Stochastic Model of a Metastability-Based True Random Number Generator

Molka Ben-Romdhane[1,2], Tarik Graba[1], and Jean-Luc Danger[1,2]

[1] Institut Mines-Télécom; Télécom ParisTech; CNRS LTCI
[2] Secure-IC S.A.S.
{benromdh,graba,danger}@telecom-paristech.fr

Abstract. True random number generator (TRNG) designers should provide a stochastic model of the target of evaluation to be compliant with the AIS-31 standard evaluation process. In this paper, we present a model of a TRNG that extracts its randomness from the metastable behavior of a D-Latch. Such a model needs to be set up for the TRNG evaluation process. In this work, we describe and analyse the randomness coming from a chain of D-Latches when set near their metastable state. Then, we present a physical model of a metastability-based TRNG. The main novelty of this paper is the stochastic modeling process of a metastability-based TRNG. The presented model is validated on FPGA and a 65nm CMOS technology prototype chip.

Keywords: TRNG, metastability, model, randomness, noise, AIS-31.

1 Introduction

Randomness generation is needed for many applications spanning from Monte Carlo simulations to security communications. Also many cryptographic protocols are contingent to the unpredictability of random variable. A critical part to validate a true random number generator (TRNG) is to satisfy stringent verifications to make sure the function is not biased. For instance, statistical tests have been precisely specified by NIST in [1], BSI in [2] or FIPS in [3]. In the case of AIS-31 evaluation methodology of physical true random number generators [2], TRNG designers should provide a stochastic model of the TRNG behavior besides the compliance with the statistical tests.

On-chip TRNGs extract randomness from the chip ambient noise. There are many noise sources in CMOS circuits. Some of them are deterministic and others are random. Thermal noise, shot noise and (1/f) noise are considered as random noise sources [4]. By applying the central limit theorem, the noise exhibits a Normal probability density distribution [5].

In this paper, a stochastic model of a metastability-based TRNG is presented. This TRNG design is an open-loop structure which extracts the noise entropy by placing a memorizing cell in a metastable state, then observing the stable state which is the consequence of the noise impact. The presented metastability-based

M. Huth et al. (Eds.): TRUST 2013, LNCS 7904, pp. 92–105, 2013.
© Springer-Verlag Berlin Heidelberg 2013

TRNG output takes advantage of a metastable state, *MSS*, which converges to a final stable state depending on the noise value. Simulations have been performed to estimate the parameters that describe the proposed model. To validate this model, we perform AIS-31 standard statistic tests on acquisitions of both FPGA and ASIC targets.

Stochastic models of a PLL-based TRNG, a noisy diodes physical RNG and a floating-gate-based TRNG were introduced respectively in [6], [7] and [8]. Several analog and digital TRNG designs that extracts randomness from metastability have been proposed in ([9], [10], [11], [12] and [13]). Given our current knowledge, there is no such model for metastability-based TRNG in the literature.

As TRNGs require specific certifications, randomness must be proven first by model then by applying the generated sequence a battery of standard tests. We devote this paper to these two important steps of TRNG design. This paper is organized as follows: In the second section, an introduction to the basics of metastability is given. Then, an analytic expression is established to compute the model parameters. The third section deals with the modeling process and probability computation of the metastability-based TRNG output. In the fourth section, we validate the presented metastability-based TRNG model by comparing simulation results against test-chip measurements.

2 Modeling and Characterisation of Metastability

In storage elements, such as latches and flip–flops, whenever the delay between the clock and data violates the setup or hold time requirements, the normal behavior is not guaranteed. In fact, the input D must be stable for a duration of at least t_{setup} before the active edge of clock and it must remain stable for at least t_{hold} after the same clock edge. If those timing conditions are not met, the output state can go through an intermediate state where its value is not a valid logic value. This intermediate state is called metastable state. The final valid state of the storage element, either 0 or 1, is then not predictable and depends on the circuit ambient noise. The metastability-based TRNG design exploits this phenomenon to generate unpredictable random numbers. The main goal of this work is to try to model the behavior of the TRNG structure and quantify the output entropy.

To characterise this behaviour, let us consider the internal structure of a standard cell D-Latch as shown in Fig. 1a. This D-Latch is designed using tri–state gates controlled by the clock signal G and two back-to-back inverters commonly used in static storage elements. In the following, we consider an active low transparent D-Latch. When the value of the input clock signal G is '0', the D-Latch is said to be transparent, i.e. the output Q is equal to the input D, and when the value of the input clock signal G is '1' the D-Latch is said to be memorizing, i.e., the output Q keeps its value.

Depending on signal arrival times, the three situations are possible as shown in Fig. 1b:

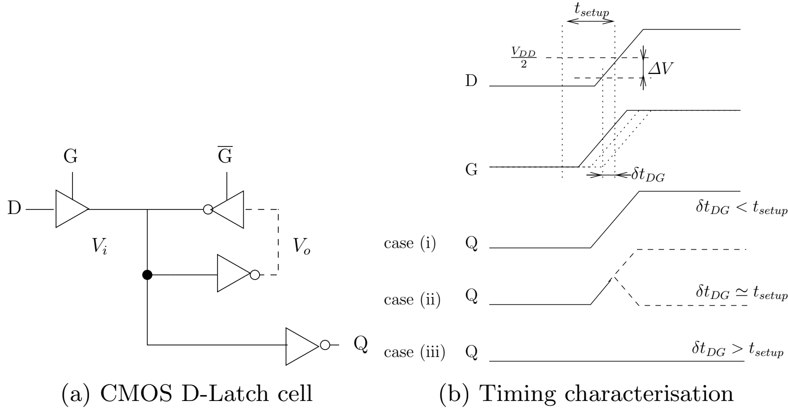


Fig. 1. D-Latch internal structure and timing characterisation

(i) The delay between the clock G and the data D, δt_{DG}, is greater than t_{setup}. This implies the Q output goes rapidly to V_{DD}.
(ii) $\delta t_{DG} \simeq t_{setup}$. This means there is a t_{setup} violation and Q may remain stuck around an intermediate voltage level V_{MSS} which is neither a $0V$ nor V_{DD}.
(iii) δt_{DG}, is less than t_{setup} the output Q never leaves $0V$.

Fig. 2 shows the clock-to-output propagation delay T_{GQ} versus the data-to-clock delay δt_{DG}.

When the setup requirements are respected ($\delta t_{DG} < t_{setup}$), the propagation delay is constant and corresponds to the propagation delay of a transparent D-Latch $T_{GQ_{max}}$ given by the manufacturer. When δt_{DG} decreases, the propagation time T_{GQ} increases with a logarithmic shape. This increase is due to the recovery time from metastability. The asymptotic limit defines a minimum setup time for which the propagation delay T_{GQ} becomes infinite. In the following, we refer to this asymptotic value as T_{setup0}.

The metastable state, *MSS*, is a state where the output voltage is neither a valid low nor a high logic state such as depicted in Fig. 3a. In this state the voltage values of both the input and the output of the static storage element, have the same value $V_{MSS} \simeq \frac{V_{DD}}{2}$.

Around this point, the inverters of the static storage element can be modeled as two amplifiers with a negative gain ($-A$) where $A \gg 1$ [14] [15] (we consider equal gains for both inverters for the simplicity of expression). Each inverter drives a resistance R and a capacitive load C (considered equal to simplify the expression) which models the gates and connections at each outputs as represented in Fig. 3b. In the absence of noise, the voltage of the internal node V_o

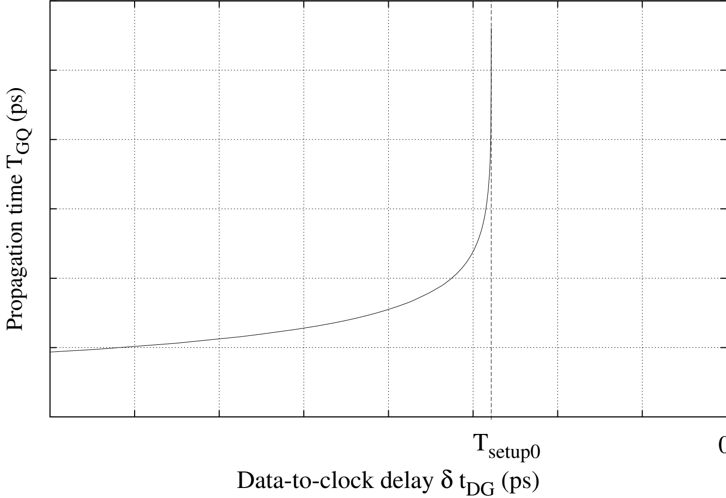


Fig. 2. Behavior of the propagation delay time T_{GQ} vs. δt_{DG} of a CMOS D-Latch.

should remain stuck at this intermediate voltage, around $\frac{V_{DD}}{2}$. The probability to enter a *MSS* whose duration is longer than t_m is expressed as follows [16]:

$$p(t > t_m) = e^{-\frac{(A-1)}{\tau} \cdot t_m} \quad (1)$$

Practically, when the G switches to '1' the node voltage is never exactly $\frac{V_{DD}}{2}$, and even then, ambient noise can shift this position. This bias will condition the final logical value and the time to reach it as shown in Fig. 3c. In fact, ΔV_{DG_0} impacts on the final state of the D-Latch. Fig. 3d shows the behavior of the internal memorizing net at *MSS* state for different data-to-clock delays. The figure (b) is a zoom of (a) around $\frac{V_{DD}}{2}$.

The expression of the voltage difference $V(t) = V_o(t) - V_i(t)$ around *MSS* is given in equation (2) [15]:

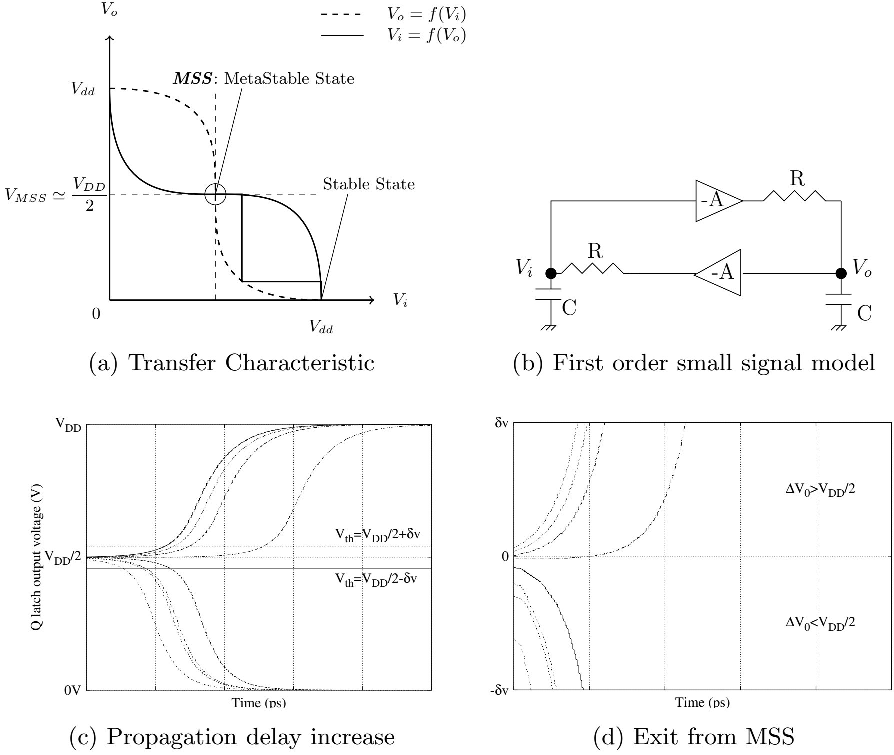
$$V(t) = \Delta V_{DG_0} \cdot e^{\frac{A-1}{\tau} t} \quad (2)$$

Where $\Delta V_{DG_0} = (V_o - V_i)(0)$ is the voltage difference at the moment where the D-Latch switches to memorizing mode. $\tau = R \cdot C$ is the time constant.

We introduce a threshold voltage V_{th} around *MSS*. This threshold corresponds to the voltage over which the state goes from *MSS* to a valid logic value.

$$T_r = \frac{\tau}{A-1} \ln\left(\frac{\Delta V_{th}}{\Delta V_{DG_0}}\right) \quad (3)$$

T_r represents the time needed to leave the metastable state or the increase in the propagation delay.



(a) Transfer Characteristic

(b) First order small signal model

(c) Propagation delay increase

(d) Exit from MSS

Fig. 3. D-Latch characterization around metastability

As shown in Fig. 1b, we consider a linear relation between the voltage differences ΔV and the delay in arrival times of the D and G signals such as:

$$\Delta V_{th} = \alpha \ A \cdot \delta t_{th}$$
$$\Delta V_{DG_0} = \alpha \ A \cdot \delta t_{DG} \tag{4}$$

Where α is the slope of the clock and data input and A the gain of inverter.

Thus, by replacing the expression of V_{th} in (3) we can express the resolving time as a function of the time delays as in equation (5).

$$T_r = \frac{\tau}{A-1} \ln(\frac{\delta t_{th}}{\delta t_{DG}}) \tag{5}$$

Which can be rewritten as:

$$T_r = \gamma(\beta - \ln \delta t_{DG}) \tag{6}$$

Equation (6) shows that the D-Latch propagation delay $T_{GQ} = T_r + T_{GQ_{max}}$ increases as δt_{DG} decreases. And this is what we obtain at simulation as shown in Fig. 2.

The next section provides a detailed analysis of the noise impact on the TRNG and the probability analysis of the output.

3 Stochastic Model of the Metastability-Based TRNG

3.1 Randomness Extraction

To maximize the probability to catch a metastable event at each clock cycle,a high speed metastability-based TRNG structure [10] has been introduced. This structure is illustrated in Fig. 4 and is composed of N latches and a delay structure to assure a race between the clock and data signals. The offset is first adjusted by two coarse chains with two control signals *ctrd* and *ctr* for the data and the clock, respectively.

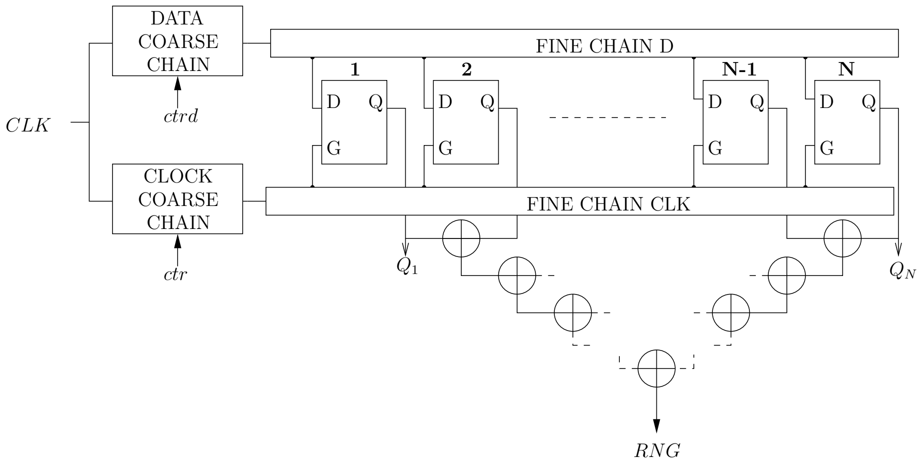


Fig. 4. Structure of the metastability-based TRNG

For the ith D-Latch, δt_{DG_i} represents the delay between D and G signals (G being the clock input of the latch). This delay is incremented between two consecutive latches by a differentiel delay δt, as expressed in equation (7). δt comes from the difference between the two fine delay chains D and CLK.

$$\delta t_{DG_{i+1}} = \delta t + \delta t_{DG_i} \tag{7}$$

Fig. 5 shows the clock-to-data delay at consecutive latches, superposed with the propagation characteristic of a D-Latch. This delay can be expressed,

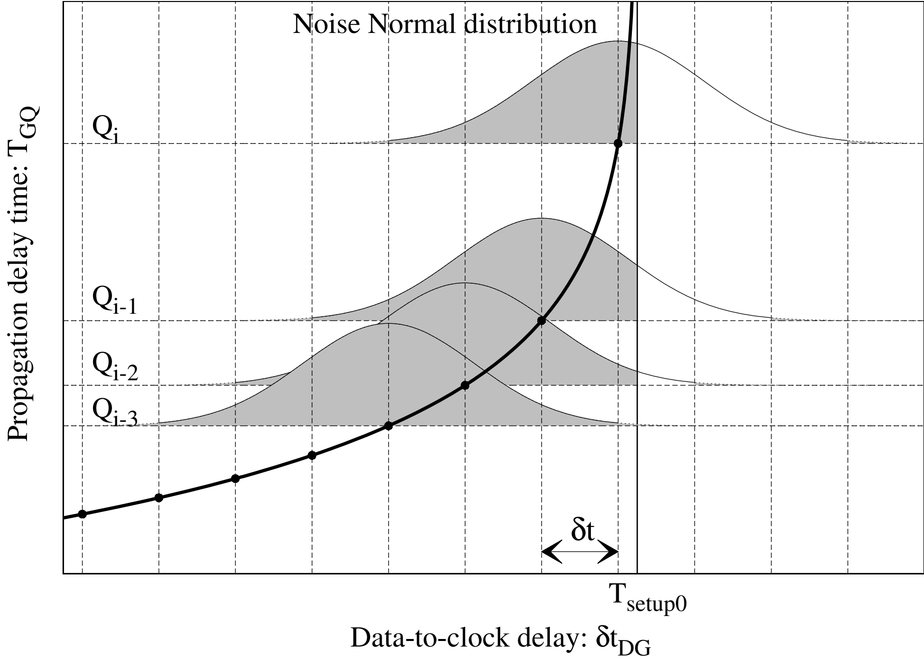


Fig. 5. The probability to correctly sample the input for consecutive latches

as in (8), as the sum of a deterministic delay, which correspond to the signals race and a random delay, which models the noise impact.

$$\delta t_{DG_i} = \Delta D_0 - i \cdot \delta t + \mathcal{N}(\delta t) \tag{8}$$

Where $\mathcal{N}(\sigma)$ is the Normal distribution and ΔD_0 is the initial delay between G and D introduced by the data and clock coarse chains. The incertitude distribution is considered Normal as it models the influence of the multiple noise sources in accordance with the central limit theorem [17].

The D-Latch will sample a high logic value 1 if this delay is smaller than T_{setup0}. We denote $p_{Q_i} = p(Q_i = 1)$ this probability:

$$p_{Q_i} = p(\delta t_{DG_i} < T_{setup0}) \tag{9}$$

This corresponds to the gray colored area of the Normal bell in Fig. 5. This probability can thus be analytically expressed as:

$$p_{Q_i} = \frac{1}{2}\left[1 - \mathrm{erf}(\frac{\delta t_{DG_i} - T_{setup0}}{\sigma\sqrt{2}})\right] \tag{10}$$

Where:

- T_{setup0} is the experimental asymptotic limit such as represented in Fig. 5.
- $\mathrm{erf}(x)$ is the error function.

3.2 Probabilistic Analysis of Metastability-Based TRNG

In the following, we use the notation p_X, representing $p(X = 1)$, where X is a Normal random variable. Since the TRNG output is the XOR of the N D-Latch, as illustrated in Fig. 4, the probability to have TRNG output equal to 1 is the probability parity of having an odd number of the N Q outputs D-Latch settling down to a logic 1. Let $p_{TRNG} = p(TRNG = 1)$ be the probability to have 1 on the TRNG output. Here we distinguish two cases:

(i) Influence of noise on each of the N Latches is independent.
(ii) The value of Q_i of D-Latch i impacts the output value Q_{i+1} of the $(i+1)^{th}$ D-Latch.

In the case (i), computing this probability p_{TRNG} is equivalent to compute the probability of a N-inputs XOR to be equal to 1. Let us consider the first two latches Q_1 and Q_2. Equation (11) represents the probability to obtain '1' at the output of the first stage 2-inputs XOR.

$$\begin{aligned} p_{Q_1 \oplus Q_2} &= p_{Q_1} \cdot \overline{p_{Q_2}} + \overline{p_{Q_1}} \cdot p_{Q_2} \\ &= p_{Q_1} \cdot (1 - p_{Q_2}) + (1 - p_{Q_1}) \cdot p_{Q_2} \\ p_{Q_1 \oplus Q_2} &= p_{Q_1} + p_{Q_2} - 2 p_{Q_1} p_{Q_2} \end{aligned} \tag{11}$$

Equation (12) is the factorized expression of (11).

$$\begin{aligned} 1 - 2p_{Q_1 \oplus Q_2} &= 1 - 2p_{Q_1} - 2p_{Q_2} + 4 p_{Q_1} p_{Q_2} \\ &= (1 - 2p_{Q_1}) \cdot (1 - 2p_{Q_2}) \end{aligned} \tag{12}$$

Then, by mathematical induction, we can generalize the expression for N-inputs XOR as shown in (13).

$$1 - 2p(\bigoplus_{i=1}^{N} Q_i = 1) = \prod_{i=1}^{N} (1 - 2p_{Q_i}) \tag{13}$$

Thus, from equation (13), the final expression of $p(TRNG = 1)$ is:

$$p_{TRNG} = \frac{1}{2}[1 - \prod_{i=1}^{N} (1 - 2p_{Q_i})] \tag{14}$$

In case (ii) where p_{Q_i} impacts $p_{Q_{i+1}}$ if Q_i equals '1' there is no way that Q_{i+1} equals '0', we can thus eliminate some terms in eq. 14.

For example, for a 3-inputs XOR, only the following input triplets (1,0,0) and (1,1,1) are left. Hence, the probability of the output of XOR $p_{Q_0 \oplus Q_1 \oplus Q_2} = p(Q_0 \oplus Q_1 \oplus Q_2 = 1)$ would be expressed as follows:

$$p_{Q_1 \oplus Q_2 \oplus Q_3} = p_1 \cdot (1 - p_2) \cdot (1 - p_3) + p_1 \cdot p_2 \cdot p_3$$

For a 4-inputs XOR, the product of all p_i does not appear in the final probability, as the XOR of an even number of ones is 0.

$$p_{Q_1 \oplus Q_2 \oplus Q_3 \oplus Q_4} = p_1 \cdot (1 - p_2) \cdot (1 - p_3) \cdot (1 - p_4) + p_1 \cdot p_2 \cdot p_3 \cdot (1 - p_4)$$

By mathematical induction, we can establish a general expression of $p_{TRNG} = p(TRNG = 1)$ for an N-inputs XOR (here N is even). Eq. (15) represents thus the probability p_{TRNG} in case (ii).

$$p_{TRNG} = \sum_{i=1}^{\frac{N}{2}} \prod_{j=1}^{2i-1} p_{Q_j} \cdot \prod_{j=2i}^{N} (1 - p_{Q_j}) \tag{15}$$

In the next section, we present the model verifications by simulation and experimental results on the test-chip. Then, the AIS-31 statistical tests are applied on the random number generated by metastability-based prototypes on both FPGA and ASIC technology targets.

4 Model Verification

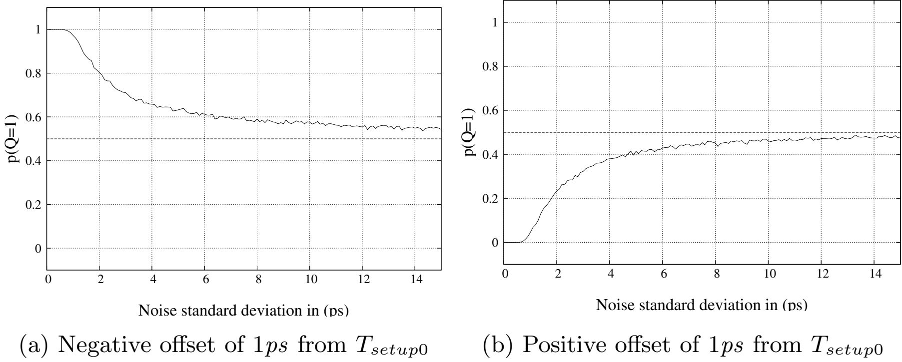
TRNG simulations with noise show that the impact of noise on the D-Latch chain is correlated such as explained in case (ii) of the section 3.2.

4.1 Model Validation by Simulation

We plot the increase of T_{GQ} vs. δt_{DG} for a D-Latch standard cell with $1fs$ resolution to estimate the model parameters of equation (10). We find that T_{setup0} is equal to -38.385ps. The differential delay δt introduced by the fine delay chains equals to $1ps$. Then, to extract the parameter σ, standard deviation of the TRNG noise source, transient electrical simulation of a single D-Latch standard cell are held with a noisy data input D for different σ.

Fig. 6 depicts the probability $p(Q = 1)$ as a function of noise standard for two different deterministic delays chosen around T_{setup0}. In Fig. 6a the offset is of -1ps from T_{setup0} and for Fig. 6b it is $1ps$. When the standard deviation of the noise is small, the probability is either 1 or 0 depending on the relative position to T_{setup0}. In this case, no random behaviour will be observed. When the standard deviation is higher than $10ps$, the probability tends to 0.5 making the output final logic value unpredictable.

Fig. 7 represents the simulated probability $p(Q = 1)$ with a noise standard deviation $\sigma = 5ps$ for offsets from T_{setup0} in the interval [-10,10]ps. The dashed curve represents, the theoretical $p(Q = 1)$, i.e. the function $f(x) = \frac{1}{2}(1 - erf(\frac{x}{\sqrt{2}\sigma}))$ with $\sigma = 5$ while the plane line curve represents the simulated probability.



(a) Negative offset of $1ps$ from T_{setup0} (b) Positive offset of $1ps$ from T_{setup0}

Fig. 6. The probability $p(Q = 1)$ *vs.* the noise standard deviation

Then, the same simulation experiment is performed on the TRNG composed of $N = 64$ latches while varying the standard deviation of the noisy data input. Fig. 8 shows side to side the probability p_{TRNG} *vs.* the noise standard deviation obtained from both analytic expression (Eq. (15) and Eq. (14)) and from the spice simulation for one configuration the coarse delay chain ($ctr = 0x00$, $ctrd = 0x00$). We see that for small noise standard deviation both analytic expressions give similar values. This figure also shows that the proposed model matches well the simulation results.

4.2 Silicon Proven Metastability-Based TRNG

In order to validate the TRNG model, we have applied standard statistical tests. FIPS 140-2, AIS-31 and NIST are three evaluation test standards commonly used to validate the randomness quality.

T0-T5 AIS-31 tests are applied on the digitized noise signal after post-processing. FIPS 140-2 [3] are similar to T1-T4 tests with different rejection limits. P2 tests class of AIS-31 (corresponding to T6-T7-T8) are the sole that have to be applied on the raw output of the TRNG, i.e. before any post-processing, as specified in the AIS-31 evaluation methodology [2].

In what follow, we will thus only present the results of the AIS-31 tests. We ran the different AIS-31 statistical tests on $20Mbits$ samples from an ASIC test-chip and for an FPGA implementation. In both FPGA and ASIC prototype, the TRNG structure is composed of N=64 latches.

ASIC Test-Chip Experiments. The test-chips were fabricated in the 65nm CMOS technology process by STMicroelectronics. Two versions of the TRNG have been use, the first one has a δt equals to $5ps$, later referred to as TRNG1, while the second has a δt smaller than a $1ps$, later referred to as TRNG2.

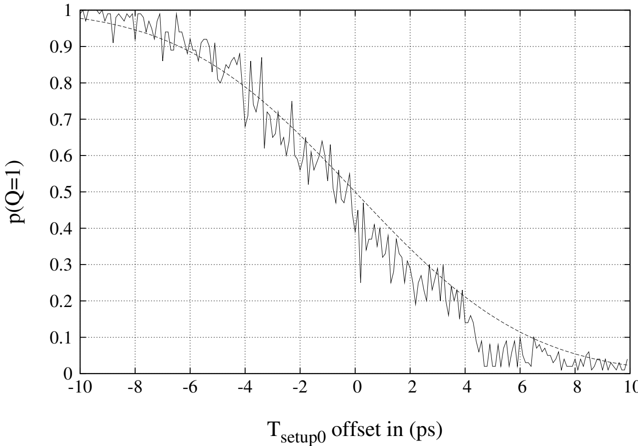


Fig. 7. The probability $p(Q = 1)$ *vs.* the offset from T_{setup0} for a noise standard deviation $\sigma = 5ps$.

The probability $p(TRNG = 1)$ has been measured for different values of the clock to data offset adjusted by *ctrd* and *ctr* coarse chain control signals. The values reported in Table 1 for TRNG1 allow to conclude that the noise standard deviation is rather low compared to the diffrential delay δt as most of the probability value are far from 0.5, as shown by the model and simulation probability curves. For exemple, for the coarse chain configuration ($ctr = 0x00$, $ctrd = 0x00$), the probability p_{TRNG} measured on the testchip over 100000 samples as in Table 1 is 84.25%. If we compare this value to the probability obtained for the same configuration from the model and the spice simulation (Fig. 8a and Fig. 8b), we can see that this probability corresponds to a noise standard deviation around $2ps$.

Table 1. $p(TRNG = 1)$ measured on the testchip for TRNG1 and diffrent *ctr* and *ctrd* configurations of the coarse delay chains

ctrd \ *ctr*	0x00	0x01	0x03	0x07	0x0F	0x1F	0x3F	0x7F
0x00	84.25	95.97	77.91	94.13	88.45	4.98	8.11	91.79
0x01	0.14	0.68	21.43	49.65	96.93	100	94.88	55.91
0x03	100	100	74.94	53.8	98.95	99.99	2.16	99.87
0x07	0.11	7.23	98.49	99.73	74.98	0.28	27.95	100
0x0F	0	0	100	97.39	99.7	26.31	49.83	63.27
0x1F	0	0	93.9	44.96	28.17	76.4	94.09	9.37
0x3F	0	0	0	58.84	2.16	40.51	32.82	99.97
0x7F	0	0	0	1.6	38.2	99.98	5.47	66.77

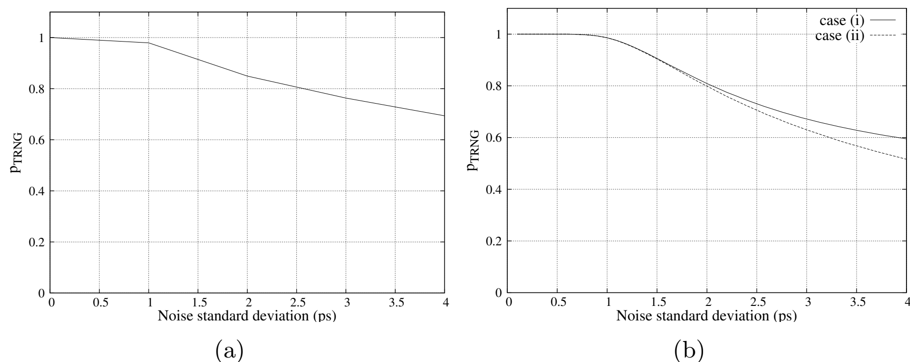


Fig. 8. The probability p_{TRNG} *vs.* the noise standard deviation (a) simulation (b) analytic expressions.

Table 2. AIS-31 Class P2 Statistical tests results of ASIC (TRNG2 version) and FPGA TRNG

AIS-31 Class P2 Tests	**FPGA**	**ASIC**
Uniform distribution test procedure T6a	Pass	Pass
Uniform distribution test procedure T6b	Pass	Pass
Test for homogeneity procedure T7a	Pass	Pass
Test for homogeneity procedure T7b	Pass	Pass
Entropy estimation test T8	Pass	Fail

Results of P2 Class statistical tests on the ASIC TRNG2 without post-processing are reported in Table 2.

P1 class tests have also been run on post-processed samples. Only Von Neumann post-processing have been used here to balance the number of zeros and ones and both TRNGs pass this class of tests.

Results of the TRNG1 version are not presented because more tests fail (3 over 5). This is basically due to a larger δt, which is larger than the exploitable noise standard deviation.

FPGA Experiments. The FPGA implementation has been done on a Xilinx Virtex-5 FPGA device, the delay δt is equal to $6ps$. Random bits acquired on this implementation passes both P1 and P2 classes tests of the AIS-31 statistical tests, without any post-processing as shown in Table 2. This makes us think that in an FPGA exploitable noise has a larger standard deviation than what can be observed in an ASIC implementation. This difference could come from the routing structure of the FPGA which contains more active elements (switch matrices, line buffers . . .) that generate more noise.

5 Conclusion

In this paper, we presented a stochastic approach to model and characterize a metastability-based TRNG. The principle is to place a D-Latch in a metastable state, then sample the stable state which is the consequence of the chip ambient noise impact. We discussed and presented the method that allows to compute the parameters of the modeling equation through electrical simulation. The probability expression of the TRNG is computed in terms of the noise standard deviation, the characteristics of the D-Latch T_{setup0}, and the delay δt of the delay chain elements. This stochastic model has been validated on an ST 65nm test-chip and FPGA.

References

1. NIST: Recommendation for the entropy sources used for random bit generation (2012), http://csrc.nist.gov/publications/drafts/800-90/draft-sp800-90b.pdf
2. Schindler, W., Killmann, W.: A proposal for: Functionality classes for random number generators1 (September 2011)
3. Federal Information Processing Standards (FIPS) Publication 140-2. Security requirements for cryptographic modules (May 25, 2001), http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
4. Mandal, M.K., Sarkar, B.C.: Ring oscillators: Characteristics and applications. Indian Journal of Pure and Applied Physics 48, 136–145 (2010)
5. Korkmaz, P., Akgul, B.E.S., Palem, K.V.: Characterizing the behavior of a probabilistic cmos switch through analytical models and its verification through simulations (2005)
6. Simka, M., Drutarovsky, M., Fischer, V., Fayolle, J.: Model of a true random number generator aimed at cryptographic applications. In: Proceedings of the 2006 IEEE International Symposium on Circuits and Systems, ISCAS 2006, p. 4 (May 2006)
7. Killmann, W., Schindler, W.: A design for a physical RNG with robust entropy estimators. In: Oswald, E., Rohatgi, P. (eds.) CHES 2008. LNCS, vol. 5154, pp. 146–163. Springer, Heidelberg (2008)
8. Xu, P., Horiuchi, T., Abshire, P.: Stochastic model and simulation of a random number generator circuit. In: IEEE International Symposium on Circuits and Systems, ISCAS 2008, pp. 2977–2980 (May 2008)
9. Kinniment, D.J., Chester, E.G.: Design of an on-chip random number generator using metastability. In: Proceedings of the 28th European Solid-State Circuit Conference (2002)
10. Danger, J.-L., Guilley, S., Hoogvorst, P.: High Speed True Random Number Generator based on Open Loop Structures in FPGAs. Microelectronics Journal 40(11), 1650–1656 (2009), doi:10.1016/j.mejo.2009.02.004
11. Suresh, V.B., Burleson, W.P.: Entropy extraction in metastability-based TRNG. In: HOST, pp. 135–140 (2010)
12. Majzoobi, M., Koushanfar, F., Devadas, S.: FPGA-based true random number generation using circuit metastability with adaptive feedback control. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 17–32. Springer, Heidelberg (2011)

13. Hata, H., Ichikawa, S.: Fpga implementation of metastability-based true random number generator. IEICE Transactions 95-D(2), 426–436 (2012)
14. Chen, D., Singh, D., Chromczak, J., Lewis, D., Fung, R., Neto, D., Betz, V.: A comprehensive approach to modeling, characterizing and optimizing for metastability in fpgas. In: Proceedings of the 18th Annual ACM/SIGDA International Symposium on Field Programmable Gate Arrays, FPGA 2010, pp. 167–176. ACM, New York (2010)
15. Ginosar, R.: Metastability and synchronizers: A tutorial. IEEE Design Test of Computers 28(5), 23–35 (2011)
16. Veendrick, H.J.M.: The behaviour of flip-flops used as synchronizers and prediction of their failure rate. IEEE Journal of Solid-State Circuits 15(2), 169–176 (1980)
17. Trotter, H.F.: An elementary proof of the central limit theorem. Archiv der Mathematik 10, 226–234 (1959)