# A Closer Look at a Recent Pipelined True Random Number Generator Design

Markus Dichtl
mdspam1968@gmail.com

November 16, 2022

**Abstract**

[12] suggests a pipelined TRNG design and a stochastic model for it. The stochastic model is shown to be inadequate and other problems of the TRNG design are identified. Possible fixes for the problems are considered.

## 1 A pipelined TRNG design

[12] suggests a pipelined TRNG design. In the first stage of the pipeline, two ring oscillators $DC0$ and $DC1$ of length 5 are started simultaneously. The periods of both ring oscillators are counted. When the ring oscillator $DC0$ has finished $n$ periods, the ring oscillator $TDC0$ of length 3 in the second pipeline stage is started. Analogously, the ring oscillator $TDC1$ starts when $DC1$ has finished $n$ periods. The output signal $TDC_1$ of $TDC1$ is used as clock input of a D-flip-flop which samples the output signal $TDC_0$ of $TDC0$. As soon as the value sampled by this flip-flop changes, the generation of a random bit is finished. The bit generated is based on the parity of the number of oscillations of $TDC1$ since it was started.

The frequencies of $TDC0$ and $TDC1$ are chosen very similarly, so the jittering time difference between the start of $TDC0$ and $TDC1$ can be evaluated with high precision.

## 2 The stochastic model for the pipelined TRNG design

[12] models the phases of the ring oscillators as Wiener processes with drift. This is based on the assumption that the ring oscillator jitter is caused by thermal noise, that is white noise. Subsequently [12] analyses how the jitter modelled by the Wiener processes propagates through the TRNG design.

## 3 The fundamental logical fallacy of [12]

[12] is based on exploiting thermal jitter in ring oscillators. It concedes that there might be other kinds of jitter of the ring oscillators as well. In section 4 of [12], there are some jitter measurements. It is not at all clear what caused the jitter contributions measured. However, the theory provided in this section is fundamentally

based on the assumption that thermal jitter was measured, that is, statistically independent jitter contributions. This theory of independent jitter contributions is used to determine the jitter strength defined in [12], which is conservatively estimated from the various measurements. However, this conservative estimation is made from the perspective of thermal jitter. It is not conservative from the perspective of the origin of the jitter. It may very well be that a large part of the jitter measured is due to statistically dependent noise. It is not possible to determine a lower bound for the thermal jitter contributions from the measurements described. Subsection 7.1 of this paper will provide references to prior attempts to distinguish quantitatively between dependent and independent jitter contributions.

The climax of the logical fallacy is achieved in the last sentence of the first paragraph of section 3 of [12]: "As we assume thermal noise is independent from all other sources of noise, the coexistence of these other noise sources will not lead to an entropy reduction and the estimation provided here is certainly a lower bound." In this way, measurements of jitter with unclear provenance are incorrectly turned into lower bounds for thermal jitter.

## 4 Is the stochastic model adequate?

Probably most people working in the field would have found it adequate to model the jitter of a ring oscillator as a Wiener process with drift ten years ago. But many insights were gained since then.

The author of this paper heard publicly for the first time in 2011 that ring oscillator jitter does not accumulate according to the central limit theorem of probability theory from [11]. The reason behind this, at that time, unexpected behaviour is that the jitter contributions are not statistically independent. As there are also variants of the central limit theorem for short range dependencies, the underlying statistical dependencies must persist over long temporal ranges. The PhD thesis of Patrick Haddad in 2015 [6] was a major step forward in understanding dependent ring oscillator jitter contributions. Below, in subsection 7.1, the approach of [6] to quantify the dependent and independent jitter contributions will be described. [13], a publicly available draft version to succeed the quotation KS11 from [12], the seminal AIS20/31 document to require a stochastic model as the base for the evaluation of true random number generators, also points out the problem of dependent flicker noise making the measurement of the 'useful jitter' more difficult.

However, people who want to generate true random numbers and therefore strive to get as much jitter as possible are outsiders in the world of electronics. Most people want to minimise jitter. So detailed studies of oscillator jitter, including ring oscillator jitter, were published first from the perspective of minimising jitter. E. g. [7] discussed the influence of 1/f noise on ring oscillator jitter already in 1998.

So, it is clearly not adequate in 2022 to base the stochastic model of a true random number generator on the assumption that there is only thermal noise. [12] mentions that here can be other jitter contributions, but does not take them into account, neither for the stochastic model nor for the experimental jitter measurement.

Instead of just assuming that the jitter contributions are statistically independent, it would have been possible to investigate this question experimentally. However, [12] does not provide this. But one can look at the experimental results provided in figure 12 of [12]. The axes of figure 12 are labelled 'DC0 period length' and

'DC0 period variance', however from the text in section 4.3 it becomes clear that this should be the duration of $n$ periods of DC0 and the corresponding variation, with $n$ assuming the values 1, 2, 4, and 8. Especially for chip 0 and chip 3 the variance measurements for $n = 8$ are considerably above the values one would assume for linear jitter accumulation. The most obvious explanation for this behaviour would be the quadratic accumulation of the variance for 1/f noise.

When introducing equation (5) of [12], which describes a Wiener process with drift, it is stated that it is assumed that the phase of an oscillator affected by thermal noise behaves as a Wiener process with drift. This is logically equivalent to assuming that dependent noise does not have a noticeable influence on ring oscillator noise. As shown above, it is not adequate to assume this.

So the whole theoretical considerations of section 3 of [12] are quite pointless, as they just are not adequate for real world ring oscillators.

The last sentence of section 3 of [12] is: As the entire system does not contain a state that is transferred from one bit generation to another, individual bits are IID by design. This emphasises again the unsuitability of the Wiener process with drift model. For 1/f noise in semiconductors, state information can be transferred over very long time periods, up to weeks (e. g. [3]). On the quantum mechanical level, this state transfer to a distant future is based on charges tunnelling into charge traps, staying there for a long time and slightly influencing the behaviour of the semiconductor, until leaving the charge trap after a long time, again by tunnelling with a very low probability (see e. g. [9]). Now, how does this state transfer into the future work in our case of ring oscillators? As the charge in the trap influences the phase of the ring oscillator in the same way during each period while it stays trapped, the variance of the (dependent) jitter contributions resulting from this accumulates proportionally to the square of the numbers of periods, whereas the variance of independent jitter contribution accumulates only linearly, according to the central limit theorem of probability theory. This explains why ring oscillator jitter is dominated by 1/f noise in the long run.

Another problem in the stochastic model from [12] is that it is based on the simplifying assumption that the jitter measured in the second stage of the pipeline originates completely from the first stage. [12] does not give comprehensible arguments for this. Even if this assumption holds for the stochastic model based on the Wiener process, it may fail for a correct model considering also 1/f noise. If one considers the case that the oscillators in the first pipeline stage oscillate for only one period before those in the second stage start, 1/f noise can not accumulate well, as the charges in the traps can influence the phase only once. However, to evaluate the small jitter contributions in the difference of the two period lengths from the first stage, a considerable number of periods of the ring oscillators of the second stage are required. The variance of the 1/f jitter contributions from the ring oscillators of the second state accumulates with the square of the number of periods.

Although it does not really matter in this situation: Section 3 of [12] claims that the two half period lengths of a ring oscillator are identically distributed, without giving any reason for this claim. Experiments on very long ring oscillators with high resolution half period measurements from [4] show that average half period lengths can be slightly different.

## 5 Will the sampling D-flip-flop work correctly?

An implicit assumption for all stochastic models of TRNGs is that all components work as intended. However, for all electronic components, there are operating conditions one has to meet for the component to work correctly. If the conditions are violated, the component may fail.

For D-flip-flops, the setup- and hold-times are important conditions to meet (e. g. [8]). They specify for how long the signal to be sampled must be constant before and after the clock edge which causes the sample to be taken. When the setup- or hold-time is violated, various unwanted things may happen. The flip-flop may start oscillating, or it may take a very long time to assume its final output value. It may also keep its output on an intermediate voltage level between logical 0 and 1 for some time. The behaviour of D-flip-flops with violated setup- or hold-times also depends on the logical value stored in the flip-flop before.

Now, is there a risk that setup- or hold-times are violated in D-flip-flops in the TRNG design of [12]? This risk definitely exists for the D-flip-flop whose data input is $TDC_0$ and whose clock input is $TDC_1$. Both signals are initially in random phases assumed to be independent. As the design from [12] is highly parametrisable, and as [12] rarely specifies the parameter chosen, it is not possible to provide a numerical estimate for the probabilities of the setup- or hold-time violations.

But the situation in the design of [12] is much worse than the risk of occasionally violating setup- or hold-time conditions! Actually, the design lets, by the only slightly different periods of $TDC_0$ and $TDC_1$, on purpose get their edges closely together. But when they are too closely together, it just means a violation of the setup- or hold-time. Whether the setup or hold-time is necessarily violated depends on the frequency difference of $TDC_0$ and $TDC_1$ and of course of the D-flip-flop. If the resolution $res$, which is defined as the absolute value of the difference between the period of TDCO and the period of TDC1, is smaller than the setup-time of the flip-flop, the probability of a violation is 1. So, for the design of [12] the risk of setup- or hold- is definitely much higher than the risk of accidentally sampling a signal at the wrong time.

Of course the risk of setup- or hold-time violations should be treated in the stochastic model of a TRNG, but this is not the case in [12].

In general, setup- and hold-time violations are a topic seldom considered in papers on TRNGs, but often there is a risk, e. g. always when jittering signals are sampled. [5] points out the risk of setup- and hold-time violations for a TRNG design were signals with an extremely high frequency are sampled. [13] also points out the risk of setup- and hold-time violations.

## 6 Jitter measurement

Often, stochastic models of TRNGs are based on a set of parameters whose values have to be determined experimentally. In the case of [12], there is only a single parameter to match, namely the jitter strength defined to be relation of the variance of the half period length of a ring oscillator and its expected value. This quantity is not easy to measure, as very precise measurements of the half periods are required in order to determine the variance. In [12] the jitter strength of the ring oscillator DC0 is stated to be conservatively estimated by a value of 30 fs. From figure 12 of the

paper, one can see that the half period length of DC0 is about 9 ns, so its variance is roughly $2.7 \times 10^{-22}\,\mathrm{s}^2$ . This corresponds to a standard deviation of about 16 ps.

### 6.1 Possible quantisation noise

Apart from the fact that it is just impossible to match a parameter from a stochastic model unable to describe the real behaviour of the TRNG, there is also quantisation noise, which might be wrongly interpreted as jitter of n periods of $DC0$.

Where does this quantisation noise come from? To measure the jitter of $n$ periods of $DCO$, it is counted how many periods of TDC1 occur during the $n$ periods of $DCO$. This count is called $R$. The variance of the $n$ periods of $DCO$ is derived from the variance of $R$. Now, by $R$ necessarily being an integer, and suitable phase conditions, extremely small variations may cause R to vary by 1, leading to an incorrect value for the jitter of $n$ periods of $DCO$. To give a concrete example: Let $n = 1$ and the mean period of $DC0$ be 10 ns and very little jitter, a standard deviation of 1 fs , the frequency of $TDC1$ be 100 ps and no jitter. For the sake of simplicity, it is assumed that the first periods of both oscillators start simultaneously, and also that there is just independent jitter. With probability 1/2 R will count to 99 and with probability 1/2 it will count to 100. The standard deviation of R is $1/\sqrt{2}$, so the standard deviation of the period of $DC0$ is wrongly assumed to be $100/\sqrt{2}$ ps, about 71 ps. The standard deviation of the jitter is, due to quantisation noise, overestimated by a factor of more than 70000.

### 6.2 Parametrisation used for the jitter measurements

As described in subsection 5.4 of [12], the ring oscillators can be parametrised in many ways, totalling in $2^{64}$ possible choices. For DCO, whose jitter strength [12] wants to measure, there are 4 inverter stages (there is also a NAND gate in the ring to control the on- and off-state of the ring, so the number of inverters is indeed odd). In each stage, there is one fixed CMOS inverter, and, in parallel, 4 inverters of different channel lengths which may be switched on and off to parametrise the speed of the ring oscillator. However, it is not so clear how this influences the ring oscillator jitter. Using parallel transistors was a technique to reduce noise in analogue audio devices (e. g. [10], but the technique is definitely much older), so it seems plausible that the parametrisation should influence the jitter, an aspect completely ignored by [12]. It does not specify which parametrisation of the ring oscillator DC0 the measured jitter corresponds to nor does it indicate for which parameters the claimed lower bound of 30 fs for the jitter strength holds.

## 7 Can the problems be fixed and how difficult is this?

### 7.1 The stochastic model

[6] tries to distinguish the contributions from white noise and 1/f noise in jitter by studying the accumulation of ring oscillator jitter over varying periods of time. The variation of the jitter due to white noise increases proportionally to the accumulation time, whereas the variation due to 1/f noise increases proportionally to the square of the accumulation time. [6] uses the equation $var(t) = at + bt^2$ to describe the dependence of the variance of the jitter accumulated in time $t$. The values of $a$ and

$b$ are chosen to to fit the experimental data. The TRNG suggested in [6] only relies on the white noise contribution characterised by $a$ whereas the 1/f contribution is ignored. However, this approach seems to be numerically quite unstable. This is possibly due to the fact that for the shortest accumulation times measured, the number of periods observed was more than 20000, whereas the variation of these numbers was below 2. So, quantisation effects, which are not taken into account, probably influence the results. If one tries to expand the approach from [6] by adding a constant $c$ to account for quantisation noise ([2]), resulting in $var(t) = a*t+b*t^2+c$, the data from [6] lead to a negative value of $a$. This does not make any sense, so obviously the approach from [6] has some problems.

However, it might be possible that the approach from [6] works better for the jitter measurement of [12], as [12] can measure the jitter of a very small number of ring oscillator periods and even a single period, compared to more than 20000 in [6]. So, perhaps the white noise contribution can be determined before the 1/f part dominates.

Another approach to distinguish between contributions from dependent and independent noise is suggested by [11], [1], and [13]: using the Allan variance.

But even if the white noise and 1/f noise contributions can be measured individually, it is not clear how this can lead to a stochastic model for the complete TRNG from [12]. In [6], one can reasonably assume that both kinds of jitter accumulate independently, and that the fixed time of sampling is determined in such a way that the white noise contribution alone is large enough to provide sufficient entropy. In the much more involved TRNG design from [12], one can not argue easily that both kinds of jitter run through the pipelined architecture independently. It seems that a suitable stochastic model for the TRNG from [12] could be a hard problem.

### 7.2 Violating setup- or hold-times

When the parameters of the ring oscillators and the properties of the D-flip-flop are known and if a suitable stochastic model is available, it does not seem too hard to determine the probabilities of setup- and hold-time violations. If these probabilities are sufficiently low, it could be discussed whether the errors caused by the violations are seldom enough to achieve the security goal of the TRNG despite them. But it seems doubtful whether this will be really the case, as the design of the TRNG forces the edges of $TDC_0$ and $TDC_1$ to come closely together. If setup- or hold-times are violated, it is probably a hard task to model the behaviour of the TRNG adequately, as it is generally not specified how a D-flop-flop behaves in these cases. Perhaps the behaviour of the flip-flop could be characterised experimentally.

### 7.3 Quantisation effects in jitter measurements

If a suitable stochastic model of the jittering ring oscillators is available, it should not be too difficult to determine lower bounds for the variations of jittering edges even with quantisation effects.

## 8 Conclusion

The TRNG suggested in [12] was shown to suffer from several severe, well known problems, and most of them seem to be not easy to fix. It seems rather surprising

that a TRNG with such problems is suggested in 2022, but even more surprising that it is accepted for a major conference.

## References


[1] Elie Noumon Allini, Maciej Skórski, Oto Petura, Florent Bernard, Marek Laban, and Viktor Fischer. Evaluation and monitoring of free running oscillators serving as source of randomness. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 214–242, 2018.

[2] Pascale Böffgen and Markus Dichtl. A critical look at measurements of the statistically independent components of ring oscillator noise, June 2015. Presentation at CryptArchi workshop.

[3] Michael A. Caloyannides. *A Mathematical and Experimental Investigation of Microcycle Spectral Estimates of Semiconductor Flicker Noise*. PhD thesis, California Institute of Technology, Pasadena, California, 1972.

[4] Markus Dichtl. On jitter in very long ring oscillators, May 2022. Presentation at CryptArchi workshop.

[5] Markus Dichtl and Jovan Dj. Golic. High-speed true random number generation with logic gates only. In Pascal Paillier and Ingrid Verbauwhede, editors, *CHES*, volume 4727 of *Lecture Notes in Computer Science*, pages 45–62. Springer, 2007.

[6] Patrick Haddad. *Caractérisation et modélisation de générateurs de nombres aléatoires dans les circuits intégrés logiques*. Theses, Université Jean Monnet - Saint-Etienne, 2015. `https://tel.archives-ouvertes.fr/tel-01538434/file/These-HADDAD-Patrick-2015.pdf`.

[7] A. Hajimiri, S. Limotyrakis, and T.H. Lee. Jitter and phase noise in ring oscillators. *IEEE Journal of Solid-State Circuits*, 34(6):790–804, 1999.

[8] Paul Horowitz and Winfield Hill. *The Art of Electronics*. Cambridge University Press, USA, 3rd edition, 2015.

[9] C. Jakobson, I. Bloom, and Y. Nemirovsky. 1/f noise in cmos transistors for analog applications from subthreshold to saturation. *Solid-State Electronics*, 42(10):1807–1817, 1998.

[10] W Marshall Leach Jr. Noise relations for parallel connected transistors. *Journal of the Audio Engineering Society*, 47(3):112–118, 1999.

[11] Richard Newell. Measurement of fpga ring oscillator noise, and analysis using the allan variance method, 2011. Presentation at CryptArchi workshop.

[12] Adriaan Peetermans and Ingrid Verbauwhede. An energy and area efficient, all digital entropy source compatible with modern standards based on jitter pipelining. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2022(4):88–109, Aug. 2022.

[13] Matthias Peter and Werner Schindler. A proposal for functionality classes for random number generators, version 2.35, draft. `https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Certification/Interpretations/AIS_31_Functionality_classes_for_random_number_generators_e.pdf?__blob=publicationFile&v=5`, September 2022.