On the security of oscillator-based random number generators

Mathieu Baudet[1], David Lubicz[2,3], Julien Micolod[2], and André Tassiaux[1]

[1] DCSSI, 51 blv de la Tour Maubourg, 75007 Paris
[2] CÉLAR, BP 7419, F-35174 Bruz
[3] IRMAR, Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes

Abstract. True Random Number Generators (TRNGs) are a critical building block of many cryptographic systems. It is thus of first importance to design TRNGs with a proved assessment of security. A common and attractive way to implement a TRNG on a chip is to sample a ring oscillator and take advantage of its phase jitters as a source of entropy. In this paper, we present a comprehensive statistical model for TRNGs based on this principle. In order to use this model, typically to evaluate the entropy rate or to control the biases of certain bit patterns, it is necessary to assess the physical parameters of the ring oscillator. We propose a method for filtering out the perturbations due to the global deterministic component of the jitters, and for precisely measuring the statistics of the Gaussian jitters, that is, the secure source of entropy. Finally we outline two specific statistical tests applicable to the bit stream of a TRNG in order to check for its good operation, or in some cases, to recover the parameters of the underlying oscillator.

Keywords: hardware random number generators, ring oscillators, jitter model, entropy, statistical tests.

1 Introduction

Random Number Generators (RNGs) are crucial components for the security of cryptographic systems — typical usages including key generation, initialization vectors and even counter measures against side-channel attacks. Yet it is not easy to design hardware-based RNGs with a proved entropy rate, together with the flaw-tolerance and attack-resistance properties required by cryptographic applications. Most often, cryptographic RNGs consist of two parts: on one side, a physical (or True) Random Number Generator (TRNG) producing a random bit-stream by harvesting some entropy source, and on the other side, a cryptographic mode of operation ensuring that the final outputs remain computationally unpredictable even in case of an undetected failure of the TRNG. In this paper, we investigate the design of a hardware-based TRNG with a proved security, following the recommendations of [12]. This explains our focus on a simple design, suitable for a complete and precise modeling.

A source of randomness commonly used in FPGA and ASIC implementations of TRNGs is the instability of signal propagation time across logic gates. This instability is typically accumulated in so-called ring oscillators, consisting in a series of inverters or delay elements connected in a ring. The phase jitter of a ring oscillator is then extracted by means of a sampling unit, for instance a type-D flip-flop triggered by another ring oscillator or by an external clock signal. This simple structure has been widely studied in the literature as a building block for many on-chip TRNGs [8,3,14]. This paper aims to present a comprehensive statistical model of such a basic random unit, and contribute more generally to improving the security analysis of hardware random number generators.

Previous work on provably secure TRNGs based on sampled oscillators includes the work of [11,9,4], who consider mathematical models based on the flipping times T_k of the signal, that is, the times of its rising and falling edges. These models are natural to consider as they correspond to what can be experimentally observed on an oscilloscope. Existing work [9,4,2] report that the durations $X_k = T_{k+1} - T_k$ between the flipping times appear in many cases to be independent and identically distributed (in short *i.i.d.*), as one could expect from the physical intuition of electronic noise. This allows one to compute a safe lower bound of the entropy rate of the TRNG [9]. Yet, we found that such time-oriented models become quickly intractable when one wishes to compute more precise security parameters, such as the maximal bias on a short vector, or the probabilities of outputting certain bit patterns.

Our first contribution is an original approach to address this limitation using a different family of statistical models based on Wiener processes, a classical tool in the study of noisy oscillators [6]. More precisely, we identify the phase of an oscillator to a one-dimensional Brownian motion, and see the outputs of the generator as a (periodic, possibly probabilistic) function of the phase. This new, phase-oriented presentation allows us to achieve exact and approximate formulas for the probabilities of occurrence and for the entropy of arbitrary-length bit vectors, as well as a simple lower bound for the entropy rate. We validate these computations from a physical perspective by arguing, after [6], that the time-oriented and the phase-oriented models should be equivalent whenever the jitters of oscillators are small compared to their nominal periods. (This is always verified in practice.) Our formulas take as input a small number of physical parameters that still need to be measured in order to provide a full security assessment.

For that purpose, we also present an experiment designed to compute the relevant physical parameters of a given layout and a given technology. The main difficulty here is that the phase jitter of a ring oscillator, according to the model presented in [16], is made up of several different components depending on whether the jitter is local or global, deterministic or nondeterministic. From a security perspective, it is important to be able to distinguish the local Gaussian component, which is the entropy source of the TRNG, from the global deterministic jitter which can be manipulated from outside the device. Our results show that the measure of the statistical parameters of the jitter usually described in the literature [14,4,2] can be inaccurate and, sometimes, largely over-estimated. To solve this issue, we present an experiment able to extract and precisely measure the local Gaussian component of phase jitters, by comparing the signals of two free running oscillators on a same FPGA.

Finally, we apply our formulas to deduce statistical tests directly applicable to the output sequence of a TRNG. Our tests are specifically tailored to detect over-sampled oscillators, and potentially much stronger than the general-purpose tests routinely used [1]. In particular, for a sufficiently large amount of over-sampled bits, we observe that it is feasible to recover the main statistical parameters of a TRNG.

Organization of the paper. In Section 2, we recall the classical, time-oriented models for the sampling of oscillators, then we introduce our new, phase-oriented approach and use it to compute the security parameters of oscillator-based TRNGs. Section 3 presents an experiment designed to extract the Gaussian component of the phase jitter of a ring oscillator. Finally, in Section 4, we outline two special-purpose statistical tests applicable to the outputs of a TRNG in order to assess its statistical properties. Appendices A and B contain related proofs and additional justifications.

2 Statistical models for the sampling of oscillators

Motivated by the example of TRNGs based on ring oscillators, we describe two approaches to model an oscillator subject to phase jitters, and sampled by a time reference (e.g. a quartz clock signal). Whereas the first approach, based on flipping times, is classical [11,9,4], to our knowledge, the second approach, based on a Wiener processes, has never been considered in the field of secure random number generators. We focus on this new approach and derive several formulas to compute the security parameters of a TRNG, notably the biases and the entropy of bit-vectors, and as well as a lower bound of the entropy rate.

For simplicity, in what follows, we keep in line with previous work in the area [11,9,4] and concentrate on symmetric (in particular balanced) oscillators, for which the falling and rising transitions are equally distributed.

2.1 Classical approach (time-oriented)

A common and natural model for jittered oscillators consists in assuming that the half-periods, that is, the durations $X_k = T_{k+1} - T_k$ between the flipping times T_k ($k \geq 0$) of the signal, are independent and identically distributed random variables. In the sequel, we write $m_X = \mathrm{E}(X_k)$ for the mean, and $s_X^2 = \mathrm{V}(X_k)$ for the variance of X_k.

Once the flipping times T_k are defined, the corresponding signal $s(t) \in \{0,1\}$ at time $t \geq 0$ is described by $s(t) = \max\{k+1 \,|\, T_k \leq t\} \mod 2$. This model of $s(t)$ is often referred to as an *alternated renewal process* (see for instance [15]). Assuming a start-up time t_S and a fixed sampling period $\varDelta t$, the successive outputs of the random number generator are finally given by $s(t_S)$, $s(t_S + \Delta t)$, $\ldots$, $s(t_S + n\Delta t)$,$\ldots$

This model has been widely studied in the community of cryptographic random number generation [11,4], and even generalized [9] to allow for short-term dependencies between the X_k. Notably, Killman and Schindler [9] provide an approximate lower-bound for the source entropy, and present experimental results on a TRNG based on noisy diodes, which appear compatible with the i.i.d. assumption on the X_k.

Although an elegant explicit formula exists for the Laplace transform of $\mathbb{P}\left[s(t) = 1\right]$ (see [15, p. 334]), to our knowledge there is no general way to compute the probabilities of sampling arbitrary-length bit-vectors from alternating renewal processes, let alone if one wishes to abstract away the initial conditions by letting the start-up time t_S tend to $+\infty$. Yet, evaluating these probabilities is important to predict residual biases in the outputs of a TRNG, design specific statistical tests, or simply validate the physical model and the amount of Gaussian noise at a higher level. For these reasons, we consider another approach that directly models the phase evolution of an oscillator.

2.2 New approach (phase-oriented)

Motivated by typical solutions of equations in the study of noisy oscillators [6], we consider a family of model where the phase φ of an oscillator is analogue to a (stationary) one-dimensional Brownian motion. Accordingly, we model the evolution of the phase by a Wiener stochastic process $(\varphi(t))_{t\in\mathbb{R}}$ with drift $\mu > 0$ and volatility $\sigma^2 > 0$. In other words, for any times $t \geq t_0$, the phase $\varphi(t)$ conditioned on the values $(\varphi(t'))_{t'\leq t_0}$ prior to t_0 follows a Gaussian distribution of mean $\varphi(t_0) + \mu(t - t_0)$ and variance $\sigma^2(t - t_0)$. Equivalently, in terms of conditional density of probability, we have for all t, t_0, x, x_0,

$$\begin{aligned}\frac{d}{dx}\mathbb{P}\left[\varphi(t) \leq x \mid \varphi(t_0) = x_0,\ (\varphi(t'))_{t'<t_0} = \ldots\right] \\ = \qquad \frac{1}{\sigma\sqrt{2\pi(t-t_0)}} \exp\left(\frac{-(x - x_0 - \mu(t-t_0))^2}{2\sigma^2(t-t_0)}\right) \qquad (1)\end{aligned}$$

where the dots denote any set of values. (Note that both μ and σ^2 are frequencies here.)

Given a value x of the phase at a given time t, the output bit $s(t)$ is then modeled by a random variable such that the probability of $s(t) = 1$ is equal to $g_1(x)$, for some fixed 1-periodic function g_1. Let $g_0 = 1 - g_1$ be the symmetric function. Again, in terms of conditional probability, we have for all t, b, x

$$\mathbb{P}\left[s(t) = b \mid \varphi(t) = x,\ (\varphi(t'), s(t'))_{t'\neq t} = \ldots\right] = g_b(x). \qquad (2)$$

The fact that g_1 is 1-periodic is related to the periodicity of the sampled signal, whose average period is thus equal to $\frac{1}{\mu}$. Another noticeable consequence is that $s(t)$ depends only on the quantity $\overline{\varphi}(t) = \varphi(t) \mod 1$.

In the following, we concentrate on the (almost) deterministic sampling process defined by

$$g_1(x) = \begin{cases} 1 & \text{if } x \bmod 1 \in]\frac{1}{2}, 1[, \\ 0 & \text{if } x \bmod 1 \in]0, \frac{1}{2}[, \\ \frac{1}{2} & \text{if } x \bmod 1 \in \{0, \frac{1}{2}\}. \end{cases} \tag{3}$$

In other words, for such a choice of g_1, we have that $\overline{\varphi}(t) \in]0, \frac{1}{2}[$ implies $s(t) = 0$, $\overline{\varphi}(t) \in]\frac{1}{2}, 1[$ implies $s(t) = 1$, and $\overline{\varphi}(t) \in \{0, \frac{1}{2}\}$ implies that $s(t)$ is a pure random bit. (This last case is negligible and only motivated by Fourier series.) We note that more complex signals, for instance featuring unbalanced and/or noisy sampling, could be modeled as well, simply by adapting the definition of g_1.

When no initial precondition is given, we assume that $\varphi(0)$ follows the uniform distribution on $[0, 1[$, thereby modeling an infinite amount of time spent after the start-up of the oscillator. In particular, this ensures that each $\overline{\varphi}(t_0)$ follows the (same) uniform distribution, and that the source $(s(t))_{t\in\mathbb{R}}$ is stationary, that is, the probabilities of sampling bit vectors are invariant by time-shifting.

2.3 Equivalence formulas between models

For real physical systems, we expect the jitters to be small, that is, $\sigma^2 \ll \mu$, in terms of Wiener process. Arguably, the sampling of such a Wiener process is equivalent to that of an alternated renewal process where the durations X_k follow an inverse Gaussian distribution (a.k.a. Wald distribution):

$$p_{X_k}(x) = \left(\frac{\lambda}{2\pi x^3}\right)^{\frac{1}{2}} \exp \frac{-\lambda(x - m_X)^2}{2m_X^2 x} \qquad \text{for } x > 0 \tag{4}$$

with parameters

$$m_X = \frac{1}{2\mu} \quad \text{and} \quad \lambda = \frac{m_X^3}{s_X^2} = \frac{1}{4\sigma^2}. \tag{5}$$

Indeed, on the one hand, it is well-known that this distribution corresponds to the first passage time, from $\varphi(0) = \frac{k}{2}$ to $\varphi(x) = \frac{k+1}{2}$, of a Wiener process with drift μ and volatility σ^2 (see for instance [5, p. 221]). On the other hand, the assumption $\sigma^2 \ll \mu$ allows us to ignore the possibility for the sampled signal to flip in a detectable manner because of the phase going backward: indeed by another classical result of Wiener processes [5, p. 212], the probability $\mathbb{P}\left[\exists t \geq 0,\ \varphi(t) \leq \varphi(0) - \alpha\right] = e^{-2\alpha\frac{\mu}{\sigma^2}}$ will be infinitesimal for meaningful $\alpha > 0$.

Remark 1. We note that Equation (5) allows one to set the parameters m_X and s_X^2 in function of μ and σ^2, and use other distribution laws for X_k. For instance, we may use a Gamma distribution:

$$p_{X_k}(x) = \frac{1}{\Gamma(k)\theta^k}\, x^{k-1} e^{\frac{x}{\theta}} \tag{6}$$

with parameters $k = \frac{\mathrm{E}(X_k)^2}{\mathrm{V}(X_k)} = \frac{\mu}{2\sigma^2}$ and $\theta = \frac{\mathrm{E}(X_k)}{k} = \frac{\sigma^2}{\mu^2}$.

In any case, we will have $\frac{s_X^2}{m_X^2} = \frac{2\sigma^2}{\mu} \ll 1$, therefore, we expect that the shape of a given distribution law will have little influence on the behavior of processes. By extension, this suggests that Wiener processes suffice to approximate every physically relevant model based on renewal alternating processes. In the literature of noisy oscillators, we found that Demir et al. [6] do relate phase-oriented processes to time-oriented processes based on Gaussian distributions.

2.4 Controlling bit-vector probabilities, source entropy and biases

Let $\varDelta t > 0$ be some fixed sampling period. Using either kind of model, we define the *quality factor* $Q = \sigma^2 \, \varDelta t = \frac{s_X^2 \, \varDelta t}{4 \, m_X^3}$ of an oscillator-based TRNG as the phase variance accumulated between two samples, and let $\nu = \mu \, \varDelta t = \frac{\varDelta t}{2 \, m_X}$ be *frequency ratio* between the sampled and the sampling signal.

As mentioned before, in physical random generators based on phase jitter, we expect that $\frac{Q}{\nu} = \frac{\sigma^2}{\mu} \ll 1$.

Remark 2. We note that the notion of quality factor is in line with the intuitive definition for a alternating renewal process: the average relative variance accumulated during a time $\varDelta t$ (that is, approximately for $\frac{\varDelta t}{2 \, \mathrm{E}(X_k)} = \nu$ periods) is given by

$$\nu \, \frac{\mathrm{V}(X_{2k} + X_{2k+1})}{\mathrm{E}(X_{2k} + X_{2k+1})^2} = \frac{\nu}{2} \, \frac{\mathrm{V}(X_k)}{\mathrm{E}(X_k)^2} = \sigma^2 \varDelta t = Q. \tag{7}$$

We expect the sampled bits to behave as a perfect random source when the quality factor Q is significantly larger than 1. Indeed the accumulated phase jitter between two samples then amounts to more than one period of the oscillator.

In order to make this statement rigorous, we provide several formulas for the probabilities and the entropy of arbitrary-length bit vectors.

Proposition 1. *Consider a Wiener process $(\varphi(t))$ with parameters μ and σ^2 and define $(s(t))$ as previously. Let $\nu = \mu \, \varDelta t$ and $Q = \sigma^2 \, \varDelta t$.*

1. *The probability to sample 1 at time $t \geq 0$ conditioned on the phase at time 0 verifies*

$$\mathbb{P}\left[s(t) = 1 \mid \varphi(0) = x\right] = \frac{1}{2} - \frac{2}{\pi} \sin(2\pi(\mu t + x)) \, e^{-2\pi^2 \sigma^2 t} + O(e^{-4\pi^2 \sigma^2 t}). \tag{8}$$

2. *The probability to output a vector $\boldsymbol{b} = (b_1, \ldots, b_n) \in \{0,1\}^n$ at sampling times $0, \varDelta t, \ldots (n-1)\varDelta t$ satisfies*

$$\begin{aligned} p(\boldsymbol{b}) &= \mathbb{P}\left[s(0) = b_1, \ldots, s((n-1)\, \varDelta t) = b_n\right] & (9) \\ &= \frac{1}{2^n} + \frac{8}{2^n \pi^2} \left(\sum_{j=1}^{n-1} (-1)^{b_j + b_{j+1}} \right) \cos(2\pi\nu) e^{-2\pi^2 Q} + O(e^{-4\pi^2 Q}). & (10) \end{aligned}$$

3. The entropy of such an output is

$$H_n = \sum_{\boldsymbol{b}\in\{0,1\}^n} -p(\boldsymbol{b})\log p(\boldsymbol{b}) \tag{11}$$

$$= n - \frac{32(n-1)}{\pi^4 \ln(2)} \cos^2(2\pi\nu)\, e^{-4\pi^2 Q} + O(e^{-6\pi^2 Q}). \tag{12}$$

These expressions result from a careful study of the mathematical model, based on Fourier series and outlined in appendix A. Our study also provides exact formulas suitable for precise numerical simulations.

Lower bound for entropy. For a stationary process, it is well-known [13] that $\frac{1}{n}H_n$ and $H_n - H_{n-1}$ tends (from above) to a same limit H, called the *bit-rate entropy* of the source. We emphasize that the approximation of H_n above (Equation (12)) is not provably uniform in n, and thus cannot be used to provide a rigorous lower bound of H. However, following similar ideas as in [9], it is easy to state a lower bound of H based on the entropy of $s(\mathit{\Delta} t)$ conditioned on $\varphi(0)$.

Corollary 1. *Let $H(s(\mathit{\Delta} t) \mid \varphi(0)) = \int_0^1 H(s(\mathit{\Delta} t) \mid \varphi(0) = x)\, dx$ denote the average conditional entropy of $s(\mathit{\Delta} t)$ with respect to $\varphi(0)$, where by definition*

$$H(s(\mathit{\Delta} t) \mid \varphi(0) = x) = -p\log_2(p) - (1-p)\log_2(1-p) \tag{13}$$

if $p = \mathbb{P}\left[s(\mathit{\Delta} t) = 1 \mid \varphi(0) = x\right]$. Then we have that

$$H \;\geq\; H(s(\mathit{\Delta} t) \mid \varphi(0)) \;=\; 1 - \frac{4}{\pi^2 \ln(2)} e^{-4\pi^2 Q} + O(e^{-6\pi^2 Q}). \tag{14}$$

Remark 3. For a sanity check, note that $\frac{4}{\pi^2 \ln(2)} \approx 0.58 > \frac{32}{\pi^4 \ln(2)} \approx 0.47$.

Bounding biases in function of Q and n. We should emphasize that the given approximation for $p(\boldsymbol{b})$ (Equation (10)) hold when $e^{-2\pi^2 Q}$ is small enough for a fixed parameter $n = |\boldsymbol{b}|$. Preliminary numerical experiments suggest that these approximations might not hold uniformly in n. As a consequence, controlling the biases of the source may require to limit the number of consecutive outputs returned by the random source to not exceed a fixed value $n_{\max}$. To help designers assess $n_{\max}$ in a safe way, we provide exact bounds on the biases $\epsilon(\boldsymbol{b}) = 2^n p(\boldsymbol{b}) - 1$.

Proposition 2. *Let $\vartheta(x) = \sum_{k\in\mathbb{Z}} x^{k^2}$ for $|x| < 1$ and $B = e^{-2\pi^2 Q}$. For every n and every $\boldsymbol{b} \in \{0,1\}^n$, it holds that $|\epsilon(\boldsymbol{b})| \leq \vartheta(B)^{n-1} - 1$. In particular, for every n such that $n \leq n_{\max} = \lfloor 1 + \frac{1}{\log_2(\vartheta(B))} \rfloor$, we have $|\epsilon(\boldsymbol{b})| < 1$ and $H_n \geq n - 2$.*

Although these bounds may appear pessimistic compared to the approximate expressions given in the previous section, we note that small values of Q still allow for large n, as the following table illustrates:

Q	$B = e^{-2\pi^2 Q}$	$n_{\max} = \lfloor 1 + \frac{1}{\log_2(\vartheta(B))} \rfloor$
0.1	$1.3 \cdot 10^{-1}$	3
0.2	$1.9 \cdot 10^{-2}$	18
0.3	$2.6 \cdot 10^{-3}$	130
0.5	$5.1 \cdot 10^{-5}$	6701
1	$2.6 \cdot 10^{-9}$	$129 \cdot 10^{6}$
2	$7.1 \cdot 10^{-18}$	$48 \cdot 10^{15}$

3 Measuring the phase jitter of ring oscillators

In Section 2, we recalled classical models based on flipping times, and showed how to use a new family of models based on Wiener processes to analyze the security of a TRNG. Such security analyses rely on the physical parameters of the generators, that is, the frequency ratio ν and a quality factor Q.

In this section, we first report several experiments in order to assess the physical parameters of a single ring oscillator embedded on a FPGA, and to confirm the physical relevance of the model in use. Note that, as mentioned before, the choice between time and phase models does not matter as long as $Q \ll \nu$.

Whereas the experiments are satisfactory for well-stabilized FPGAs (see for instance [4,2]), we observe that the general case is more complex as the frequencies of oscillators may fluctuate. As emphasized by Valtchanov *et al.* [16], an important component of such fluctuations, the global deterministic jitters, typically low-frequency and global to a FPGA, should not be confused with (local) Gaussian phase jitters, as the former generally depends on signals such as the power source, that may leak or even be controlled by an attacker.

For that reason, we introduce a modified statistical model where the nominal frequency of an oscillator is subject to deterministic variations. We show how to validate this model experimentally by considering a layout made of two ring oscillators, and by simulating the sampling of one oscillator by the other, in a similar manner as a type D flip-flop.

3.1 Simple measures

Let $\boldsymbol{t} = (t_0, \ldots, t_n)$ be the increasing sequence of flipping times observed in the course of an experiment. Let $\boldsymbol{x} = (x_0, \ldots, x_{n-1})$ be the corresponding durations $x_k = t_{k+1} - t_k$. If we neglect the effect of global deterministic jitters, we expect the durations x_k to be mutually independent and to follow a same distribution of mean $m_X = \mathrm{E}(X_k)$ and variance $s_X^2 = \mathrm{V}(X_k)$.

To evaluate m_X, we use the classical estimator $\hat{\mathrm{E}}(\boldsymbol{x}) = \frac{1}{n}\sum_{i=0}^{n-1} x_i$. In theory, it should also be possible to directly measure s_X^2 using $\hat{\mathrm{V}}(\boldsymbol{x}) = \frac{1}{n}\sum_{i=0}^{n-1} x_i^2 - \hat{\mathrm{E}}(\boldsymbol{x})^2$. However, for very high frequency oscillators such as the one typically used for random generation, this method can be inaccurate (even in favorable cases) due to the quantification noise of the oscilloscope — and perhaps other factors. For that reason, it is classical to estimate the variance of $T_{k+\ell} - T_k$ ($\ell > 0$) by letting

$$V_s(\ell) = \hat{\mathrm{V}}(t_\ell - t_0,\ t_{2\ell} - t_\ell,\ \ldots, t_{\lfloor \frac{n}{\ell} \rfloor \ell} - t_{(\lfloor \frac{n}{\ell} \rfloor - 1)\, \ell}) \tag{15}$$

and carry on a linear regression on $V_s(\ell)$. Indeed, for $\frac{n}{\ell}$ big enough, we expect that $V_s(\ell) \approx \ell\, s_X^2$. By Formula (5), the parameters of the corresponding Wiener process are then $\mu = \frac{1}{2m_X}$ and $\sigma^2 = \frac{s_X^2}{4m_X^3}$.

Experimental results. We have made a series of experiments on an Altera Stratix II board with a non-well-stabilized switching power supply. We have implemented two different ring oscillators R and R' made up of a NAND gate and the same number of delay elements (see Figure 1). The clock signals of the two oscillators are connected to an output PIN and analyzed with a digital oscilloscope at 10 Gigasamples per second.

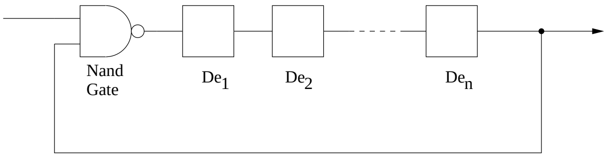

Fig. 1. Ring oscillator.

From the data recorded by the oscilloscope we recover two sequences $\boldsymbol{t} = (t_0, \ldots, t_n)$ and $\boldsymbol{t'} = (t'_0, \ldots, t'_{n'})$ corresponding to the flipping times of the signals of R and R', respectively. We obtained that the mean period of R is $14,5$ns and that of R' is $14,7$ns. We remark that although R and R' have identical VHDL specifications, their mean periods are not equal because of the variability of routing. Starting from the sequence $\boldsymbol{t} = (t_i)$ of flipping times of R, we compute the estimator $V_s(\ell)$ from the time gaps $(t_{\ell(i+1)} - t_{\ell i})$. Figure 2 represents the graph of $V_s(\ell)$ as a function of ℓ.

We remark that $V_s(\ell)$ is not a straight line with slope s_X^2 as one might expect if the global deterministic jitters were negligible. The accumulation phenomenon of the Gaussian jitter is nevertheless perfectly visible as the function $V_s(\ell)$ is globally increasing. We can explain the shape of $V_s(\ell)$ by introducing a frequency perturbation function $\alpha(t)$ to model the effect of global deterministic jitters. Specifically, assume that the expected value of $T_{k+1} - T_k$ given that $T_k = t_k$ is close to $\frac{m_X}{\alpha(t_k)}$ where $\frac{1}{\alpha(t)} = 1 + A \sin(\frac{2\pi t}{P} + B)$ is sinusoidal of period P with $P \gg m_X$. If ℓ is such that $2\ell\, m_X$ is very close to a multiple of P then in average the sampling of $(T_{\ell(k+1)} - T_{\ell k})$ will cancel out the contribution of $\alpha(t)$ to the variance of the jitter, thus giving a local minimum of $V_s(\ell)$. On the contrary, if $2\ell\, m_X$ is very close to a value of the form $jP + \frac{1}{2}P$, $j \in \mathbb{N}$, then the contribution

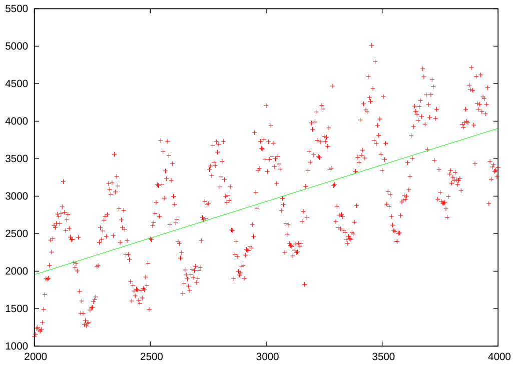

Fig. 2. Simple measure: $V_s(\ell)$ as a function of ℓ.

of $\alpha(t)$ to the variance of the jitter is maximal and we obtain a local maximum of the graph of $V_s(\ell)$.

3.2 Differential measures

The previous experiments suggest that the statistical models of Section 2 may not be accurate in general, for a non-well-stabilized oscillator, due to slow fluctuations of the average frequency μ (or equivalently of the half-period m_X). This phenomenon naturally leads us to model the phase of such an oscillator by a Wiener process with a non-constant drift of the form $\mu(t) = \mu\,\alpha(t)$, where $\alpha(t) > 0$ is a perturbation function, intuitively close to 1, and equal to 1 in average.

Alternatively, in terms of flipping times T_k, we may equivalently consider a modified classical model where the i.i.d. variables X_k now represent half-periods that are scaled by $\alpha(t)$. More precisely, to define T_{k+1} with respect to T_k and X_k, the relation $X_k = T_{k+1} - T_k$ is now replaced by $X_k = \int_{T_k}^{T_{k+1}} \alpha(t)dt$.

Following the empirical conclusions of Valtchanov *et al.* [16] regarding a decomposition between local and global jitters of oscillators, we expect $\alpha(t)$ to be *global*, that is, applicable to all the (similar) oscillators running on a given FPGA, and to have *slow variations* compared to the nominal frequency of oscillators.

Based on these considerations, we provide an experiment that we call "differential measure", which aims at eliminating the global factor $\alpha(t)$ in the measurements of local jitters. The experiment runs as follows. Consider two similar ring oscillators R and R' running on a same FPGA. Let $\boldsymbol{t} = (t_0, \ldots, t_n)$ and $\boldsymbol{t'} = (t'_0, \ldots, t'_{n'})$ be the two increasing sequences of flipping times observed for R and R', respectively. Intuitively, we wish to rescale the first sequence $\boldsymbol{t}$ according to the second sequence $\boldsymbol{t'}$, seen as a time reference, and then apply the same statistical treatment as in Subsection 3.1 to conclude.

More precisely, let $m_{X'}$ be the average half-period of R' (typically estimated as in Subsection 3.1) and let ϕ be the simplest, continuous, strictly increasing, piecewise-affine function from $[t'_0, t'_{n'}]$ to $[0, n']$ such that $\phi(t'_k) = k\, m_{X'}$ $(0 \leq k \leq n')$. Assume for simplicity that $t'_0 \leq t_0$ and $t_n \leq t'_{n'}$. We define the rescaled sequence $\boldsymbol{\tau} = (\tau_0, \dots, \tau_n)$ by $\tau_j = \phi^{-1}(t_j)$ $(0 \leq j \leq n)$, that is, more concretely: for every j,

$$\frac{\tau_j}{m_{X'}} = k(j) \; + \; \frac{t_j - t'_{k(j)}}{t'_{k(j)+1} - t'_{k(j)}} \tag{16}$$

where $k(j) = \max\{k \in \mathbb{N} \mid t'_k \leq t_j\}$. Finally, we consider the differential estimators $V_d(\ell)$ defined by

$$V_d(\ell) = \hat{\mathrm{V}}(\tau_\ell - \tau_0,\ \tau_{2\ell} - \tau_\ell,\ \dots, \tau_{\lfloor \frac{n}{\ell} \rfloor \ell} - \tau_{(\lfloor \frac{n}{\ell} \rfloor - 1)\, \ell}). \tag{17}$$

We note that, by construction, sampling the digital signal corresponding to the flipping times $\boldsymbol{t}$ at times $(t'_0, t'_2, \dots, t'_{2\lfloor \frac{n'}{2} \rfloor})$ — this is typically done by connecting the outputs of R and R' to a type-D flip-flop — would give exactly the same binary outputs as the sampling of the signal corresponding to $\boldsymbol{\tau}$ by a clock signal of constant period $2\, m_{X'}$.

As we show in Appendix B, this analogy also applies to $V_d(\ell)$, that is: according to the physical assumptions above, $V_d(\ell)$ should be approximately proportional to ℓ. More precisely, we show that the proportionality factor $s^2 \approx \frac{V_d(\ell)}{\ell}$ is an estimation of the amount of local noise available in R and R', in the sense that

$$s^2 \approx s_X^2 + \left(\frac{m_X}{m_{X'}}\right)^2 s_{X'}^2 \tag{18}$$

where m_X and s_X (resp. $m_{X'}$ and $s_{X'}$) are the mean and the standard deviation of the durations X_k related to R (resp. X'_k related to R').

Experimental results. We go on with the experimental results paragraph of Section 3.1 with the same experimental device and keep the same notations. From the flipping time sequences $\boldsymbol{t} = (t_i)$ and $\boldsymbol{t}' = (t'_j)$ of R and R', as described above, we compute the estimator $V_d(\ell)$ from $(\tau_{\ell(i+1)} - \tau_{\ell i})$ in the case of a differential measure.

Figure 3 represents the graph of $V_d(\ell)$ as a function of ℓ. We can see that the function $V_d(\ell)$ is well approximated by an affine function. The differential measure has canceled out the influence of the global deterministic jitter. By doing an affine regression on $V_s(\ell)$ we obtain a line with slope 0.97, while in the case of $V_d(\ell)$ the slope of the linear regression is 0.09. As a consequence, we see that the usual simple measure leads to a gross overestimation of the variance of the jitter of R.

4 Statistical tests

In the previous section, we provided low-level experiments to isolate and estimate the Gaussian noise related to a given hardware technology. However, these

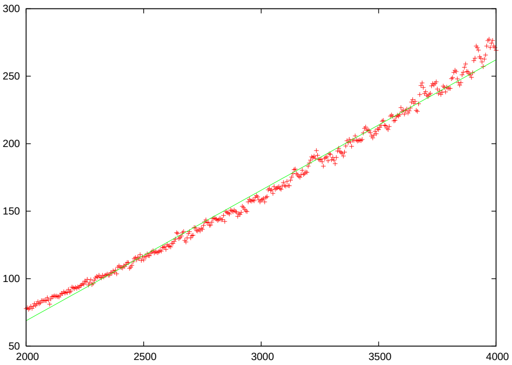

Fig. 3. Differential measure: $V_d(\ell)$ a function of ℓ.

experiments require a direct access to the (possibly multiple) ring oscillators *before* the signal is digitalized. In this section, we build upon the theoretical model presented in Section 2, and report higher-level experiments carried out directly on the bit stream of a sampled ring oscillator and applicable to any source that is presumably equivalent.

Our tests are based on the biases predicted by the statistical model when the quality factor $Q = \sigma^2 \Delta t$ (see Section 2) is insufficient, that is, when the sampling rate $\frac{1}{\Delta t}$ is too high compared to the amount of noise available σ^2. Such a weakened behavior can be obtained on purpose by accelerating the sampling clock. Interestingly, it could also occur in the case of a bad design or a physical attack on the generator. After discussing a simple auto-correlation test, we present numerical experiments related to the likelihood of a given sample.

4.1 Auto-correlation test

A consequence of Proposition 1 is that the first coefficient of auto-correlation of a sample $\boldsymbol{b} = (b_1, \ldots, b_n) \in \{0,1\}^n$ defined by $c(\boldsymbol{b}) = \frac{1}{n-1} \sum_{j=1}^{n-1} (-1)^{b_j + b_{j+1}}$, gives a statistical test especially well suited to detect biases in the bit-stream of random generators based on oscillators. Indeed, we note that the expectation of $c(\boldsymbol{b})$ is 0 on a perfect random source, but amounts to

$$\sum_{\boldsymbol{b}} c(\boldsymbol{b}) p(\boldsymbol{b}) = \frac{8}{\pi^2} \cos(2\pi\nu) e^{-2\pi^2 Q} + O(e^{-4\pi^2 Q}) \tag{19}$$

on a random generator such as considered in Section 2 (with the same notations). Besides, on perfect random sources, by the central limit theorem, $c(\boldsymbol{b})$ approximately follows a centered Gaussian distribution of variance $\frac{1}{n-1}$. Therefore, we may expect a source with low quality factor Q and $\cos(2\pi\nu) \neq 0$ to be easily distinguished from an ideal source for large enough n.

Experimental results. We have implemented a single ring oscillator R composed of 49 inverters on a Proasic 3E starter kit. We let the oscillator R be sampled via a type D flip-flop triggered by a divider applied to the quartz clock signal of the FPGA, running at frequency $f = 40$MHz (see Figure 4). Using a digital oscilloscope, we could measure the mean period of the ring oscillator: $2\,m_X = 38.4\,ns$. By performing a differential measure, we also estimated the variance of the jitter per half period of R to be approximately $s_X^2 = 0.0072\,ns^2$. From this, we could estimate the quality factor of the generator for a given division factor D to be $Q \approx \frac{s_X^2}{4\,m_X^3}\frac{D}{f} \approx \frac{D}{157286}$. Table 1 shows the empirical auto-correlation results obtained for various samples. We observe as expected that too small quality factors cause the source to be immediately discarded as $c(\boldsymbol{b}) \gg \frac{1}{\sqrt{n}}$.

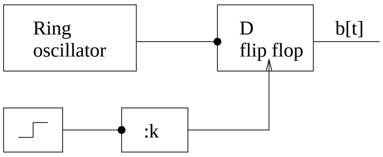

Fig. 4. Scheme of the experiment

Div. fact.	Qual. fact.	$c(\boldsymbol{b})$	$\frac{1}{\sqrt{n}}$
2559	0.016	0.0994	0.0011
22598	0.143	0.0181	0.0034
99245	0.630	0.0080	0.007

$c(\boldsymbol{b})$	-4	-2	0	2	4
$f(\boldsymbol{b})$	0.0004	0.0130	0.0589	0.1135	0.1398

Table 1. $c(\boldsymbol{b})$ for different quality factors (left) and 4-bit patterns against auto-correlations ($D = 2700$) (right).

To study the impact of (19) on short bit patterns, we also evaluated the empirical frequencies $f(\boldsymbol{b})$ of 4-bit patterns for different auto-correlations among the outputs of the source for $D = 2700$, and observed an affine progression as expected (Table 1).

4.2 Maximum likelihood estimation

The auto-correlation test is useful to detect flaws, but is not sufficient to estimate the physical parameters of a generator, namely its quality factor Q and its frequency ratio ν. On the other hand, the techniques used for proving Proposition 1 (see Section A in appendix) make it possible to compute the probability $p(Q, \nu, \boldsymbol{b})$ of a sample $\boldsymbol{b}$ in function of (Q, ν) efficiently and with good precision.

Following the rational of Maximum Likelihood estimators, we may then choose the two parameters (Q, ν) that maximize the probability of a given sample. Note that the mathematical model of sampling entails $p(Q, \nu, \boldsymbol{b}) = p(Q, \pm\nu + k, \boldsymbol{b})$ for any $k \in \mathbb{Z}$. Therefore, we can only observe $\bar{\nu} = |(\nu + \frac{1}{2} \mod 1) - \frac{1}{2}| \in [0, \frac{1}{2}]$.

Numerical experiments. The graphs of Figure 5 result from the evaluation of these probabilities on two bit samples of size $n = 50000$: one sample taken from a perfect simulated source (right-hand side), and the other from our FPGA for a division factor $D = 22598$ (left-hand side). On both graphs, Q is represented on the X-scale, ν on the Y-scale, and the plotted value on the Z-scale is $\log_2(1 + 2^n p(Q, \nu, \boldsymbol{b}))$. We observe that contrary to the simulated perfect source, the real data cause two symmetric peaks indicating very plausible values for Q and $\nu \mod 1$, that appear to be compatible with the computed quality factor $Q = \frac{22598}{157286} \approx 0.143$.

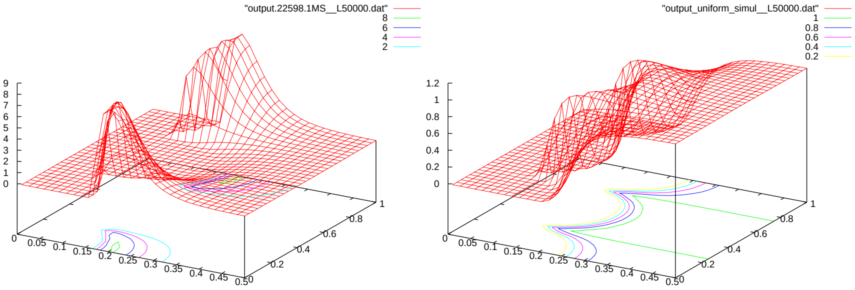

Fig. 5. Maximum likelihood estimations.

We also carried out the analysis of 800 bits of the source $D = 2559$ and 20000 bits of the source $D = 99245$ (Figure 6, left and right respectively). Interestingly, for a very low quality factor (left), the precision of numerical computations, i.e. the number of terms kept in power series, must be significantly augmented. On the opposite, for a higher quality factor (right), no characteristic peeks could be observed from the available samples.

Finally, to validate the equivalence of mathematical models, we simulated several sources of parameters $Q = 0.15$ and $\nu = 50.2$, according to the model of Wiener processes and two models of alternating renewal processes using Gamma and Inverse Gaussian laws (see Figure 7 and Figure 8). The resulting graphs for 50000 bits of data confirm the intuition that the three sources behave similarly and the fact that the graphs provide correct estimations of the physical parameters.

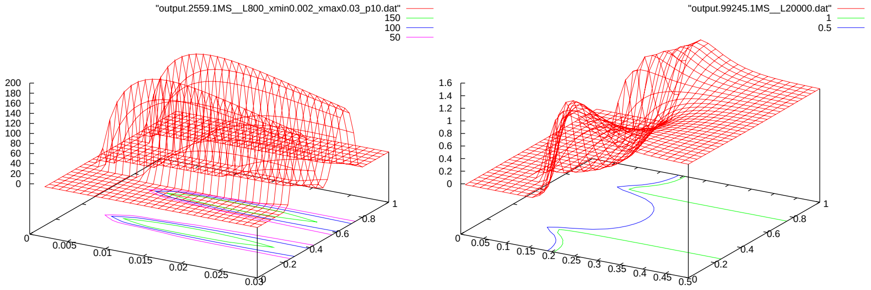

Fig. 6. Maximum likelihood estimations (2).

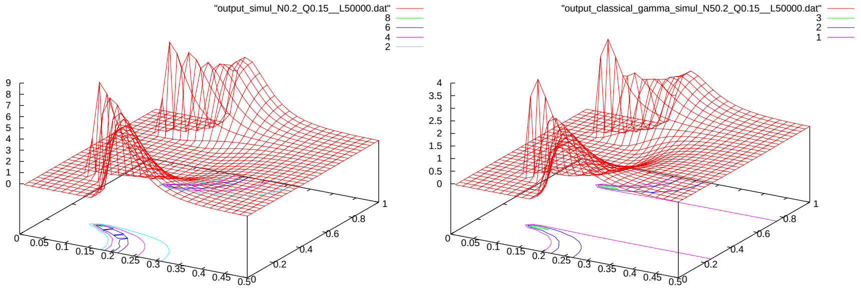

Fig. 7. Maximum likelihood estimations (3).

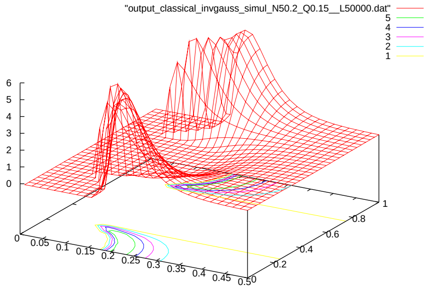

Fig. 8. Maximum likelihood estimations (4).

5 Conclusion

We have seen that the generic design of TRNGs that consists in a ring oscillator sampled via a type-D flip-flop is amenable to a comprehensive statistical study.

On the conception side, we provide practical formulas and an experimental method to control the main security parameters of a TRNG — in particular its entropy rate and the probability biases in the output bits. Incidentally, our experiments give an explanation for the observation reported in the literature that ring oscillators have a tendency to couple with each other. Indeed, there is at least one coupling between ring oscillators by the way of the global deterministic jitters. Some authors [7] conclude that this phenomenon significantly reduces the amount of randomness produced by a TRNG. Our observations tend to show that the global deterministic jitters do not impede the randomness of a TRNG by itself, but can lead to dangerous overestimations.

On the attackers' side, we have seen that it is easy to recover the statistical parameters of an oversampled oscillator from a sufficiently large amount of output bits. In extreme cases, we note that this allows one to implement optimized brute-force attacks on the unknown output vectors of such a generator. Indeed, one may determine the corresponding distributions and try out the most probable values first (see [10] for a detailed analysis).

Finally, on the performance side, we observe that, in order to achieve a near-to-one quality factor and obtain almost perfectly random bit-sequences, it is necessary to sample the ring oscillator at a very low frequency. Interestingly, our statistical model uncovers some possible approach to improve the throughput of such a TRNG. Indeed, our theoretical study (Proposition 1) suggests that the residual biases of the generator would be considerably lowered if one could lock the term $\cos(2\pi\nu)$ to a very small value.

Acknowledgments. We are very thankful to Frédéric Valette for his support to this project and for his contributions to the physical experiments. Our work also greatly benefited from early discussions with Sébastien Kunz-Jacques, who brought the idea of using specific statistical tests, and with Jean-Michel Lévy-Bruhl, who suggested the need for a simpler mathematical model.

References

1. A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication (SP) 800-22 rev. 1, 2008. Available at `http://csrc.nist.gov/CryptoToolkit/tkrng.html`.
2. A. Abcunas, C. Coughlin, G. Pedro, and D. Reisberg. Evaluation of random number generators on FPGA's. Technical report, Worcester Polytechnic Institute, 2004.
3. Holger Bock, Marco Bucci, and Raimondo Luzzi. An offset-compensated oscillator-based random bit source for security applications. In *CHES*, pages 268–281, 2004.
4. W. Coppock and C. Philbrook. A mathematical and physical analysis of circuit jitter with application to cryptographic random bit generation. Technical report, Worcester Polytechnic Institute, 2005.

5. David Roxbee Cox and Hilton David Miller. *The Theory of Stochastic Processes*. CRC Press, 1977.
6. Alper Demir, Amit Mehrotra, and Jaijeet Roychowdhury. Phase noise in oscillators: a unifying theory and numerical methods for characterisation. In *DAC '98: Proceedings of the 35th annual conference on Design automation*, pages 26–31, New York, NY, USA, 1998. ACM.
7. Markus Dichtl and Jovan Dj. Golic. High-speed true random number generation with logic gates only. In *CHES*, pages 45–62, 2007.
8. Michael Epstein, Laszlo Hars, Raymond Krasinski, Martin Rosner, and Hao Zheng. Design and implementation of a true random number generator based on digital circuit artifacts. In *CHES*, pages 152–165, 2003.
9. Wolfgang Killmann and Werner Schindler. A design for a physical RNG with robust entropy estimators. In *CHES*, pages 146–163, 2008.
10. John Pliam. The disparity between work and entropy in cryptology. Cryptology ePrint Archive, Report 1998/024, 1998. http://eprint.iacr.org/.
11. Werner Schindler. A stochastical model and its analysis for a physical random number generator presented at CHES 2002. In *Cryptography and Coding*, pages 276–289, 2003.
12. Werner Schindler and Wolfgang Killmann. Evaluation criteria for true (physical) random number generators used in cryptographic applications. In *CHES*, pages 431–449, 2002.
13. C. E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27:379–423, 623–656, 1948.
14. B. Sunar, W. J. Martin, and D. R. Stinson. A provably secure true random number generator with built-in tolerance to active attacks. *IEEE*, 2007.
15. Henk C. Tijms. *A first course in stochastic models*. Wiley, 2003.
16. B. Valtchanov, A. Aubert, F. Bernard, and V. Fischer. Modeling and observing the jitter in ring oscillators implemented in FPGAs. In *11th IEEE Workshop on Design and Diagnostics of Electronic Circuits and Systems*, pages 1–16. IEEE, 2008.

A Computing probabilities and source entropy

This section provides the mathematical justifications and additional details related to Section 2.

A.1 Exact expression of probabilities by means of Fourier series

Fourier coefficients of $\varphi(t)$. From the point of view of an outside observer, the state of the generator at a given time t corresponds to a certain probability measure on the phase $\varphi(t)$.

More precisely, let $p_t(x \mid \xi)$ be the density of probability (possibly a distribution) of $\varphi(t)$ after a certain experiment described by precondition ξ. We introduce the Fourier coefficients of $p_t(x \mid \xi)$:

$$c_t(k \mid \xi) = \int_{-\infty}^{+\infty} p_t(x \mid \xi)\, e^{-2\pi ikx} dx \tag{20}$$

for every $k \in \mathbb{Z}$.

Remark 4. We note that $c_t(0 \mid \xi) = \int_{-\infty}^{+\infty} p_t(x \mid \xi)\, dx = 1$.

Remark 5. The reason why we restrict k to integer values is that we are only interested in the probability measure of $\overline{\varphi}(t) = \varphi(t) \mod 1$, which is described by the 1-periodic density function:

$$\overline{p_t}(x \mid \xi) = \sum_{k \in \mathbb{Z}} p_t(x + k \mid \xi) \tag{21}$$

Indeed we observe that

$$c_t(k \mid \xi) = \sum_{u \in \mathbb{Z}} \int_0^1 p_t(x + u \mid \xi)\, e^{-2\pi i k x} dx \tag{22}$$

$$= \int_0^1 \overline{p_t}(x \mid \xi)\, e^{-2\pi i k x} dx \tag{23}$$

Assuming that the inverse formula for Fourier series holds for $c_t(k \mid \xi)$, we obtain:

$$\overline{p_t}(x \mid \xi) = \sum_{k \in \mathbb{Z}} c_t(k \mid \xi)\, e^{2\pi i k x} \tag{24}$$

Effect of time evolution. The following lemma expresses the effect of time evolution on the Fourier coefficient of a density of probability $p_t(x \mid \xi)$.

Lemma 1. *Assume an average drift speed μ and volatility σ^2 ($\sigma > 0$) for the Wiener process $\varphi(t)$. For any $t_0 \leq t$ and for every precondition ξ concerning only events prior to t_0, we have*

$$c_t(k \mid \xi) = c_{t_0}(k \mid \xi)\; e^{-2\pi i \mu (t - t_0)\, k}\; e^{-2\pi^2 \sigma^2 (t - t_0)\, k^2} \tag{25}$$

Proof. Let $f(x) = \frac{1}{\sigma\sqrt{2\pi(t-t_0)}}\ \exp \frac{-(x-\mu(t-t_0))^2}{2\sigma^2(t-t_0)}$ be the density probability of the Gaussian distribution with mean $\mu(t - t_0)$ and variance $\sigma^2(t - t_0)$. By construction of Wiener processes (Eq. 1), we have that $p_t(x \mid \xi) = p_{t_0}(x \mid \xi) * f(x)$ where $*$ denotes the convolution product. The result then follows from the property of Fourier transform w.r.t. convolution, and the computation of Fourier coefficients for normal distributions. □

Notation. Let $\boldsymbol{c}_t(\xi)$ denote the infinite vector $(c_t(k \mid \xi))_{k \in \mathbb{Z}}$. Let $\boldsymbol{\delta}_k$ be the Dirac (infinite) column vector with a one in k-th position, and $\boldsymbol{\pi}_j$ be Dirac (infinite) row vector with a one in j-th position.

The linear relation above is written

$$\boldsymbol{c}_t(\xi) = \boldsymbol{E}[t - t_0]\; \boldsymbol{c}_{t_0}(\xi) \tag{26}$$

where $\boldsymbol{E}[t - t_0]$ denotes the $(t - t_0)$-*evolution operator* with coefficient $(j, k) \in \mathbb{Z}^2$ given by:

$$\boldsymbol{\pi}_j\, \boldsymbol{E}[t - t_0]\, \boldsymbol{\delta}_k = \begin{cases} 0 & \text{if } j \neq k \\ e^{-2\pi i \mu (t-t_0)\, k}\; e^{-2\pi^2 \sigma^2 (t-t_0)\, k^2} & \text{otherwise if } j = k \end{cases} \tag{27}$$

Remark 6. Let $\mathbf{1} = (1)_{k\in\mathbb{Z}}$ denote the vector made of ones. We note that $\sigma > 0$ implies that for any $t > 0$, $\|\boldsymbol{E}[t]\ \mathbf{1}\|_1 < \infty$.

Effect of sampling. The next lemma expresses the effect of sampling a bit b on the Fourier coefficient of a density $p_t(x \mid \xi)$.

Lemma 2. *For any t and for every precondition ξ concerning only events prior to t, we have*

$$c_t(j \mid \xi,\ s(t) = b) = \frac{1}{P} \sum_{k\in\mathbb{Z}} \gamma_b(j-k)\ c_t(k \mid \xi) \tag{28}$$

where $\gamma_b(k) = \int_0^1 g_b(x)\, e^{-2\pi ikx} dx$ is the k-th Fourier coefficient of the (periodic) sampling probability g_b, and

$$P = \mathbb{P}\left[s(t) = b \mid \xi\right] = \sum_{k\in\mathbb{Z}} \gamma_b(-k)\ c_t(k \mid \xi) \tag{29}$$

Proof. By definition and by Bayes formula on probability densities, we have

$$p_t(x \mid \xi,\ s(t) = b) = \frac{1}{P}\ p_t(x \mid \xi)\ g_b(x)$$

where

$$P = \mathbb{P}\left[s(t) = b \mid \xi\right] = \int_{-\infty}^{+\infty} p_t(x \mid \xi)\ g_b(x)\ dx$$

The result follows from the usual property of Fourier coefficients, which transform products into convolutions, and maps mean values of functions to their 0-th coefficients. □

Notation. The relation above is written

$$\boldsymbol{c}_t(\xi,\ s(t) = b) = \frac{1}{P}\ \boldsymbol{S}[b]\ \boldsymbol{c}_t(\xi) \tag{30}$$

where $\boldsymbol{S}[b]$ denotes the *b-sampling operator* with coefficient (j, k) given by

$$\boldsymbol{\pi}_j\ \boldsymbol{S}[b]\ \boldsymbol{\delta}_k = \gamma_b(j-k) \tag{31}$$

and $P = \pi_0\ \boldsymbol{S}[b]\ \boldsymbol{c}_t(\xi)$.

Exact expressions of the probabilities. We may now determine the probabilities of sampling arbitrary bit patterns from a jittered oscillator.

Proposition 3. *Let $A_0 = e^{-2\pi i\mu}$ and $B_0 = e^{-2\pi^2\sigma^2}$. For any $x \in \mathbb{R}$, let $\mathbf{1}_x = (e^{-2i\pi kx})_{k\in\mathbb{Z}}$. Using the other vector notations above, we have for every $t > 0$,*

$$\begin{aligned} p_{1,x}(t) &= \mathbb{P}\left[s(t) = 1 \mid \varphi(0) = x\right] && (32)\\ &= \pi_0\ \boldsymbol{S}[1]\ \boldsymbol{E}[t]\ \mathbf{1}_x && (33)\\ &= \sum_{k\in\mathbb{Z}} \gamma_1(-k)\, e^{-2i\pi kx} A_0^{tk} B_0^{tk^2} && (34) \end{aligned}$$

and for every $t_1 < t_2 < \ldots < t_n$*, letting* $i_0 = i_n = 0$*, we have*

$$\begin{aligned} f_{\boldsymbol{b}}(\boldsymbol{t}) &= \mathbb{P}\left[s(t_1) = b_1, \ldots, s(t_n) = b_n\right] && (35)\\ &= \pi_0 \; \boldsymbol{S}[b_n] \; \boldsymbol{E}[t_n - t_{n-1}] \; \ldots \; \boldsymbol{S}[b_2] \; \boldsymbol{E}[t_2 - t_1] \; \boldsymbol{S}[b_1] \; \boldsymbol{\delta}_0 && (36)\\ &= \sum_{(i_1, \ldots, i_{n-1}) \in \mathbb{Z}^{n-1}} \; \prod_{k=0}^{n-1} \gamma_{b_k}(i_k - i_{k+1}) \; A_0^{\sum_{k=1}^{n-1} i_k (t_{k+1} - t_k)} \; B_0^{\sum_{k=1}^{n-1} i_k^2 (t_{k+1} - t_k)} && (37) \end{aligned}$$

Note that the expression of $f_{\boldsymbol{b}}(\boldsymbol{t})$ shows in particular that $(s(t))_{t \in \mathbb{R}}$ is a stationary source. For numerical computations, for $|B_0|$ small enough, we observe that the expression of $f_{\boldsymbol{b}}(\boldsymbol{t})$ can be approximated by means of a product of n finite matrices.

Proof. We observe that

$$\begin{aligned} p_1(t) &= \mathbb{P}\left[s(t) = 1 \mid \varphi(0) = x\right] \\ &= \pi_0 \; \boldsymbol{S}[b] \; \boldsymbol{c}_t(\varphi(0) = x) \qquad \text{by Lemma 2} \\ &= \pi_0 \; \boldsymbol{S}[b] \; \boldsymbol{E}[t] \; \boldsymbol{c}_0(\varphi(0) = x) \qquad \text{by Lemma 1} \\ &= \pi_0 \; \boldsymbol{S}[b] \; \boldsymbol{E}[t] \; \mathbf{1}_x \qquad \text{by definition of Fourier coefficients } c_t(k|\varphi(0) = x) \end{aligned}$$

Similarly, letting $q_n = \mathbb{P}\left[s(t_1) = b_1, \ldots, s(t_n) = b_n\right]$, we have for all $n > 0$

$$\begin{aligned} & q_n \, \boldsymbol{c}_{t_n}(s(t_1) = b_1, \ldots, s(t_n) = b_n) \\ &= \frac{q_n}{P_n} \; \boldsymbol{S}[b_n] \; \boldsymbol{c}_{t_n}(s(t_1) = b_1, \ldots, s(t_{n-1}) = b_{n-1}) \\ &= q_{n-1} \; \boldsymbol{S}[b_n] \; \boldsymbol{c}_{t_n}(s(t_1) = b_1, \ldots, s(t_{n-1}) = b_{n-1}) \\ &= q_{n-1} \; \boldsymbol{S}[b_n] \; \boldsymbol{E}[t_n - t_{n-1}] \; \boldsymbol{c}_{t_{n-1}}(s(t_1) = b_1, \ldots, s(t_{n-1}) = b_{n-1}) \\ &= \boldsymbol{S}[b_n] \; \boldsymbol{E}[t_n - t_{n-1}] \; \big(q_{n-1} \; \boldsymbol{c}_{t_{n-1}}(s(t_1) = b_1, \ldots, s(t_{n-1}) = b_{n-1})\big) \end{aligned}$$

where $P_n = \mathbb{P}\left[s(t_n) = b_n \mid s(t_1) = b_1, \ldots, s(t_{n-1}) = b_{n-1}\right]$.

Given that $q_0 \, \boldsymbol{c}_{t_0}() = \boldsymbol{\delta}_0$ and $\boldsymbol{E}[t_1 - t_0] \; \boldsymbol{\delta}_0 = \boldsymbol{\delta}_0$, we obtain by induction on n:

$$\begin{aligned} & q_n \, \boldsymbol{c}_{t_n}(s(t_1) = b_1, \ldots, s(t_n) = b_n) \\ & \qquad = \boldsymbol{S}[b_n] \; \boldsymbol{E}[t_n - t_{n-1}] \; \ldots \; \boldsymbol{S}[b_2] \; \boldsymbol{E}[t_2 - t_1] \; \boldsymbol{S}[b_1] \; \boldsymbol{\delta}_0 \end{aligned}$$

The first expression of $f_{\boldsymbol{b}}(\boldsymbol{t})$ follows from $\pi_0 \, \boldsymbol{c}_t(\xi) = c_t(0|\xi) = 1$.

In the end, we obtain the desired final expressions by expanding the matrix products (the conditions $\sigma > 0$, $t > 0$ and $t_1 < \ldots < t_n$ ensuring that every sum is absolutely convergent). □

A.2 Approximate expressions of probabilities and entropy

Consider the function $g_1(x)$ defined in Section 2. The Fourier coefficient of $g_1(x)$ are given by

- $\gamma_1(0) = \frac{1}{2}$;

- for every $k \neq 0$, $\gamma_1(2k) = 0$; and
- for every k, $\gamma_1(2k+1) = \frac{i}{(2k+1)\pi}$.

From $g_0 + g_1 = 1$, we also deduce that $\gamma_0(0) = \frac{1}{2}$ and $\gamma_0(k) = -\gamma_1(k)$ for $k \neq 0$. In particular, the exact expression of $p_{1,x}(t)$, taken from Proposition 3, becomes

$$\begin{aligned} p_{1,x}(t) &= \sum_{k \in \mathbb{Z}} \gamma_1(-k)\, e^{-2\pi i k(\mu t + x)} e^{-2\pi^2 \sigma^2 t k^2} && (38) \\ &= \frac{1}{2} - \frac{2}{\pi} \sum_{N=0}^{+\infty} \frac{\sin(2\pi(\mu t + x)(2N+1))}{2N+1}\, e^{-2\pi^2\sigma^2 t(2N+1)^2} && (39) \end{aligned}$$

We now focus on periodic sampling times: $\boldsymbol{t} = (0, \Delta t, \ldots, (n-1)\Delta t)$ for some period $\Delta t > 0$. Let $Q = \sigma^2 \Delta t$ and $\nu = \mu\, \Delta t$. Let $A = A_0^{\Delta t} = e^{-2\pi i \nu}$, $B = B_0^{\Delta t} = e^{-2\pi^2 Q}$ and $i_0 = i_n = 0$. The exact expression of $p(\boldsymbol{b}) = f_{\boldsymbol{b}}(\boldsymbol{t})$, taken from Proposition 3, becomes

$$\begin{aligned} p(\boldsymbol{b}) &= \sum_{(i_1,\,\ldots,\,i_{n-1}) \in \mathbb{Z}^{n-1}} \prod_{k=0}^{n-1} \gamma_{b_k}(i_k - i_{k+1})\ A^{\sum_{k=1}^{n-1} i_k}\ B^{\sum_{k=1}^{n-1} i_k^2} && (40) \\ &= \sum_{N=0}^{+\infty} a_N(\boldsymbol{b}) B^N && (41) \end{aligned}$$

where

$$a_N(\boldsymbol{b}) = \sum_{\sum_{k=1}^{n-1} {i_k}^2 = N} \prod_{k=0}^{n-1} \gamma_{b_k}(i_k - i_{k+1})\ A^{\sum_{k=1}^{n-1} i_k}. \qquad (42)$$

From the expressions of $\gamma_0(k)$ and $\gamma_1(k)$, we obtain in particular the first terms $a_N(\boldsymbol{b})$:

$$\begin{aligned} a_0(\boldsymbol{b}) &= \frac{1}{2^n} && (43) \\ a_1(\boldsymbol{b}) &= \gamma_{b_1}(-1)\ \gamma_{b_2}(1)\ \gamma_{b_2}(0)\ \ldots \gamma_{b_n}(0)\ A \\ &+ \gamma_{b_1}(0)\ \gamma_{b_2}(-1)\ \gamma_{b_3}(1)\ \ldots \gamma_{b_n}(0)\ A \\ &+ \ldots \\ &+ \gamma_{b_1}(0)\ \ldots \gamma_{b_{n-2}}(0)\ \gamma_{b_{n-1}}(-1)\ \gamma_{b_n}(1)\ A \\ &+ \gamma_{b_1}(+1)\ \gamma_{b_2}(-1)\ \gamma_{b_2}(0)\ \ldots \gamma_{b_n}(0)\ A^{-1} \\ &+ \gamma_{b_1}(0)\ \gamma_{b_2}(+1)\ \gamma_{b_3}(-1)\ \ldots \gamma_{b_n}(0)\ A^{-1} \\ &+ \ldots \\ &+ \gamma_{b_1}(0)\ \ldots \gamma_{b_{n-2}}(0)\ \gamma_{b_{n-1}}(+1)\ \gamma_{b_{n-1}}(-1)\ A^{-1} && (44) \\ &= \frac{A + A^{-1}}{2^{n-2}\pi^2} \left(\sum_{j=1}^{n-1} (-1)^{b_j + b_{j+1}} \right) && (45) \\ &= \frac{8}{2^n \pi^2} \cos(2\pi\nu) \left(\sum_{j=1}^{n-1} (-1)^{b_j + b_{j+1}} \right) && (46) \end{aligned}$$

We now address the development of $H_n = -\sum_{\boldsymbol{b}\in\{0,1\}^n} p(\boldsymbol{b}) \log_2 p(\boldsymbol{b})$. Given that $(1+x)\ln(1+x) = x + \sum_{N=2}^{+\infty} \frac{(-1)^N}{N(N-1)}\, x^N$ for $|x| < 1$, and that $p(\boldsymbol{b})$ tends to $a_0(\boldsymbol{b}) = \frac{1}{2^n}$ when $B \to 0$, we have for sufficiently small values of B:

$$
\begin{aligned}
-p(\boldsymbol{b}) \log_2(p(\boldsymbol{b})) &= np(\boldsymbol{b}) - \frac{1}{2^n \ln(2)} (2^n p(\boldsymbol{b})) \ln(2^n p(\boldsymbol{b})) && (47)\\
&= np(\boldsymbol{b}) - \frac{1}{2^n \ln(2)} \sum_{N=2}^{+\infty} \frac{(-1)^N}{N(N-1)}\, \epsilon(\boldsymbol{b})^N && (48)
\end{aligned}
$$

where we use $\epsilon(\boldsymbol{b}) = 2^n p(\boldsymbol{b}) - 1$ to denote the *bias* of a vector $\boldsymbol{b}$. Using that $\sum_{\boldsymbol{b}\in\{0,1\}^n} p(\boldsymbol{b}) = 1$ and $a_0(\boldsymbol{b}) = \frac{1}{2^n}$, we obtain

$$
\begin{aligned}
H_n &= n - \frac{1}{2^n \ln(2)} \sum_{\boldsymbol{b}\in\{0,1\}^n} \sum_{N=2}^{+\infty} \frac{(-1)^N}{N(N-1)} \left(\sum_{M=1}^{+\infty} 2^n a_M(\boldsymbol{b}) B^M \right)^N && (49)\\
&= n - \frac{2^{n-1}}{\ln(2)} \sum_{\boldsymbol{b}\in\{0,1\}^n} a_1(\boldsymbol{b})^2\, B^2 + O(B^3) && (50)
\end{aligned}
$$

But, by the previous expression of $a_1(\boldsymbol{b})$, we have

$$
\begin{aligned}
\sum_{\boldsymbol{b}\in\{0,1\}^n} a_1(\boldsymbol{b})^2 &= \frac{64}{2^{2n}\pi^4} \cos^2(2\pi\nu) \sum_{\boldsymbol{b}\in\{0,1\}^n} \left(\sum_{j=1}^{n-1} (-1)^{b_j + b_{j+1}} \right)^2 && (51)\\
&= \frac{64}{2^{2n}\pi^4} \cos^2(2\pi\nu)\; 2^n (n-1) && (52)\\
&= \frac{64(n-1)}{2^n \pi^4} \cos^2(2\pi\nu) && (53)
\end{aligned}
$$

Therefore, we may conclude that $H_n = n - \dfrac{32(n-1)}{\pi^4 \ln(2)} \cos^2(2\pi\nu)\, B^2 + O(B^3)$.

A.3 Safe bounds on bias and entropy

The proof of Corollary 1 runs as follows.

Proof (of Corollary 1). By definition $H_n = H(s((n-1)\mathit{\Delta} t), \ldots, s(\mathit{\Delta} t), s(0))$ and we have that

$$
\begin{aligned}
H_{n+1} - H_n &= H(s(n\mathit{\Delta} t) \mid s((n-1)\mathit{\Delta} t), \ldots, s(\mathit{\Delta} t), s(0))\\
&\geq H(s(n\mathit{\Delta} t) \mid \varphi((n-1)\mathit{\Delta} t)\\
&= H(s(\mathit{\Delta} t) \mid \varphi(0))\\
&= \int_0^1 H(s(\mathit{\Delta} t) \mid \varphi(0) = x)\, dx
\end{aligned}
$$

but

$$H(s(\varDelta t) \mid \varphi(0) = x) = 1 - \frac{1+\epsilon}{2}\log_2(1+\epsilon) - \frac{1-\epsilon}{2}\log_2(1-\epsilon)$$
$$= 1 - \frac{\epsilon^2}{2\ln(2)} + O(\epsilon^3)$$

where $\epsilon = 2\,\mathbb{P}\left[s(\varDelta t) = 1 \mid \varphi(0) = x\right] - 1 = \frac{4}{\pi}\sin(2\pi(\nu + x))\, e^{-2\pi^2 Q} + O(e^{-4\pi^2 Q})$. The results follows from replacement of ϵ and by integration. (Equation 39 of Section A.2 in appendix shows that the last $O(.)$ is indeed uniform in x.) □

Next, we give a proof of Proposition 2.

Proof (of Proposition 2). Using the expression of $p(\boldsymbol{b})$ at Equation (42) and the fact that $\gamma_b(0) = \frac{1}{2}$, we have that

$$\epsilon(\boldsymbol{b}) \;=\; 2^n p(\boldsymbol{b}) - 1 \tag{54}$$
$$= \sum_{(i_1,\ldots,i_{n-1})\neq 0} \prod_{k=0}^{n-1} (2\;\gamma_{b_k}(i_k - i_{k+1}))\; A^{\sum_{k=1}^{n-1} i_k}\; B^{\sum_{k=1}^{n-1} i_k^2} \tag{55}$$

Since $|A| = 1$, $B > 0$ and for every k, $|\gamma_b(k)| \leq \frac{1}{2}$, we obtain

$$|\epsilon(\boldsymbol{b})| \;\leq\; \sum_{(i_1,\ldots,i_{n-1})\neq 0} B^{\sum_{k=1}^{n-1} i_k^2} \;=\; \vartheta(B)^{n-1} - 1 \tag{56}$$

The lower bound of H_n results the fact that the function $x \mapsto x\log_2 x$ is monotone:

$$-\,p(\boldsymbol{b})\log_2(p(\boldsymbol{b})) = np(\boldsymbol{b}) - \frac{1}{2^n}(2^n p(\boldsymbol{b}))\log_2(2^n p(\boldsymbol{b})) \tag{57}$$
$$\geq np(\boldsymbol{b}) - \frac{1}{2^n}\vartheta(B)^{n-1}\log_2\vartheta(B)^{n-1} \tag{58}$$

Hence, by summing on $\boldsymbol{b}$, we have $H_n \geq n - \vartheta(B)^{n-1}\log_2(\vartheta(B)^{n-1}) \geq n-2$. □

B Physical justifications of differential measures

The goal of this section is to justify that the physical assumptions of Subsection 3.2 implies $V_d(\ell) \approx \ell\, s^2$ for some value s^2 that we relate to the amount of noise available in R and R'.

In line with Subsection 3.2, for simplicity, we directly model the flipping times T_k of R and assume the variables $X_k = \int_{T_k}^{T_{k+1}} \alpha(t)\,dt$ to be i.i.d. according to some distribution of mean m_X and standard deviation s_X. We model R' in a similar way using the corresponding prime symbols.

The physical assumptions of our models are the following:

(i) $s_X \ll m_X$ (small local jitters for R),

(ii) $s_{X'} \ll m_{X'}$ (small local jitters for R'), and

(iii) $\alpha(t) \approx 1$ (small deterministic perturbations on R and R').

(iv) $|\alpha'(t)| \ll \frac{1}{m_X}$ and $|\alpha'(t)| \ll \frac{1}{m_{X'}}$ (slow variations of $\alpha(t)$).

Note that the last assumption implies that the equation $X_k = \int_{T_k}^{T_{k+1}} \alpha(t)\, dt$ can be simplified into

$$T_{k+1} - T_k \approx \frac{X_k}{\alpha(T_k)} \tag{59}$$

(and similarly for $T'_{k+1} - T'_k$).

Following the notations of Subsection 3.2, from the two sequences of times $\boldsymbol{t} = (t_0, \ldots, t_n)$, $\boldsymbol{t'} = (t'_0, \ldots, t'_{n'})$, we define a rescaled sequence $\boldsymbol{\tau} = (\tau_0, \ldots, \tau_n)$ such that for every j $(t'_0 \le t_j < t'_{n'})$,

$$\frac{\tau_j}{m_{X'}} = k(j) \ + \ \frac{t_j - t'_{k(j)}}{t'_{k(j)+1} - t'_{k(j)}}, \tag{60}$$

where $k(j) = \max\{k \in \mathbb{N} \mid t'_k \le t_j\}$.

To show that $V_d(\ell) = \hat{\mathrm{V}}(\tau_\ell - \tau_0,\ \tau_{2\ell} - \tau_\ell,\ \ldots, \tau_{\lfloor \frac{n}{\ell} \rfloor \ell} - \tau_{(\lfloor \frac{n}{\ell} \rfloor - 1)\, \ell})$ is approximately proportional to ℓ, we argue that each $\tau_{j+1} - \tau_j$ independently follows a distribution with mean $m \approx m_X$ and variance $s^2 \approx s_X^2 + \left(\frac{m_X}{m_{X'}}\right)^2 s_{X'}^2$.

Indeed, by definition, we have

$$\begin{aligned} \frac{\tau_{j+1} - \tau_j}{m_{X'}} &= \frac{t_{j+1} - t'_{k(j+1)}}{t'_{k(j+1)+1} - t'_{k(j+1)}} + k(j+1) - \frac{t_j - t'_{k(j)}}{t'_{k(j)+1} - t'_{k(j)}} - k(j) &(61)\\ &= \frac{t_{j+1} - t'_{k(j+1)}}{t'_{k(j+1)+1} - t'_{k(j+1)}} + \sum_{k=k(j)}^{k(j+1)-1} \frac{t'_{k+1} - t'_k}{t'_{k+1} - t'_k} + \frac{t'_{k(j)} - t_j}{t'_{k(j)+1} - t'_{k(j)}}. &(62) \end{aligned}$$

For all $0 \le k \le n' - 1$, let

$$\epsilon'_k = \frac{\alpha(t'_k)\,(t'_{k+1} - t'_k)}{m_{X'}} - 1. \tag{63}$$

By Equation (59) and assumption (ii), ϵ'_k approximately follows a centered Gaussian distribution of variance $\frac{s_{X'}^2}{m_{X'}^2} \ll 1$. As a consequence, we may write

$$\frac{m_{X'}}{(t'_{k+1} - t'_k)} = \frac{\alpha(t'_k)}{1 + \epsilon'_k} \approx \alpha(t'_k)\,(1 - \epsilon'_k). \tag{64}$$

By assumption (iv), for $k(j) \le k \le k(j+1)$, a first-order approximation of $\alpha(t'_k)$ is $\alpha(t_j)$. Therefore, putting altogether (62) and (64) and neglecting second-order terms, we have

$$\begin{aligned} \tau_{j+1} - \tau_j \approx \alpha(t_j)\,(t_{j+1} - t_j) \ &- \ \alpha(t'_{k(j+1)})\,\epsilon'_{k(j+1)}\,(t_{j+1} - t'_{k(j+1)}) \\ &- \sum_{k=k(j)}^{k(j+1)-1} \alpha(t'_k)\,\epsilon'_k\,(t'_{k+1} - t'_k) \qquad (65) \\ &- \ \alpha(t'_{k(j)})\,\epsilon'_{k(j)}\,(t'_{k(j)} - t_j). \end{aligned}$$

We note that the first part of the equation approximately follows a Gaussian distribution of mean m_X and variance s_X^2, whereas the second half approximately (and independently) follows a centered Gaussian distribution of variance $(\frac{s_{X'}}{m_{X'}})^2\, m_X^2$. Therefore, we may conclude that the $(\tau_{j+1} - \tau_j)$ are independent outcomes of a Gaussian distribution of mean m_X and variance $s^2 = s_X^2 + s_{X'}^2 (\frac{m_X}{m_{X'}})^2$.