS device is shunted to the NMOS device ($I_O = 0$ in Fig. 1a). We refer to the input voltage that meets this condition as V_S, or the switching voltage of the inverter. The transconductances of the NMOS and PMOS devices (g_{mn}, g_{mp}) are added together to form the transconductance of the inverter (G_m). Mathematically, we describe the inverter as in (1) [5, eq. (2)].

$$I_O = -G_m(V_{in} - V_S) \tag{1}$$

The load capacitance C_L for a single inverter arises from the combination of device parasitics, input capacitance of subsequent gates, and routing parasitics. Note that the coupling capacitance, C_c, in Fig 1a is primarily due to parasitic gate-drain capacitance in the transistors.

Offsets are induced in the latch through two forms: static offsets and dynamic offsets [5]. Static offsets are attributed to size and threshold mismatch during manufacturing, and are grouped into the switching voltage constant for the inverter [5]. Dynamic offsets arise from sources such as charge injection onto mismatched load capacitors (C_1, C_2 in Fig. 1a). Mismatch between C_1 and C_2 arises from both differences between transistors and layout parasitics from metal routing. While the mismatched capacitors do not influence V_S, they can lead to significant offsets during operation [5].

B. Resetting the Latch

Equation (2), models dynamic offsets attributed to mismatched load capacitors [5, eq. (40)].

$$V_{off\_C} = \frac{1}{2} \cdot \frac{\Delta C}{C + C_c} \cdot (V_{out,0} - V_S) \tag{2}$$

where V_{off_C} is the offset voltage due to capacitive mismatch, $V_{out,0}$ is the initial common-mode voltage on the latch, $C = C_1$, and $\Delta C = C_2 - C_1$. Note that (2) isolates the effect of dynamic mismatch, so it was derived in the case where static offsets are eliminated ($V_S = V_{S1} = V_{S2}$) [5]. While other factors, such as charge injection, prevent completely eliminating capacitive offsets, setting the output reset voltage to V_S ($V_{out,0} = V_S$), significantly reduces it's impact.

C. Noise Generation

The entropy harvested by the TRNG originates from thermal noise in the inverters generated by constituent NMOS and PMOS transistors. Here, we make the assumption that the 1/f noise corner for the devices is below the operating frequency of the latch, and consequently has little impact. Therefore, the 1/f noise is omitted from this discussion. An examination of transistor noise Power-Spectral-Density (PSD) is provided in [6], where particular attention is paid to short-channel effects. From [6], noise the input referred voltage noise PSD for NMOS and PMOS transistors is modeled by (3).

$$\widetilde{V}_n^2(f) = 4kT\frac{\gamma}{\alpha \cdot g_m} \tag{3}$$

Equation (3) informs us that increasing the overall g_m in the latch reduces the quantity of harvested noise. This is contrary to the requirements to reduce the latch evaluation time, which is also inversely proportional to g_m.

Both g_m and γ/α vary with the bias condition of the inverter. Our goal is to maximize the quantity $\frac{\gamma}{\alpha \cdot g_m}$ to maximize

the total noise produced. In an inverter, the relative V_{gs} of each device is set by the relative sizing of the PMOS and NMOS devices. For example, by increasing the strength of the NMOS device, the reset output voltage of the inverter will decrease, increasing the V_{gs} of the PMOS transistor while reducing the V_{gs} of the NMOS transistor. The V_{gs} of both the NMOS and PMOS transistors is increased when a device with a lower threshold voltage (V_t) is chosen. Note that reducing V_{th} will also increase the overall current used by the latch.

The prior discussion shows that there are a few possible parameters we can tune in order to increase the noise produced by the devices: device V_t (device type), relative device size, and total size. In the next section we will vary these parameters and observe their effect on probability of random outputs, bit-rate, and overall power consumption.

IV. Latch Simulations

As described by [3], the evaluation time of the dynamic latch can be characterized in terms of an initial and final voltage, ΔV_i and ΔV_f.

$$t_d \propto \ln\left(K\frac{\Delta V_f}{\Delta V_i}\right) \tag{4}$$

where K is a device/process constant. Values for ΔV_f and ΔV_i are set to $Vdd/3$ and $50\mu V$ respectively to measure the evaluation time of the latch, shown in Fig. 1b.

The sensitivity of the latch to offsets is simulated by sweeping a static offset voltage inserted at the gates of the two latch inverters while transient noise is invoked in the simulation. For each offset voltage, 100 transient noise simulations are evaluated (with different noise seeds) to capture the probability that noise would overcome the offset present in the latch. The transient simulation is curve fitted to a Gaussian Cumulative-Distribution-Function (CDF) to find the standard-deviation (σ) of the latch with relation to offset. σ provides a metric to judge the sensitivity of the latch to noise.

The results for one of these offset-sweep simulations is shown in Fig. 2. Each point on the graph shows how likely the latch is to produce a '1' as output for a given offset value. For equal distribution of output bits a, probability of 0.5 is desired; therefore it is beneficial for the CDF to remain near this value for a large range of offsets. This occurs when the σ for the distribution is large. Using these definitions for t_d and σ, we can explore the parameters of relative device size, type, and total size.

Relative transistor strength, denoted α, is defined in (5).

$$\alpha = \frac{\text{PMOS Width}}{\text{NMOS Width}} \tag{5}$$

Figure 3 shows a summary of latch and inverter characteristics while sweeping α for both regular and low threshold devices. Figures 3a and 3b show the input referred noise V_n^2 and G_m values for the individual latch inverters respectively. As shown in Fig. 3a, increasing the inverter skew up to a value of about $\alpha = 17$ increases the inverter input referred noise. At this point, the PMOS device stops contributing gain as

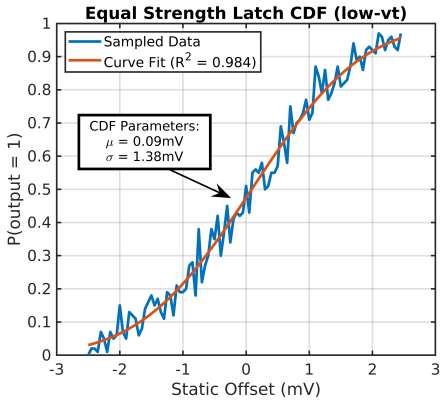


Fig. 2: This figure shows an equal NMOS/PMOS strength latch's cumulative-distribution-function (CDF) in response to static offsets. Each point on the graph shows how likely the latch is to produce a '1' as output for a given offset value. It also shows the raw data collected along side a Gaussian curve fit used to extract statistics.

seen by the G_m curve leveling off in Fig. 3b. These inverter parameters directly influence the behavior of the latch as a whole. Latch evaluation time (Fig. 3c) is inversely proportional to G_m while latch power (Fig. 3d) is well correlated with it. Moreover, Fig. 3e shows that, up to $\alpha \approx 17$, increasing α expands the influence noise has over the output of the latch; as the increased σ values show reduced sensitivity to offset in the presence of noise. This is in contrast to a sizing that minimizes evaluation time by maximizing G_m using equal strength NMOS and PMOS transistors.

Next, the total width of the NMOS and PMOS devices is varied by increasing the number of device fingers, increasing the overall G_m of the latch. We expect from (3) that increasing G_m will cause a reduction in noise proportional to the increase in G_m, which is evident when examining the results in Figs. 4a and 4b. As was seen with α, increasing latch G_m decreases both the t_d and σ of the latch (Fig. 4(c) and (e)), while increasing overall power use (Fig. 4d). It should be noted that reducing the total device size increases the V_{th} variation between transistors by Pelgrom's law, thereby increasing the need for calibration.

The impact of device type is also explored by varying both α and total device size with regular and low-vt transistors. Figures 3 and 4 show that regular threshold devices are slower than their low threshold counterparts due to their reduced g_m. Also, the regular threshold inverters exhibit a higher input referred noise, also due to their lower g_m. However, for devices with a large α, the low threshold devices overtake the regular threshold devices in terms of noise distribution (Fig. 3e). Device skew also presents a trade-off with speed, with a highly skewed low-vt inverter showing similar t_d as the corresponding regular threshold device with a lower α (Fig. 4c)

V. Summary and Conclusion

In summary, this analysis indicates that for maximizing both bit-rate and randomness it is beneficial to choose a latch with low-vt devices and with a relatively high α. Choosing

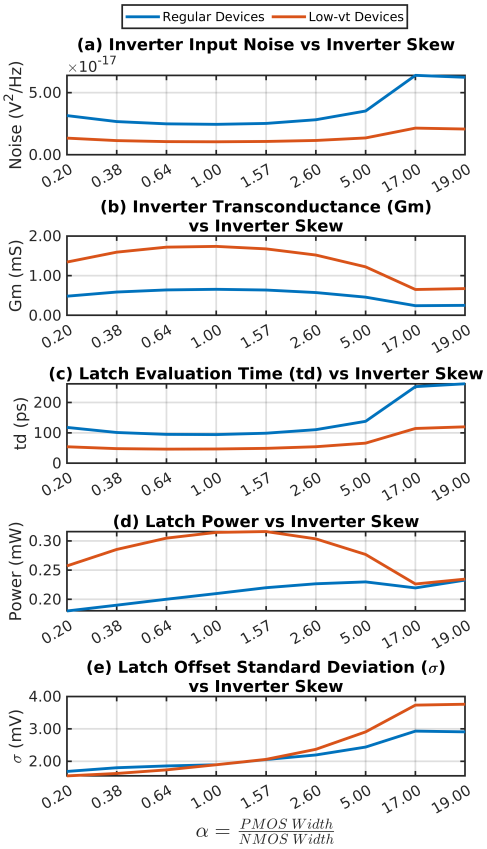


Fig. 3: Parameters of interest for both the individual inverters (subplots a and b) and the latch as a whole, while sweeping α. (a) shows the input referred voltage noise for a single inverter. (b) is the G_m for the latch inverters. (c) shows the evaluation times for the latch as measured with a $50\mu V$ offset. (d) shows the average power used by the latch over 100 evaluation cycles. Finally, (e) shows the standard deviation of the latch in response to static offsets. Choosing a low threshold device with a high α, decreases the sensitivity of the latch to offsets.

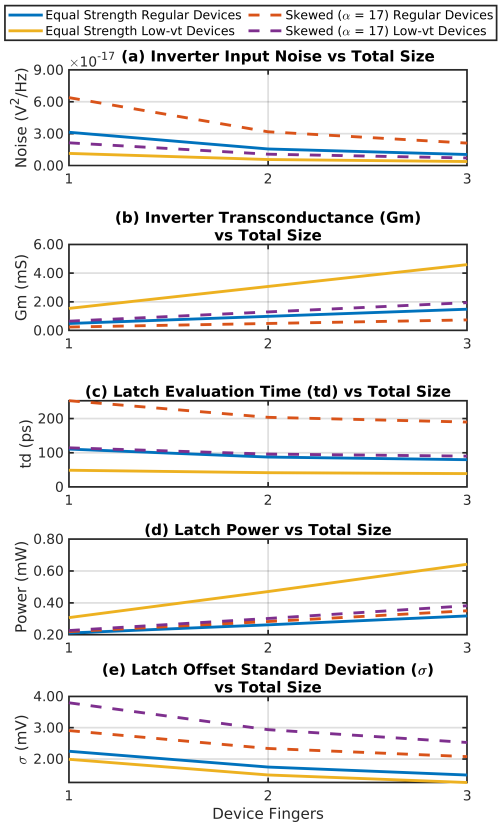


Fig. 4: Inverter and latch parameters while varying total width by increasing the number of device fingers. Plots show results for skewed and equal strength inverters using both regular and low-vt devices. (a) shows inverter input referred noise, (b) shows inverter G_m, (c) shows latch evaluation time, (d) shows average power use, and (e) standard deviation (σ) in response to static offsets. The trends of the graph are that σ and t_d decrease as the total width increases, while power increases.

an appropriate value for α presents a trade-off between the evaluation time and the sensitivity of the latch to offsets. A high α can significantly increase the noise, reducing the need for high accuracy calibration while reducing power; however, it also increases the evaluation time, reducing the achievable bit-rate of the TRNG.

In this paper, we explored the performance of a latch TRNG design with regards to relative device strength, type, and size. Based on the results, we conclude that constructing a latch from low-vt devices with a high PMOS to NMOS strength ratio increases the robustness of the design by reducing sensitivity to offsets. A tradeoff is made between robustness and bit-rate of the TRNG, where the bit-rate can be increased at the cost of higher overall power use and increased latch offset sensitivity. Future work is to provide an analytical model for the latch, incorporating both noise and circuit parameters in order to make predictions on the entropy of the TRNG for a given offset.

References

[1] S. K. Mathew, S. Srinivasan, M. A. Anders, H. Kaul, S. K. Hsu, F. Sheikh, A. Agarwal, S. Satpathy, and R. K. Krishnamurthy, "2.4 Gbps, 7 mW All-Digital PVT-Variation Tolerant True Random Number Generator for 45 nm CMOS High-Performance Microprocessors," *IEEE Journal of Solid-State Circuits*, vol. 47, no. 11, pp. 2807–2821, Nov. 2012.

[2] V. R. Pamula, X. Sun, S. Kim, F. u. Rahman, B. Zhang, and V. S. Sathe, "An All-Digital True-Random-Number Generator with Integrated De-correlation and Bias Correction at 3.2-to-86 MB/S, 2.58 PJ/Bit in 65-NM CMOS," in *2018 IEEE Symposium on VLSI Circuits*, Jun. 2018, pp. 1–2, iSSN: 2158-5601.

[3] C. Tokunaga, D. Blaauw, and T. Mudge, "True Random Number Generator With a Metastability-Based Quality Control," *IEEE Journal of Solid-State Circuits*, vol. 43, no. 1, pp. 78–85, Jan. 2008.

[4] M. Alioto, "Trends in Hardware Security: From Basics to ASICs," *IEEE Solid-State Circuits Magazine*, vol. 11, no. 3, pp. 56–74, 2019.

[5] A. Nikoozadeh and B. Murmann, "An Analysis of Latch Comparator Offset Due to Load Capacitor Mismatch," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 53, no. 12, pp. 1398–1402, Dec. 2006.

[6] Y. Cui, G. Niu, Y. Li, S. S. Taylor, Q. Liang, and J. D. Cressler, "On the Excess Noise Factors and Noise Parameter Equations for RF CMOS," in *2007 Topical Meeting on Silicon Monolithic Integrated Circuits in RF Systems*, Jan. 2007, pp. 40–43.