Mathematical Model of Physical RNGs Based On Coherent Sampling

Florent Bernard, Viktor Fischer, Boyan Valtchanov

Tatra Mt. Math. Publ. **45** (2010), 1–14

TATRA MOUNTAINS
Mathematical Publications

MATHEMATICAL MODEL OF PHYSICAL RNGs BASED ON COHERENT SAMPLING

Florent Bernard — Viktor Fischer — Boyan Valtchanov

ABSTRACT. Random number generators represent one of basic cryptographic primitives used in creating cryptographic protocols. Their security evaluation represents very important part in the design, implementation and employment phase of the generator. One of important security requirements is the existence of a mathematical model describing the physical noise source and the statistical properties of the digitized noise derived from it. The aim of this paper is to propose the model of a class of generators using two jittery clocks with rationally related frequencies. The clock signals with related frequencies can be obtained using phase-locked loops, delay-locked loops or ring oscillators with adjusted oscillation periods. The proposed mathematical model is used to provide entropy per bit estimators and expected bias on the generated sequence. The model is validated by hardware experiments.

1. Introduction

Random number generators (RNGs) represent one of the basic cryptographic primitives used in creating cryptographic protocols. Their applications include the generation of cryptographic keys, initialization vectors, challenges, nonces and padding values, and also the implementation of counter-measures against side-channel attacks, etc. Depending on the intended security level, RNGs aimed at cryptographic applications must fulfill several security requirements, but first of all, their output values must have good statistical properties and be unpredictable.

While deterministic (or pseudo-random) RNGs can easily fulfill the first condition, their output can be guessed with a non negligible probability because of

2010 Mathematics Subject Classification: Primary: 94A60, 65C10; Secondary: 14G50, 60G50.
Keywords: physical random number generators, stochastic model, random jitter, applied cryptography, data security, hardware architectures.
Supported by the Grant NIL-I-004 from Iceland, Liechtenstein and Norway through the EEA Financial Mechanism and the Norwegian Financial Mechanism.

an existing underlying algorithm. This is the reason why such a generator must be cryptographically strong and initialized by a truly random seed. On the other side, physical (or true-random) RNGs use some uncontrollable physical phenomena and generated numbers are unpredictable, but their statistical parameters are very often insufficient and have to be enhanced by post-processing.

Recently, a very frequent requirement in RNGs design refers to their feasibility in logic devices, such as Application Specific Integrated Circuits (ASICs) or Field Programmable Logic Devices (FPGAs). Because of the nature of these devices, only limited inherent sources of randomness are available. Most generators use the timing jitter of the clock signal generated in free-running oscillators [1], [2], [3], [4], while others use the tracking jitter of phase-locked loops (PLLs) [5], [6] or metastability [7], [8].

Security evaluation represents a very important part in the RNG design and applications [9], [10]. One important requirement in RNG security evaluation is the existence of a mathematical model of the physical noise source and the statistical properties of the digitized noise derived from it [9]. In [11], K i l l m a n n and S c h i n d l e r have developed a model for the physical RNG using a pair of noisy diodes. However, it is not directly applicable to generators employing jittery clock signal especially generators based on coherent sampling. The aim of this paper is to give a mathematical model of a class of RNGs that use two noisy clocks with rationally related frequencies. Such signals can be obtained using PLLs, Delay-locked loops (DLLs) or ring oscillators with adjusted oscillation periods. The proposed mathematical model is used to estimate the expected entropy per bit of the randomness source and to compute the bias on the generated sequence. The model is validated by hardware experiments.

The paper has the following structure: Section 2 presents mathematical modeling of physical RNGs based on the coherent sampling using two related-frequency signals. In Section 3, entropy per bit estimators of the randomness source are given and the expected bias is computed thanks to the model. Finally, Section 4 concludes the paper.

2. RNG based on the coherent sampling

2.1. Sampling

The general principle of the RNG based on the sampling of a jittery clock is presented in Figure 1. At least one jittery clock signal clj having a T_{clj} period is sampled using a synchronous or asynchronous flip-flop at instants defined by a reference clock signal clk having a T_{clk} period.

The sampling process produces the '*das*' (digitized analog signal) random numbers, which can be post processed to finally give internal random numbers [10]. In this paper, we focus on the randomness extraction process, which generates *das* random numbers and determines the level of entropy included in the generated numbers. The objective is to characterize the entropy in relationship with the source of randomness and the randomness extraction in order to maximize it. If the obtained entropy is high enough, the post-processing of the *das* signal is not necessary (but still possible). For this reason, post-processing is not considered in this paper.

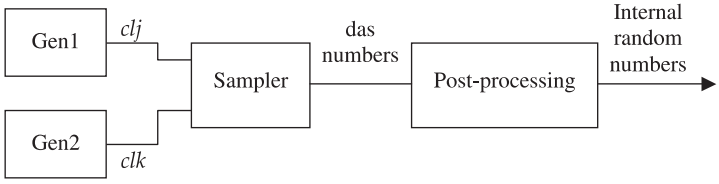

FIGURE 1. RNG based on the sampling of a jittery clock signal.

2.2. Coherent sampling

Coherent sampling is a well-known technique to capture repetitive signals at finer time intervals than a sampling clock cycle time and it is widely used to implement waveform measurement with high time resolution. More precisely, coherent sampling is defined as follows:

DEFINITION 1 (Coherent sampling)**.** Coherent sampling refers to a rational relationship between input sampled signal with frequency f_{clj}, sampling signal with frequency f_{clk}, number of cycles of a sampled signal, N_{cyc}, and number of samples, M_{samp}, such as

$$\frac{f_{clj}}{f_{clk}} = \frac{N_{cyc}}{M_{samp}}.$$

Remark 1. Even if coherent sampling is defined for arbitrary values of N_{cyc} and M_{samp} it is recommended to choose them relatively high and coprimes in order to have the highest repetition period of samples or in other words the highest resolution of the sampled signal. In the following, we will only consider coherent sampling when N_{cyc} and M_{samp} are coprimes.

One of the way to guarantee this relationship in electronic devices is to employ the PLL as clock generator of one or both related clocks. Indeed, the PLL provides two positive integer coefficients, a multiplicative one K_M and a dividing one K_D such as

$$f_{out} = \frac{K_M}{K_D} f_{in}.$$

where f_{out} is the frequency of the output signal from the PLL and f_{in} is the frequency of the input signal of the PLL.

The principle of the RNG based on coherent sampling using PLL is presented in Figure 2. The jittery clock signal clj having a T_{clj} period is sampled (using a synchronous or asynchronous flip-flop) by a signal clk having a T period, while both signal frequencies are mutually related thanks to the use of PLLs as given above. The clk signal can be produced by a quartz or another PLL. The decimator employed in the generator has to be included in the stochastic model, as it is used to extract randomness. The decimator process consists in a XOR operation of the K_D bits sampled. The result of this operation is one bit from which we want to estimate the entropy.

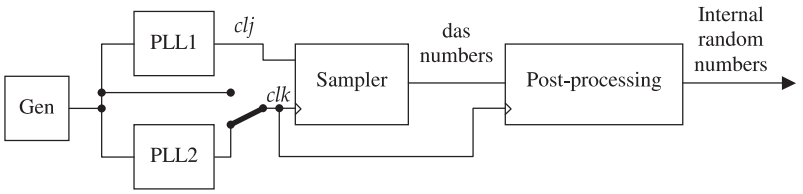

FIGURE 2. RNG based on the coherent sampling employing one or two phase-locked loops (PLLs).

2.3. Mathematical Model

First, we suppose that both clj and clk signals are ideal. That means related frequencies/periods are constant and signals do not contain any randomness.

In reality signals are seen as random variables with given distributions described with a mean and a variance. The ideal behavior is important because it corresponds to the description of the mean of these random variables.

2.3.1. Ideal behavior

DEFINITION 2 (Phase of the clj signal in time domain)**.**

$$\varphi : \begin{array}{ccc} \mathbb{R}^+ & \longrightarrow & [0, T_{clj}[, \\ t & \longmapsto & \varphi(t) \end{array}$$

is defined to be a continuous function of time t expressing the phase of the clj signal at time t.

The clj signal is sampled with the clk signal every T_{clk} seconds. Samples are obtained at discrete moment of time: $i \times T_{clk}$ with $i \in \mathbb{N}$.

Definition 3 (Samples)**.** Let $i \in \mathbb{N}$, we define φ_i the phase of the signal clj at time $i \times T_{clk}$, $\varphi_i = \varphi(i \times T_{clk})$. Moreover, the ith sample is a bit B_i defined as follows: 1 if $\varphi_i \leq \frac{T_{clj}}{2}$ and 0 otherwise.

Following Definition 3, we clearly have:

Proposition 1 (Ideal behavior)**.** *Let $i \in \mathbb{N}$,*

$$\begin{aligned} \varphi_i &= \varphi_0 + i \times T_{clk} \bmod T_{clj} \\ &= \varphi_0 + i \times T_{clk} - \left\lfloor \frac{\varphi_0 + i \times T_{clk}}{T_{clj}} \right\rfloor \times T_{clj} \end{aligned} \tag{1}$$

and

$$\begin{aligned} B_i &= 1 - \left\lfloor \frac{2\varphi_i}{T_{clj}} \right\rfloor \\ &= 1 - \left\lfloor \frac{2 \times (\varphi_0 + i \times T_{clk} \bmod T_{clj})}{T_{clj}} \right\rfloor \\ &= 1 - \left\lfloor \frac{2 \times \left(\varphi_0 + i \times T_{clk} - \left\lfloor \frac{\varphi_0 + i \times T_{clk}}{T_{clj}} \right\rfloor \times T_{clj}\right)}{T_{clj}} \right\rfloor. \end{aligned} \tag{2}$$

In the case of coherent sampling, frequencies f_{clj} and f_{clk} are rationally related: there exist two co-prime positive integers K_M and K_D such that $\frac{f_{clj}}{f_{clk}} = \frac{K_M}{K_D}$ which is equivalent to

$$K_M \times T_{clj} = K_D \times T_{clk}.$$

Definition 4 (T_Q period)**.** We call T_Q the period $K_M \times T_{clj} = K_D \times T_{clk}$. If K_D is sufficiently high, the set $\{\varphi_i\}_{i \in \{0,\dots K_D - 1\}}$ allows to rebuild the shape of clj signal.

Based on these definitions, Figure 3 presents an example of such a coherent sampling.

Then following Proposition 1, we have:

Proposition 2 (Ideal behavior of coherent sampling)**.**

$$\varphi_i = \varphi_0 + i \times T_{clk_{id}} - \left\lfloor \frac{\varphi_0}{T_{clj_{id}}} + \frac{i \times K_M}{K_D} \right\rfloor \times T_{clj_{id}} \tag{3}$$

and

$$\begin{aligned} B_i &= 1 - \left\lfloor \frac{\varphi_i}{H_{clj_{id}}} \right\rfloor \\ &= 1 - \left\lfloor 2 \times \left(\frac{\varphi_0}{T_{clj_{id}}} + \frac{i \times K_M}{K_D} - \left\lfloor \frac{i \times K_M}{K_D} + \frac{\varphi_0}{T_{clj_{id}}} \right\rfloor \right) \right\rfloor. \end{aligned} \tag{4}$$

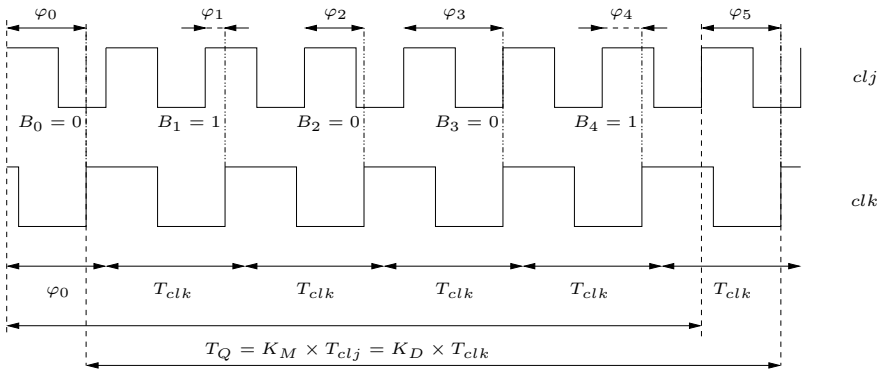

FIGURE 3. Ideal clock sampling example with rationally related frequencies.

From Equation (4), it is easy to get all informations needed to characterize the output of the RNG (e.g., number of bits equal to one per period T_Q, since if it is odd (or even), the bit after the decimation process is $'1'$ (or $'0'$), ...).

2.3.2. Behavior with timing jitter

In electronic devices, signals are not ideal because of electronic noise. They contain randomness that can be expressed in the frequency domain as a phase noise or in the time domain as the timing jitter.

DEFINITION 5 (Timing jitter)**.** Let n be a positive integer. The timing jitter δ_n is the timing deviation of a rising edge that appears at time t_n from its ideal position $n \times T_0$ where T_0 is the ideal constant period of the signal:

$$\delta_n = t_n - nT_0. \tag{5}$$

Each signal (clj or clk) contains its own absolute timing jitter. But in reality, when sampling clj with clk, we measure the relative timing jitter.

DEFINITION 6 (Relative timing jitter)**.** The relative timing jitter is obtained when supposing that the reference clock signal is jitter-free and the sampled clock clj is the only jittery clock containing both clj and clk absolute jitter contributions.

Therefore signal clk has a constant period T_{clk} and signal clj has a period which is considered to be a random variable T_j with mean T_{clj} and variance σ_j^2.

Remark 2. It is not necessary to know precisely the law of T_j since we just need the mean and the variance of this random variable.

Describing the ith sample as it is done in equation (3) makes no sense because the operation $\bmod T_{clj}$ supposes T_{clj} to be constant which is no longer the case. Instead, we use cumulative sums of realizations of T_j:

Definition 7 (Cumulative sums)**.** Let $i \in \mathbb{N}$, and let $\{T_{j_1}, \ldots, T_{j_i}\}$ be a set of i independent realizations of the random variable T_j. The cumulative sum of these realizations, denoted $T_{j_{acc}}(i)$ is defined as:

$$T_{j_{acc}}(i) := \sum_{l=1}^{i} T_{j_l}. \tag{6}$$

The following proposition gives the expression of φ_i.

Proposition 3 (Relative timing jitter behavior)**.** *Let $i \in \mathbb{N}$ and let*

$$ind(i) := max\big\{m \in \mathbb{N} \mid T_{j_{acc}}(m) < i \times T_{clk} + \varphi_0\big\}.$$

Then

$$\varphi_i = \varphi_0 + i \times T_{clk} - T_{j_{acc}}\big(ind(i)\big). \tag{7}$$

The value of $T_{j_{acc}}(m)$ is not precisely known because it depends on the relative timing jitter between signals clk and clj. In other words,

$$T_{j_{acc}}(m) = \delta_m + m \times T_{clj},$$

where δ_m has a mean 0 and a variance σ_m^2.

Using equation (7) we can see φ_i as a random variable following the same law as $\delta_{ind(i)}$ but with mean

$$\mu_{ind(i)} := i \times T_{clk} + \varphi_0 - ind(i) \times T_{clj}$$

and with variance $\sigma^2_{ind(i)}$.

2.4. Behavior in the special case of the coherent sampling

It can be seen in Figure 3 that successive samples are not sorted in an increasing order. In [12], a reorganization of these samples is proposed when K_M and K_D are co-primes. The reorganization is given with the formula

$$j(i) = i \times K_M \mod K_D \text{ for } i \text{ from 0 to } K_D - 1. \tag{8}$$

K_M and K_D are co-primes so this application is bijective. Then the reciprocal transformation is

$$i(j) = j \times K_M^{-1} \mod K_D \tag{9}$$

and we have:

$$0 < \varphi_{i(1)} - \varphi_0 \mod T_{clj} < \cdots < \varphi_{i(K_D-1)} - \varphi_0 \mod T_{clj}. \tag{10}$$

The first ($i \geq 1$) sample after the reorganization is defined to be the closest one to the initial phase $\varphi_0 = \varphi_{i(0)}$ and following samples are sorted in an increasing order. This allows to get a reconstruction of the T_{clj} period. The expression

of φ_i as a random variable can also be simplified as it is shown in the following proposition.

Proposition 4 (The random variable $\varphi_{i(j)}$)**.** *$\varphi_{i(j)}$ is a random variable with mean $\mu_{i(j)}\varphi_0 + j \times \frac{T_{clj}}{K_D} \bmod T_{clj}$ and with variance $\sigma^2_{ind(i(j))}$.*

P r o o f. According to previous definitions and notations, $\varphi_{i(j)}$ is clearly a random variable with variance $\sigma^2_{ind(i(j))}$.

Let

$$\Delta := \mu_{i(j+1)} - \mu_{i(j)} \mod T_{clj}$$

be the distance between two consecutive means of samples regarding the increasing order modulo T_{clj}. Then,

$$\Delta = \big(i(j+1) - i(j)\big) \times T_{clk} \bmod T_{clj}.$$

We should distinguish between two cases:

$$0 \leq i(j+1) - i(j) < K_D$$

or

$$-K_D < i(j+1) - i(j) < 0 \Rightarrow 0 < i(j+1) - i(j) + K_D < K_D.$$

The difference modulo K_D between $i(j+1)$ and $i(j)$ is the general case.

$$\begin{aligned}
\Delta &= \Big(\big((j+1)K_M^{-1} - jK_M^{-1}\big) \bmod K_D\Big) \times T_{clk} \bmod T_{clj} \\
&= \Big(\big(K_M^{-1}\big) \bmod K_D\Big) \times \tfrac{T_{clj} \times K_M}{K_D} \bmod T_{clj} \\
&= \Big(\big(K_M K_M^{-1}\big) \bmod K_D\Big) \times \tfrac{T_{clj}}{K_D} \bmod T_{clj} \\
&= \frac{T_{clj}}{K_D}.
\end{aligned}$$

Then,

$$\left.\begin{aligned}
\mu_{\varphi_{i(1)}} &= \mu_{\varphi_{i(0)}} + \tfrac{T_{clj}}{K_D} \\
\mu_{\varphi_{i(j+1)}} &= \mu_{\varphi_{i(j+1)}} + \tfrac{T_{clj}}{K_D}
\end{aligned}\right\} \Rightarrow \mu_{\varphi_{i(j)}} = \varphi_0 + j \times \frac{T_{clj}}{K_D}.$$

□

With the presented model of the random variable $\varphi_{i(j)}$, we are now able to give the probability for each sample to be at logic level '1'. Let us denote by $X_{i(j)}$ the random variable with values in $\{0, 1\}$, that determines the logical level of the sampled bit at time $\varphi_0 + i(j) \times T_{clk}$.

Even if the mean of $\varphi_{i(j)}$ is in the interval $[0, T_{clj}[$, the influence of the $\sigma_{ind(i(j))}$ jitter can make a realization of this random variable to be < 0 or $> T_{clj}$. For this reason, the probability to sample a $'1'$ is given by

$$P\left(X_{i(j)} =' 1'\right) = P\left(0 < \varphi_{i(j)} < \frac{T_{clj}}{2}\right) + P\left(T_{clj} < \varphi_{i(j)} < 3\frac{T_{clj}}{2}\right). \qquad (11)$$

Remark 3. The condition $\varphi_{i(j)} < 3\frac{T_{clj}}{2}$ should normally be true most of the time because $\sigma_{ind(i(j))} << \frac{T_{clj}}{2}$. This is what we suppose in the following, therefore

$$P\big(\varphi_{i(j)} < 3\frac{T_{clj}}{2}\big) = 1.$$

And we have the following proposition:

Proposition 5 (Probability to sample a '1' in a coherent sampling)**.**

$$P(X_{i(j)} =' 1') = P\left(\varphi_{i(j)} < \frac{T_{clj}}{2}\right) - P\left(\varphi_{i(j)} < 0\right) + 1 - P\left(\varphi_{i(j)} < T_{clj}\right). \quad (12)$$

3. Application: Entropy estimators and bias for the TRNG based on coherent sampling

In the previous section, we did not need to know the law of the random variable $\varphi_{i(j)}$. In the following, one has to know what is the probability distribution of the random variable. In order to model the generator behavior, designers have to investigate and to model the source of the electronic noise (law, mean, variance) inside electronic devices before employing it.

In general, it is a difficult problem, however, it is assumed that in electronic devices many independent perturbations contribute to the noise. According to the central limit theorem, many researchers assume that the source of randomness should follow a normal distribution.

To show the validity of our model, we apply this assumption on the TRNG principle based on PLLs proposed in [5].

3.1. PLL based TRNG

The principle was presented in Figure 2. Due to phase locking, the clock jitter of $T_{j_{acc}}(m)$, $\forall\, m \in \mathbb{N}$ is supposed to be constant and equals to the clock jitter obtained in one period T_j.

Using results of Section 2 and the normal distribution of the electronic noise, we can claim that $\varphi_{i(j)}$ is a random variable following a normal distribution with mean $\mu_j = \varphi_0 + j \times \frac{T_{clj}}{K_D}$ and variance σ_j^2.

Then, according to equation (12), the probability to sample a $'1'$ is given by

$$P(X_{i(j)} =' 1') = \frac{1}{\sqrt{2\pi}\sigma_j}\left(\int_0^{H_{clj_{id}}} e^{-\frac{(x-\mu_j)^2}{2\sigma_j^2}} dx \;+\; 1 \;-\; \int_{-\infty}^{T_{clj_{id}}} e^{-\frac{(x-\mu_j)^2}{2\sigma_j^2}} dx\right). \quad (13)$$

Using equation (13), we plot for each sample in one period T_Q the point $\big(i(j), P(X_{i(j)} =' 1')\big)$. Then, according to our mathematical model, we can rebuild the "ideal" period T_{clj} as it is shown in Figure 4 for parameters $K_D = 203$ and $K_M = 260$. Figure 5 represents the reconstruction of the T_{clj} period from real hardware—the FPGA device.[1] We can see that the reality is sufficiently well described by our mathematical model.

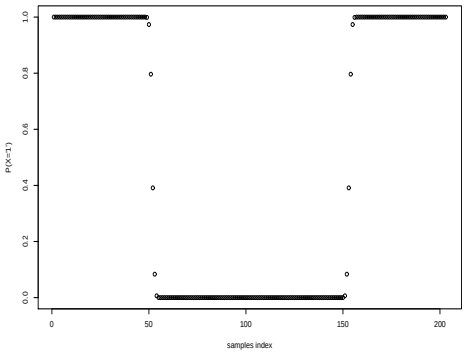

FIGURE 4. Probability of individual samples in the reconstructed T_{clj} period with $\sigma_j = 60$ ps and $\varphi_0 = \frac{\pi}{2}$ using equation (13).

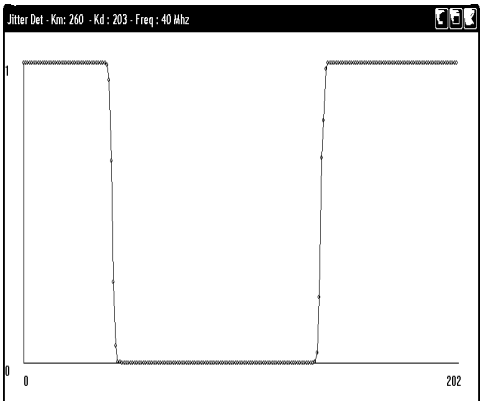

FIGURE 5. Accumulated and reconstructed T_{clj} period with $K_M = 260$, $K_D = 203$, $f_{clk} = 58$ MHz and $f_{clj} = 74.386$ MHz.

After the validation of the model, we can use it to compute the entropy per bit and the bias at the generator output, depending on the standard deviation σ_j of the clock jitter.

3.2. Bias and entropy

Following the decimation process, the output bit B_{out} is defined as follows.

DEFINITION 8 (Output bit for one period T_Q)**.**

$$B_{out} := \oplus_{i=0}^{K_D-1} X_i = \oplus_{j=0}^{K_D-1} X_{i(j)}.$$

The probability that $B_{out} = 1$ is given by

$$P(B_{out} = 1) \tag{14}$$
$$= \frac{1}{2} + (-2)^{K_D-1} \left(P(X_0 = 1) - \frac{1}{2}\right) \ldots \left(P(X_{K_D-1} = 1) - \frac{1}{2}\right).$$

[1] ACTEL Fusion evaluation board featuring the FPGA device AFS600FG256ES.

The proof of this result, based on the independence of random variables $\{X_i\}_i$, can be found in [13]. The independence of $\{X_i\}_i$ is derived from the independence of electronic noise realizations inside the chip.

If the output bits B_{out} were unbiased,

$$P(B_{out} = 1) = P(B_{out} = 0) = \frac{1}{2}.$$

Thus, according to equation (14), the bias is defined as follows:

Definition 9 (Bias)**.**

$$Bias(B_{out}) = abs\left((-2)^{K_D-1}\left(P(X_0 = 1) - \frac{1}{2}\right)\ldots\left(P(X_{K_D-1} = 1) - \frac{1}{2}\right)\right)$$

The entropy of the output bit B_{out} is defined as usually.

Definition 10 (Entropy)**.**

$$Entropy(B_{out}) =$$
$$- P(B_{out} = 1)\log_2\big(P(B_{out} = 1)\big) - P(B_{out} = 0)\log_2\big(P(B_{out} = 0)\big).$$

Then using our model, it is possible to plot the bias (Figure 6) and the entropy (Figure 7) of the output bit B_{out}, depending on the value of the clock jitter σ_j. These plots are very interesting because they can be used to derive what is the value of the jitter that is needed to obtain a sufficiently low bias and sufficiently high entropy value (close to one) for B_{out} at the output.

Example. For example, if we want the entropy to be greater than 0.999 and the bias lower than 0.001, the clock jitter must be greater than 80 ps as it can be seen in Figure 8 and 9.

4. Conclusion

Security evaluation of physical RNGs is a difficult and important task. Statistical tests are definitely not absolute criteria for their evaluation. For this reason, a mathematical characterization of the generator principle including randomness extraction (e.g., decimation process) must be done during the RGN evaluation process. The main contribution of this paper is the proposal of a statistical model of the RNG using two jittery clocks with rationally related frequencies describing random number generators based on coherent sampling. One of the way to guarantee the clock relationship is to use PLLs in hardware. They have some useful properties simplifying the mathematical model (rational related frequencies, phase locking, limited jitter accumulation. . .).

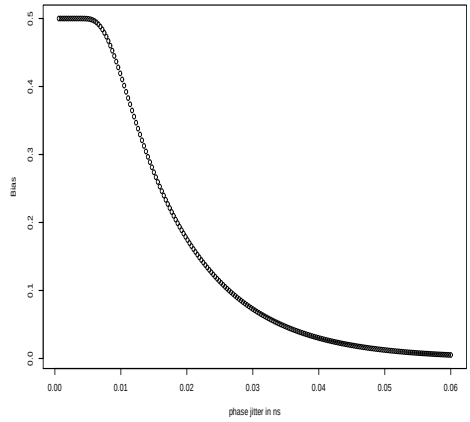

FIGURE 6. Output bias depending on the clock jitter σ_j.

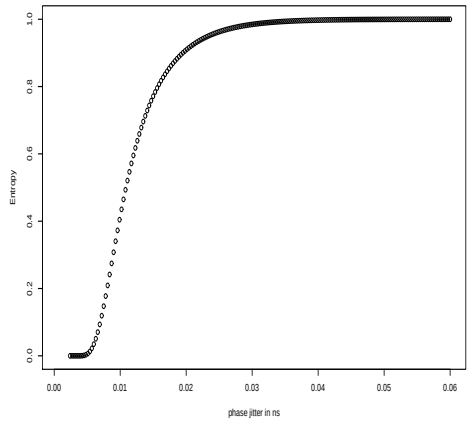

FIGURE 7. Entropy per bit depending on the clock jitter σ_j.

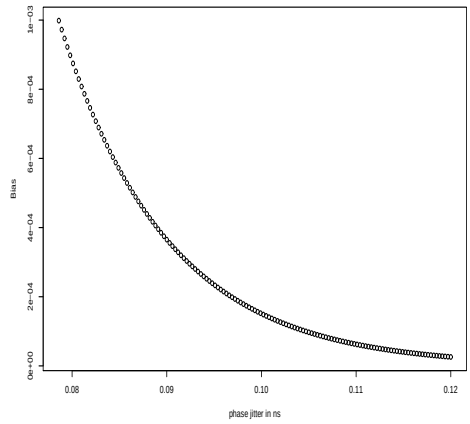

FIGURE 8. Minimum clock jitter required to satisfy $Bias(B_{out}) < 0.001$.

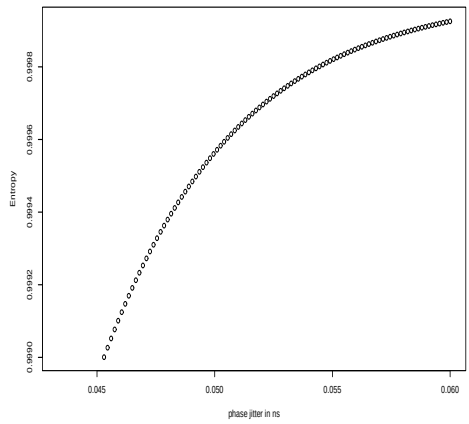

FIGURE 9. Minimum clock jitter required to satisfy $Entropy(B_{out}) < 0.999$.

The proposed model is validated by a hardware implementation. Finally, it is used to estimate the entropy per bit and the bias of the output bit-stream depending on the clock jitter value. This relationship can be used for tuning the

parameters of the generator and estimating its robustness against manipulations and attacks.

REFERENCES

[1] BUCCI, M.—LUZZI, R.: *Design of testable random bit generators*, in: Cryptographic Hardware and Embedded Systems—CHES '05, 7th International Workshop (J. Rao, B. Sunar, eds.), Lecture Notes in Comput. Sci., Vol. 3659, Springer-Verlag, Berlin, 2005, pp. 147–156.

[2] KOHLBRENNER, P.—GAJ, K.: *An embedded true random number generator for FPGAs*, in: Proc. of the 2004 ACM/SIGDA 12th Internat. Symposium on Field Programmable Gate Arrays—FPGA 04, ACM New York, NY, 2004, pp. 71–78.

[3] SUNAR, B.—MARTIN, W. J.—STINSON, D. R.: *A provably secure true random number generator with built-in tolerance to active attacks*, IEEE Trans. Comput. **56** (2007), 109–119, `http://www.cacr.math.uwaterloo.ca/~dstinson/papers/rng-IEEE.pdf`

[4] DICHTL, M.—GOLIC, J. D.: *High-speed true random number generation with logic gates only*, in: Cryptographic Hardware and Embedded Systems—CHES '07, 9th Internat. Workshop (P. Paillier, I. Verbauwhede, eds.), Lecture Notes in Comput. Sci., Vol. 4727, Springer-Verlag, Berlin, 2007, pp. 45–62.

[5] FISCHER, V.—DRUTAROVSKY, M.: *True random number generator embedded in reconfigurable hardware*, in: Cryptographic Hardware and Embedded Systems—CHES '02, 9th Internat. Workshop (B. Kaliski, Jr. et al., eds.), Lecture Notes in Comput. Sci., Vol. 2523, Springer-Verlag, Berlin, 2002, pp. 415–430.

[6] FISCHER, V.—DRUTAROVSKY, M.—SIMKA, M.—BOCHARD, N.: *High performance true random number generator in altera stratix FPLDs*, in: Field-Programmable Logic and Applications—FPL '04, 14th Internat. Conference (J. Becker et al., eds.), Lecture Notes in Comput. Sci., Vol. 3203, Springer-Verlag, Berlin, 2004, pp. 555–564.

[7] EPSTEIN, M.—HARS, L.—KRASINSKI, R.—ROSNER, M.—ZHENG, H.: *Design and implementation of a true random number generator based on digital circuit artifacts*, in: Cryptographic Hardware and Embedded Systems—CHES '03, 5th Internat. Workshop (W. Colin et al., eds.), Lecture Notes in Comput. Sci., Vol. 2779, Springer-Verlag, Berlin, 2003, pp. 152–165.

[8] VASYLTSOV, I.—HAMBARDZUMYAN, E.—KIM, Y.-S.—KARPINSKYY, B.: *Fast digital TRNG based on metastable ring oscillator*, in: Cryptographic Hardware and Embedded Systems—CHES '08, 10th Internat. Workshop (E. Oswald, P. Rohatgi, eds.), Lecture Notes in Comput. Sci., Vol. 5154, Springer-Verlag, Berlin, 2008, pp. 164–180.

[9] KILLMANN, W.—SCHINDLER, W.: *AIS 31: Functionality classes and evaluation methodology for true (physical) random number generators, version 3.1*, Bundesamt fur Sicherheit in der Informationstechnik (BSI), Bonn, 2001, `http://www.bsi.bund.de/zertifiz/zert/interpr/ais31e.pdf`.

[10] SCHINDLER, W.—KILLMANN, W.: *Evaluation criteria for true (physical) random number generators used in cryptographic applications*, in: Cryptographic Hardware and Embedded Systems—CHES '02, 9th Internat. Workshop (B. Kaliski, Jr. et al., eds.), Lecture Notes in Comput. Sci., Vol. 2523, Springer-Verlag, Berlin, 2003, pp. 431–449.

[11] KILLMANN, W.—SCHINDLER, W.: *A design for a physical RNG with robust entropy estimators*, in: Cryptographic Hardware and Embedded Systems—CHES'08, 10th Internat. Workshop (E. Oswald, P. Rohatgi, eds.), Lecture Notes in Comput. Sci., Vol. 5154, Springer-Verlag, Berlin, 2008, pp. 146–163.

[12] SIMKA, M.—DRUTAROVSKY, M.—FISCHER, V.—FAYOLLE, J.: *Model of a true random number generator aimed at cryptographic applications*, in: Proc. of the Internat. Symposium on Circuit and Systems—ISCAS '06, IEEE CAS Society, New York, NY, pp. 5619––5623, http://www.kemt.fei.tuke.sk/publication/Drutarovsky/iscas2006.pdf.

[13] DAVIES, R. B.: *Exclusive OR (XOR) and hardware random number generators*, February, 2002, http://webnz.com/robert/.

Received May 30, 2010

Université de Lyon
CNRS, UMR 5516
Laboratoire Hubert Curien
F–42000 Saint-Étienne
FRANCE

E-mail: florent.bernard@univ-st-etienne.fr
fischer@univ-st-etienne.fr
boyan.valtchanov@univ-st-etienne.fr