A Design of Reliable True Random Number Generator for Cryptographic Applications

Vittorio Bagini, Marco Bucci

Fondazione Ugo Bordoni, Via B. Castiglione 59, 00142 Roma-Italy
bagini, bucci@fub.it

Abstract. The scheme of a device that should have a simple and reliable implementation and that, under simply verifiable conditions, should generate a true random binary sequence is defined. Some tricks are used to suppress bias and correlation so that the desired statistical properties are obtained without using any pseudorandom transformation. The proposed scheme is well represented by an analytic model that describes the system behaviour both under normal conditions and when different failures occur. Within the model, it is shown that the system is robust to changes in the circuit parameters. Furthermore, a test procedure can be defined to verify the correct operation of the generator without performing any statistical analysis of its output.

Keywords: True random number generators, noise, cryptography, tests for randomness.

1 Introduction

Cryptographic systems should use only true random number generators for producing keys and other secret quantities. This paper aims at defining the scheme of a true random number generator that has a simple and reliable implementation and is not expensive in production. To ensure all these features, the generator must be able to stand large tolerances in its components without any calibration or compensation. Furthermore, possible malfunctions must be foreseen and tests to be made during prototype development, production and (possibly) operation must be defined. Since the generator is designed for cryptographic applications, the random source it uses must be suitable to be constructed in a protected and insulated environment. In this way the device can be certified to work under general and heavy operating conditions.

A popular way of generating truly random binary sequences is to sample analogical white noise after it has been quantized by means of a comparator. Because of offsets and bandwidth limitations, the generated sequence is typically affected by bias and

Ç.K. Koç and C. Paar (Eds.): CHES’99, LNCS 1717, pp. 204−218, 1999.

symbol correlation, but some tricks are used to suppress both. The bias is eliminated by sending the quantized signal into a binary counter before sampling it, whereas the bit correlation is kept under a fixed value by choosing a suitably low sampling frequency [1-5]. Therefore, in this kind of generators, defects in the bit statistics are not masked (e.g. by means of a pseudorandom transformation) but simply suppressed. This can be considered the most correct solution since the device should generate a sequence whose entropy *is* the maximum possible, not a sequence whose entropy *looks like* the maximum possible. In a certification testing one is thus forced to conclude by an analysis of the scheme that, if the output sequence looks random, i.e., if it passes the statistical tests, it is actually random.

The generator proposed in this paper (see Fig. 1) follows this scheme, but its peculiarity is that the input noise is sampled and held. This solution ensures that the input noise does not change its value during the comparator response time so that the devices in the successive stages can operate under the conditions they are designed for [3]. The proposed scheme is then well represented by an analytic model that describes the device behaviour both under normal conditions and in presence of different failures. In this way the system insensibility to changes in the circuit parameters can be evaluated. Within the same model, a test procedure can be defined to verify the correct operation of the circuit without performing any statistical analysis of its output. It is shown that, if the random source is shielded (so that no external signal is injected) and does not sustain self-oscillations, the circuit operation can be tested by simply counting the transitions of an internal signal.

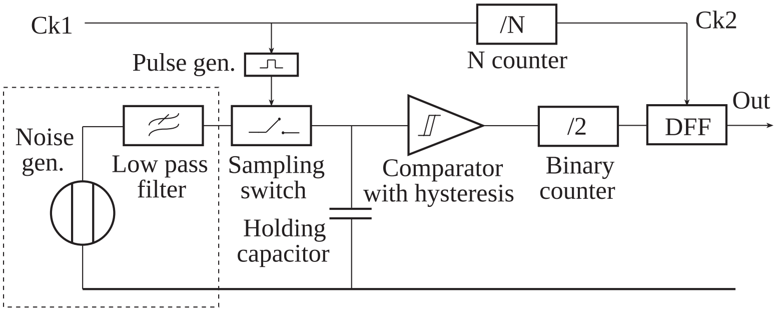

Fig. 1. Block design of the generator

The rest of the paper is organized as follows. In Section 2 each of the blocks that constitute the circuit is described and its role is explained. Furthermore, the generator self-testing procedure is proposed. In Section 3 an analytical model of the circuit is sketched and the autocorrelation function of the binary counter output, i.e., of the signal to be sampled for obtaining a binary random sequence, is given. Results of numerical simulations, which are in good agreement with the model, are also reported. A criterion for choosing the output sampling frequency, based on the form of the autocorrelation function, is then proposed. Some instructions for the practical design of the generator are given in Section 4 and conclusions of the work are presented in Section 5. The details of the calculation of the autocorrelation function are described in Appendix A and some numerical results supporting the self-testing procedure are reported in Appendix B.

2 Scheme of the Circuit

Our scheme uses a gaussian white noise source, e.g. shot noise in a directly polarized semiconductor junction. Shot noise is completely controlled by the polarization current, but its amplitude is typically very low and must therefore be strongly amplified. Since a high gain is required, some caution must be taken in the amplifier design so that external disturbances are shielded and coloured noises are not added [6]. In Fig. 1 the amplified real noise generator is represented by an ideal noise generator connected in series with a low-pass filter, whose cutoff frequency ν_0 represents the bandwidth limitations of the real generator.

The sampling and holding operation ensures that the comparator works correctly and permits to sample the binary counter output in a synchronous way. All the statistical defects that could appear in the output binary sequence if it were generated by sampling an unstable signal are therefore avoided. It will be explained in the following how the holding time, i.e., the period of the clock Ck1, must be chosen for this purpose. Details of the sample-and-hold circuit will not be examined because it is well known that such devices, operating up to some GHz, can be implemented in a simple and economical way.

To obtain simple analytic results, in the following the sampled noise that enters the comparator is supposed to be white, i.e., uncorrelated. This hypothesis is reasonable, since the sampled noise correlation is fixed by the filter bandwidth and by the input sampling frequency, i.e., the frequency of Ck1. For instance, if $x(t)$ is the signal obtained by means of a first order Butterworth filtering [7] of white noise, its autocorrelation function is, see e.g. [8],

$$R_x(\tau) = \frac{\langle x(t)x(t+\tau)\rangle}{\langle x(t)^2\rangle} = \exp\left(-2\pi\nu_0|\tau|\right) \ , \tag{1}$$

where brackets denote statistical average. If the input sampling frequency is ν_1, the correlation between two consecutive samples of $x(t)$ is

$$\exp\left(-2\pi \ \nu_0/\nu_1\right) \tag{2}$$

and is controlled by the ratio of the two frequencies.

The comparator converts the analogical noise into a binary signal. Comparators with hysteresis are generally used to obtain a fast response time. Notice that the comparator is supposed to be the slowest circuit component, so that its response time τ_c determines the whole system operating frequency. Using current technologies, this is often the case.

The binary counter ensures that its output takes on both its possible values for the same average time[1], even if its input is biased because of the offsets introduced by the comparator and by the sample-and-hold [9]. An alternative way of eliminating bias is to control the comparator threshold by means of a feedback loop, see e.g. [10]. Anyway, it is well known that this solution may introduce some degree of correlation in the output bits [2]. Furthermore, the feedback circuit is critical and requires accurate calibration, which is not needed in our scheme.

The DFF (delay flip flop) samples the binary counter output at times corresponding to the edges of the clock Ck2[2] and generates the required binary sequence. The N counter produces Ck2 as a submultiple of the clock Ck1 at which the input noise is sampled. N is chosen to keep the output bit correlation lower than a fixed value.

Since Ck2 is synchronous with Ck1 by construction, if the period of Ck1 is larger than the comparator response time τ_c[3] it is ensured that the binary counter output is sampled when it is in a stable state. Any effect due to threshold offset, asymmetry in saturation output voltages and in rising/falling times, threshold dependence upon the state of the device and bandwidth limitation of the components is therefore avoided. These effects are very insidious, since they cause fluctuations of the time required by the binary counter output for crossing the DFF threshold and can reintroduce in this way a new bias to the produced bits [3]. In fact, as long as the comparator response time is small enough, both the binary counter and the DFF work on the usual binary signals they are designed for, so that the behaviour of these devices should be extremely reliable.

On the other hand one can be persuaded that an increase in τ_c, as well as any offset and any decrease in the amplifier gain and bandwidth, can be detected. In fact, while making the output statistics worse, all these effects result in a decrease of the

[1] Corresponding to the average time between two transitions of the comparator in the same direction.

[2] Notice that the output sampling may be triggered indifferently by negative or positive edges of Ck2.

[3] Response times of the following stages are supposed to be negligible with respect to τ_c.

number of circuit internal transitions.[4] In Appendix B it is shown by numerical results that such a decrease is noticeable before the output statistics is substantially damaged. Counting the internal transitions can therefore be a simple self-testing procedure for the generator. In Appendix A the expected number of transitions during a given time interval is calculated under ideal conditions. If the counted number shows a significant departure from this expected value, it is reasonable to suspect that some circuit component is faulty enough to spoil the statistics of the produced bits, that consequently have to be discarded.

3 Model of the Circuit and Output Correlation

The amplified noise $x(t)$ is assumed to be a stationary and ergodic stochastic process and the random variable x_n represents the value sampled at the instant t_n and held until t_{n+1}. The comparator output during this interval, if there is no hysteresis and the threshold value is 0, can be defined as

$$y_n = \operatorname{sign}(x_n) = \begin{cases} +1 & \text{if} \quad x_n \geq 0 \\ -1 & \text{if} \quad x_n < 0 \end{cases} . \tag{3}$$

This transformation is known in literature as hard limiting or clipping [11]. Here the value -1 is chosen instead of 0 so that $\langle y_n \rangle = 0$ means that no bias occurs. This happens if there is no offset, i.e., the comparator threshold coincides with the sampled noise mean value, $\langle x_n \rangle = 0$. The following calculations are made under such hypothesis, that will be discussed at the end of this section. If the clipped noise produced by the comparator is unbiased, its autocorrelation function is

$$R_y(k) = \langle y_n y_{n+k} \rangle \ . \tag{4}$$

The sampled noise x_n is supposed to be δ-correlated, that is $R_x(k) = \delta_{k,\,0}$, where δ is the Kronecker symbol. As stated in the previous section, this hypothesis is not critical. In Appendix A it is shown that, as long as the comparator shows no hysteresis, $R_y(k)$ is δ-shaped too.

The binary counter output, denoted by z_n, takes on the values ± 1. For the very nature of this device, $\langle z_n \rangle = 0$ and this result holds even if there is any offset in the previous stages, causing $\langle y_n \rangle$ to differ from zero. The binary counter output autocorrelation function is

[4] This is not true for periodic disturbances, which are suppressed by a careful circuit shielding.

$$R_z(k) = \langle z_n z_{n+k} \rangle \ . \tag{5}$$

If no hysteresis is present, calculation of this function (see Appendix A) yields the result

$$R_z(k) = 2^{-|k|/2} \cos\frac{k\pi}{4} \ . \tag{6}$$

It must be remarked that, after passing through the binary counter, the noise is no longer δ-correlated.

When the comparator shows hysteresis, the relation (3) becomes

$$y_n = \begin{cases} \mathrm{sign}(x_n - x_u) & \text{if} \quad y_{n-1} = -1 \\ \mathrm{sign}(x_n - x_d) & \text{if} \quad y_{n-1} = +1 \end{cases} , \tag{7}$$

where x_u and x_d are two different threshold values and $x_u > x_d$. As it can be seen in Appendix A, the calculation of $R_y(k)$ and $R_z(k)$ is connected to the problem of counting the noise zero crossings, which in presence of hysteresis is usually considered difficult [1]. Nevertheless for discrete time evolution analytic results can be obtained if thresholds are symmetric with respect to the noise mean value, i.e., if $x_d = -x_u$. In this case, since the used input noise distribution $p(x)$ is symmetric too, the probability p of a comparator state change at any time step does not depend upon the change direction and it is given by

$$p = \int_{x_u}^{\infty} p(x)\,dx = \int_{-\infty}^{-x_u} p(x)\,dx < \frac{1}{2} \ . \tag{8}$$

In Appendix A the result

$$R_y(k) = (1-2p)^{|k|} \ , \tag{9}$$

which shows that hysteresis provides the comparator output with memory even if the input noise is white, is obtained. Furthermore in Appendix A it is shown that

$$R_z(k) = \left[r(p)\right]^{|k|} \cos\left[k\,\theta(p)\right] \ , \tag{10}$$

where

$$r(p) = \left[(1-p)^2 + p^2\right]^{1/2} \tag{11}$$

(notice that $0 < r(p) < 1$) and

$$\theta(p) = \arc\tan\left(\frac{p}{1-p}\right) . \qquad \textbf{(12)}$$

Eq. (10) shows that the envelope of $R_z(k)$ decays exponentially for any value of the probability p. In particular, the fastest possible decay takes place for $p = 1/2$, i.e., when no hysteresis is present and Eq. (10) reduces to Eq. (6).

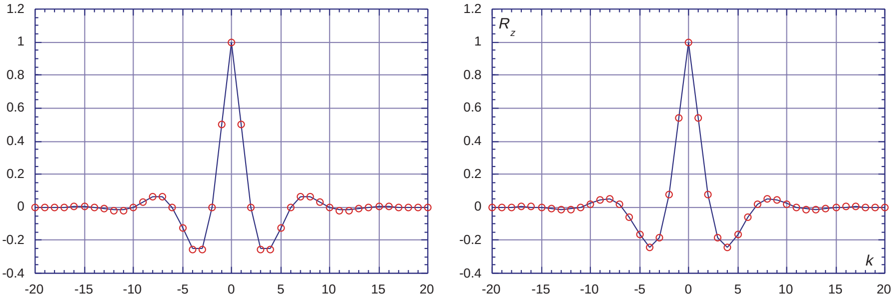

Fig. 2. Analytical form (*continuous line*) and numerical values (*circles*) of $R_z(k)$ without hysteresis (*left*) and with hysteresis (*right*). In the latter case the threshold values are ±0.1

The circuit behaviour has been numerically simulated by means of the *Simulink* software. Gaussian white noise with standard normal distribution has been used and $R_z(k)$ has been estimated as a time average using 800000 samples of z_n. The plot on the left in Fig. 2 shows the result of a simulation where no hysteresis is present, together with the theoretical curve (6), whereas the plot on the right shows the result of a simulation with $x_u = 0.1$[5], together with the theoretical curve (10). In the latter case the value of p is

$$p = \frac{1}{\sqrt{2\pi}} \int_{0.1}^{\infty} \exp\left(-\frac{x^2}{2}\right) dx \cong 0.46 \ . \qquad \textbf{(13)}$$

In both figures the agreement between theoretical values and numerical data (represented by circles) looks good. Indeed, the r.m.s. difference is about 10^{-3}.

The form of $R_z(k)$ provides us with a criterion for choosing the output sampling frequency. If a bit correlation lower than ε is required, the minimum value k_0 such that

$$[r(p)]^k < \varepsilon \quad \forall \quad k \geq k_0 \qquad \textbf{(14)}$$

[5] Notice that thresholds are measured in units of the noise mean amplitude.

has to be determined. k_0 is the optimal ratio of the input sampling frequency to the output one and therefore the value $N = k_0$ must be chosen for the N counter.[6]

Throughout the calculations no offset has been supposed. If this were the case, the comparator output would be unbiased and the binary counter would not be needed at all. The analytical study of the correlation becomes difficult and cumbersome if offset is taken into account, but the results found here under simplifying hypotheses allow a conservative estimate of the output sampling frequency even in real circumstances.

Consider indeed a comparator affected by the offset s, with thresholds $s \pm x_u$. For a given input noise this device shows a larger transition rate with respect to a comparator with no offset and thresholds $\pm x_0$, where $x_0 = |s| + x_u$. An intuitive explanation can be gained by looking at Fig. 3, where the case $s > 0$ is represented and $x(t)$ is shown instead of its samples.

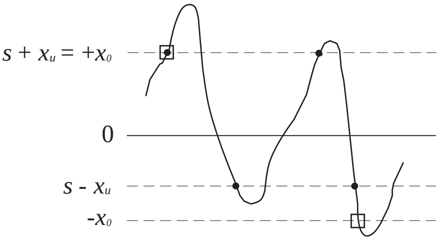

Fig. 3. Crossings of thresholds affected by offset (*dots*) and of broader thresholds with no offset (*squares*) by the same input noise

A smaller transition rate causes a slower decay of the correlation. Therefore a conservative estimate of the output sampling frequency can be obtained by considering the correlation calculated for the larger hysteresis band defined above to include offset.

4 Some Design Instructions

The designer of a random number generator of the type considered here should take into account the following set of instructions.

1) The input sampling frequency ν_1, i.e., the clock frequency of the circuit, is determined by the comparator response time τ_c through the condition

[6] N could also be chosen in order to obtain $\cos[N\theta(p)]=0$, but such a condition is more critical than the one stated in Eq. (14).

$$\nu_1 < \frac{1}{\tau_c} \ . \tag{15}$$

2) The correlation of the sampled noise must be negligible with respect to the correlation introduced by the subsequent stages. If the maximum acceptable value for the latter is ε, the amplifier cutoff frequency ν_0 must verify

$$\exp\left(-2\pi \ \nu_0 / \nu_1\right) < \varepsilon \tag{16}$$

for the filter considered here, or a similar condition for a different filter. Eq. (16) gives

$$\nu_0 > \nu_1 \frac{|\ln \varepsilon|}{2\pi} \ . \tag{17}$$

In Appendix B it is shown that a practically white input noise can be obtained even if ν_0 and ν_1 are of the same order. A similar result is obtained in [9].

3) Once the input noise distribution $p(x)$ has been estimated, the probability

$$p = \int_{x_0}^{\infty} p(x)\, dx \tag{18}$$

is determined by x_0. This positive quantity has been defined in the previous section in terms of the actual hysteresis and offset, both measured in units of the noise mean amplitude. $r(p)$ is then calculated by means of Eq. (11).

4) Finally the condition

$$N \geq \frac{|\ln \varepsilon|}{\left|\ln\left[r(p)\right]\right|} \ , \tag{19}$$

which follows from Eq. (14) with $k_0 = N$, sets the value of N and therefore of the bit rate

$$\nu_2 = \frac{\nu_1}{N} \ . \tag{20}$$

Notice that, once the bit correlation ε has been fixed, ν_2 increases with p, i.e., as it is intuitive, the bit rate grows as long as offset and comparator hysteresis, which cannot be totally suppressed, diminish with respect to the noise amplitude.

5 Conclusions

The complete unpredictability of the random numbers used by a cryptographic system is a necessary condition for the system security that can be satisfied only by means of a truly random source. On the other hand, sources of this kind often produce bit sequences whose statistics depend in a critical way on details of the implementation.

The circuit proposed in this paper belongs to a kind of true random number generators that are well known to produce unbiased bit sequences. It is designed to be insensitive as possible to fluctuations in the behaviour of the circuit components so that no calibration nor compensation is required. Furthermore, it is satisfactorily described by an analytical model that gives a relationship between the bit rate and the maximum expected bit correlation. The model gives also the expected value of the circuit internal transition rate. Since in our design phenomena that could spoil the bit statistics also slow down the circuit dynamics, counting the transitions and comparing their rate to its expected value can be a good self-testing procedure.

An actual circuit that verifies the hypotheses underlying our model generates binary sequences whose randomness is ensured by the circuit design. Such a system requires a small amount of time for its testing during production, since demanding statistical tests can be performed on prototypes only. Furthermore, true randomness of the generated bits can be controlled in a simple and effective way even while the system is operating.

Acknowledgements

This work has been carried out in the framework of the agreement between the Italian PT Administration and the Fondazione "Ugo Bordoni".

References

1. Murry, H.F.: A General Approach for Generating Natural Random Variables. IEEE Transactions on Computers C-19 (1970) 1210-1213
2. Vincent, C.H.: The Generation of Truly Random Binary Numbers. Journal of Physics E 3 No. 8 (1970) 594-598
3. Vincent, C.H.: Precautions for the Accuracy in the Generation of Truly Random Binary Numbers. Journal of Physics E 4 No. 11 (1971) 825-828
4. Maddocks, R.S., Matthews, S., Walker, E.W., Vincent, C.H.: A Compact and Accurate Generator for Truly Random Binary Digits. Journal of Physics E 5 No. 8 (1972) 542-544

5. Gude, M.: Concepts for a High Performance Random Number Generator Based on Physical Random Phenomena. Frequenz 39 No. 7-8 (1985) 187-190
6. Holman, W.T., Connelly, J.A., Dowlatabadi, A.B.: An Integrated Analog/Digital Random Noise Source. IEEE Transactions on Circuits and Systems - I 44 No. 6 (1997) 521-528
7. Terrell, T.J.: Introduction to Digital Filters. 2nd edn. Mac Millan, London (1988)
8. Bendat, J.S.: Principles and Applications of Random Noise Theory. Wiley, New York (1958)
9. Petrie, C.A.: An Integrated Random Bit Generator for Applications in Cryptography. Ph.D. Thesis, Georgia Institute of Technology (November 1997).
10. Yarza, A., Martinez, P.: A True Random Pulse Train Generator. Electronic Engineering 50 No. 614 (1978) 21-23
11. Kedem, B.: Binary Time Series. Lecture Notes in Pure and Applied Mathematics, Vol. 52. Marcel Dekker, New York (1980)
12. Papoulis, A.: Probability, Random Variables and Stochastic Processes. McGraw-Hill, New York (1965)

Appendix A: Calculation of the Autocorrelation Functions

In the following the probability $P_k(l)$ that the comparator change its state a number l of times in the interval $\left[t_n, t_{n+k}\right]$ will be needed. l is the number of noise zero crossings during the considered interval. Under the assumptions of discrete time evolution, white noise and no offset, if the distribution $p(x)$ of x_n is symmetric (not necessarily gaussian), the probability p of a comparator state change at any time step does not depend upon the change direction. Therefore $P_k(l)$ follows a binomial distribution,

$$P_k(l) = \binom{k}{l} p^l (1-p)^{k-l} \quad . \tag{A.1}$$

When the comparator shows no hysteresis,

$$p = \int_0^\infty p(x)\,dx = \frac{1}{2} \quad . \tag{A.2}$$

When hysteresis is present, the hypotheses leading to the binomial distribution $P_k(l)$ given by Eq. (A.1) still hold provided that thresholds are symmetric with respect to the sampled noise mean value, i.e., $x_d = -x_u$. In this case the value of p is given by Eq. (8).

Since the clipped noise y_n is represented by a sign function, its autocorrelation $R_y(k)$, defined as in Eq. (4), can be given the form

$$R_y(k) = \sum_{l\,\text{even}} P_k(l) - \sum_{l\,\text{odd}} P_k(l) \ . \tag{A.3}$$

It can be proven by simple algebra, using Eqs. (A.3) and (A.1), that

$$R_y(k) = (1-2p)^{|k|} \tag{A.4}$$

(here and in the following, the absolute value of k is used to generalize results to negative values of k). When no hysteresis is present, Eq. (A.2) holds and therefore

$$R_y(k) = \delta_{k,\,0} \ . \tag{A.5}$$

$R_z(k)$ can be evaluated by means of the probability $P_e(k)$ that the binary counter change its state an even number of times in $[t_n, t_{n+k}]$. Indeed $R_z(k)$ can be given a form analogous to Eq. (A.3), which is also equivalent to

$$R_z(k) = 2P_e(k) - 1 \ . \tag{A.6}$$

If at the instant t_n the comparator has changed its state an even number of times, in $[t_n, t_{n+k}]$ every transition of the counter corresponds to two transitions of the comparator. Therefore in this case the number l of comparator state changes must be equal to $4m$ or $4m+1$, where m is an integer such that $l \in \{0 \ldots k\}$, to make the counter change its state $2m$ times. On the other hand, if at the instant t_n the comparator has changed its state an odd number of times, its first transition in $[t_n, t_{n+k}]$ coincides with the first counter transition. Therefore in this case one less comparator transition is needed for an even number of counter transitions to occur and l must be equal to $4m-1$ or $4m$.

When there is no hysteresis, it follows from Eqs. (A.3) and (A.5) that the number of comparator transitions occurred before t_n has the same probability of being even or odd for every value of n. In presence of hysteresis this is no longer an exact result, but it is nevertheless a valid approximation, since $R_y(k)$ drops exponentially. In both cases thus

$$\begin{aligned} P_e(k) &= \frac{1}{2}\left(\sum_{\substack{l\equiv 0\\ \mathrm{mod}\,4}} P_k(l) + \sum_{\substack{l\equiv 1\\ \mathrm{mod}\,4}} P_k(l) \right) + \frac{1}{2}\left(\sum_{\substack{l\equiv -1\\ \mathrm{mod}\,4}} P_k(l) + \sum_{\substack{l\equiv 0\\ \mathrm{mod}\,4}} P_k(l) \right) \\ &= \frac{1}{2}\left(1 + \sum_{\substack{l\equiv 0\\ mod\,4}} P_k(l) - \sum_{\substack{l\equiv 2\\ mod\,4}} P_k(l) \right) \ . \end{aligned} \tag{A.7}$$

This result gives Eq. (A.6) the form

$$R_z(k) = \sum_{\substack{l\equiv 0 \\ \mathrm{mod}\, 4}} P_k(l) - \sum_{\substack{l\equiv 2 \\ \mathrm{mod}\, 4}} P_k(l) \ . \tag{A.8}$$

Substituting Eq. (A.1) into Eq. (A.8) gives

$$R_z(k) = \sum_n \binom{k}{2n} (-1)^n p^{2n} (1-p)^{k-2n} = \Re\left\{\left[(1-p) \pm ip\right]^k\right\} , \tag{A.9}$$

where $\Re$ denotes the real part. This expression is generalized by taking the absolute value of k and it can be put in the form (10) using the polar representation of complex numbers. If there is no hysteresis, $p = 1/2$ and Eq. (6) is obtained.

Appendix B: Number of Internal Transitions vs. Output Correlation

Counting the internal transitions is a good self-testing procedure for the generator we designed, as long as the increase in output correlation is due to phenomena that slow down the circuit dynamics and not to periodic disturbances. The connection between the number of transitions and the output correlation has been confirmed by further numerical simulations of the circuit in which two different effects have been separately considered.

The first phenomenon taken into account has been the increase in the comparator hysteresis, which, in our model, can represent lowering input noise as well as increasing offset. In each simulation 100000 samples of z_n have been generated for a fixed value of the hysteresis band half width x_0. Some of the results are shown in Table 1. Eq. (18), where $p(x)$ is the standard normal distribution, holds for the probability p and the expected number of binary counter transitions,

$$\langle N_z \rangle = \frac{p}{2} N_{samples} = 50000\, p \ , \tag{B.1}$$

is in good agreement with the counted number N_z.

In Table 1 theoretical and numerical values of $R_z(20)$ are also reported, since $N = 20$ can be a suitable value for the N counter. Theoretical values have been calculated by means of Eqs. (10-12). As the r.m.s. difference between theoretical and numerical values of $R_z(k)$ is about $5\text{x}10^{-3}$ in each experiment, simulations can be considered consistent with the model. Notice that data in parenthesis, whose absolute value is lower than the r.m.s. error, are shown only for the sake of completeness. It can be seen that a significant increase in correlation occurs when the number of transitions reduces to about one half of the initial value.

Table 1. Number of internal transitions and output correlation (both expected and numerical) for different comparator threshold values.

x_0	$\langle N_z \rangle$	N_z	$R_z(20)$	$R_z(20)$
			theor.	num.
0	25000	25166	-0.0010	(0.0045)
0.1	23029	23149	3 x 10^{-5}	(10^{-5})
0.5	15515	15463	-0.0021	(0.0006)
0.7	12208	12133	0.0105	0.0204
1	7883	7894	-0.0355	-0.0353

In the second series of simulations the effect of a finite noise bandwidth, i.e., of a correlated input, has been studied. In each experiment 100000 samples of z_n have been generated for a fixed value of the frequency ratio v_0/v_1 always assuming no hysteresis, i.e., $x_0 = 0$. Some of the results are shown in Table 2.

Table 2. Number of internal transitions (expected and numerical) and numerical output correlation for different cutoff frequencies.

v_0/v_1	$\langle N_z \rangle$	N_z	$R_z(20)$
			num.
∞	25000	25166	0.0045
0.5	24312	24384	-0.0010
0.1	16044	16071	-0.0058
0.05	11967	11953	-0.0156
0.01	5583	5706	0.1546

In this case the expected value $\langle N_z \rangle$, which looks in good agreement with the numerical value N_z, is still given by Eq. (B.1), but p has now the form

$$p = \frac{1}{\pi} \arccos\left[R_x(1)\right] = \frac{1}{\pi} \arccos\left[\exp\left(-2\pi\ \nu_0 / \nu_1\right)\right], \tag{B.2}$$

according to the well known arcsine law [12] assuming first order Butterworth filtering. It can be seen in this case too that a significant increase in correlation occurs when the number of transitions reduces to about one half of the initial value.

Notice that numerical values only of $R_z(20)$ are reported in Table 2. Indeed, the model used throughout this paper for determining the function $R_z(k)$ considers input white noise. This hypothesis is crucial for the binomial distribution (A.1) to hold. As the frequency ratio decreases, the model loses its validity and, for $\nu_0/\nu_1 \leq 0.1$, it can be seen that it gives no longer account for the numerical results. On the other hand, Table 2 shows how larger values of ν_0/ν_1, e.g. 0.5, do not cause significant deviations from the ideal case of infinite ν_0. This result confirms that the white noise hypothesis is not critical.