Random-Bit-Sequence Generator based on the Fundamental Physical Process for Secure Wideband Communication Links*

Ihor Koriakov[1,†], Oleksandr Pliushch[1,†], Maryan Kyryk[2,†], Bohdan Zhurakovskyi[3,†] and Serhii Toliupa[1,*,†]

[1] *Taras Shevchenko National University of Kyiv, 60 Volodymyrska str., 01601 Kyiv, Ukraine*

[2] *Lviv Polytechnic National University, 12 Bandery str., 79013 Lviv, Ukraine*

[3] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute," 37 Beresteiskyi ave., 03056 Kyiv, Ukraine*

Abstract

Information warfare in general and electronic warfare in particular have assumed the paramount role in modern war settings. One of the main techniques to secure electronic communication systems is the spread-spectrum method. The robustness of the pseudorandom codes used in spread-spectrum communications is considered insufficient. The paper examines the creation of an entropy source for use in random bit generators for creating true random sequences for spread-spectrum and cryptographic applications. It is shown that the real source of entropy can only be based on some fundamental physical processes; therefore, the random bit generator is designed on the base of a thermal noise generated by the active impedance in an electrical circuit. It is shown that the characteristics of the entropy source can be brought so close to those of the ideal random sources that it would take a very long time for the observer to detect the difference between the proposed entropy source and the ideal one. The designed bit generator can be used in modern communication links for spread-spectrum and cryptographic applications.

Keywords

information warfare, entropy, spread-spectrum technique, pseudorandom sequences, cryptography, random bit generator

1. Introduction

Electronic communication systems and networks play a crucial part in modern military applications [1]. Therefore, information warfare in general and electronic warfare in particular have assumed the paramount role in the strategy and tactics employed by the warring parties at modern battlefields [2, 3].

For radio communication links, three main approaches are used to achieve the aims of electronic warfare [1].

Firstly, jamming is the most widely utilized technique which is mainly employed to disrupt communication links altogether or make them impossible to be used properly.

Secondly, spoofing can be highly effective. This approach means that valid messages in the communication links are replaced by misleading or deceptive ones.

Thirdly, an alternative approach to the jamming of communication links is to intercept transmitted traffic of the enemy and use it for the aims of intelligence instead of simply disrupting (jamming) those links [4, 5].

* *CPITS 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2025, Kyiv, Ukraine*

* Corresponding author.

† These authors contributed equally.

ikor@i.ua (I. Koriakov); oleksandr.pliushch@knu.ua (O. Pliushch); marian.i.kyryk@lpnu.ua (M. Kyryk); zhurakovskybiyu@tk.kpi.ua (B. Zhurakovskyi); serhii.toliupa@knu.ua (S. Toliupa)

0009-0009-8776-1032 (I. Koriakov); 0000-0001-5310-0660 (O. Pliushch); 0000-0001-9156-9347 (M. Kyryk); 0000-0003-3990-5205 (B. Zhurakovskyi); 0000-0002-1919-9174 (S. Toliupa)

To counter the electronic warfare techniques listed above, most modern communication systems and networks include implementation of the following methods [1–3]:

- Wide use of fiber optic links to prevent useful signal suppression, as well as to preclude the interception and injection of confusing or disrupting radiations into the communication links.
- Use of highly directional antennas (adaptive antenna arrays) with low-level side lobes creates substantial problems for the enemy for useful signal detection and jamming [6].
- Use of special waveforms in time, frequency, and coding domains that allows one to counter and restrict all forms of enemy impacts: jamming, useful signals detection, and injection of deceptive or disrupting signals [7, 8].
- Use of encryption to encode sensitive messages, so that they cannot be compromised.

One can observe that at present, in addition to the listed above, the majority of electronic communication systems widely deploy different information technologies that prevent spoofing [3], but this is beyond the scope of this paper.

Although fiber optic links are more and more used on the battlefield (to control drones as well as to get visual information back to the operator), these links cannot be employed in many military settings yet. Highly directional antennas usually have big dimensions and, therefore, are visible to the enemy forces and can be easily destroyed [3].

It is well-known that the widespread utilization of modern encryption methods has mostly rendered the interception of the opposing party messages very challenging, if not altogether impossible. As a result, due to the inability to use the enemy's electronic communications to intercept the messages and try to deploy spoofing, the only viable approach is to use intensive jamming techniques [1].

As a result of the analysis made above, the vast majority of electronic communication systems commonly use an approach known as spread-spectrum communications [9–11]. If one compares this approach with the encryption/decryption of the relayed messages [12], the spread spectrum technique presents itself as the encryption/decryption of the radiofrequency signals carrying these messages [13–15].

The nature of spread-spectrum communications is such that the signal is spread over a wide radiofrequency band by deploying a pseudorandom code [16].

The opposite procedure involves the process of correlating the received pseudorandom code with the beforehand stored copy of this code at the receiver's side [17].

This correlation process, as the vital part of this spread-spectrum technique, possesses the advantage that it suppresses interference (non-correlated) by the spreading factor, which can be in the range of 20 to 60 dB [18].

As a result, the spread-spectrum technique provides the following benefits for electronic communication channels [1, 14, 15]:

- Strong resistance to interference and jamming [19].
- Multiple spread-spectrum signals transmission through communication channels using the code division multiple access (CDMA) method.
- Low probability of intercept characteristics.
- Highly accurate range measurements.

The two main types of spread-spectrum methods are known as direct sequence and frequency hopping [16].

Direct sequence spreading is more widely used [14–16]. In this method, a random code carrier is deployed to spread the spectrum of the message by multiplying useful bits by the chips of the spreading code.

The characteristics of the spreading code are vital for the spread-spectrum technique to operate efficiently [16, 20]. Usually, pseudorandom codes are generated with the help of primitive polynomials [16]. But with the advanced current state of commuter technologies, these pseudorandom codes can be compromised, which leaves the whole approach vulnerable [1].

Therefore, to secure the integrity of information over electronic communication links for both spread-spectrum techniques and encryption methods as well, one needs to obtain a code that would be random and not pseudorandom, as is the case at present [1, 10, 11]. When constructing a non-deterministic (physical, true) random bit (number, sequence) generator for spread-spectrum techniques and cryptographic applications, a high-entropy source is required [12]. Therefore, this paper aims to develop a high-entropy code with characteristics so close to the ideal ones that it will take a lot of time to detect the difference between the output signal of such a source and the ideal one. To state it differently, the length of the analyzed sequence will be unrealistically large and the electronic communication channel will never be compromised.

2. High-entropy noise generator

An efficient source of entropy can only be based on some fundamental physical process, that is, an immutable natural phenomenon, and not on some technological achievement. For example, the thermal noise voltage at the ends of a conductor (resistor) is generated by a fundamental natural phenomenon, while the noise voltage determined by the effect of avalanche breakdown of a reverse-biased p-n junction is the result of a technological achievement.

Let's consider a noise generator based on thermal noise.

One should not forget that the thermal noise voltage is created by the active component of the complex resistance of any circuit, regardless of how many resistors there are and whether there are any at all. The thermal noise electromotive force (EMF) et is equal to (in modern notation)

$$e_t = \sqrt{4\,kTRB},$$

where k is the Boltzmann constant (1.38e–23), T is the temperature in degrees Kelvin, R is the active component of the circuit resistance in Ohms, and B is the noise bandwidth in Hz.

Typically, a thermal noise generator contains a resistor and an amplifier. The equivalent circuit of such a generator is shown in Fig. 1.

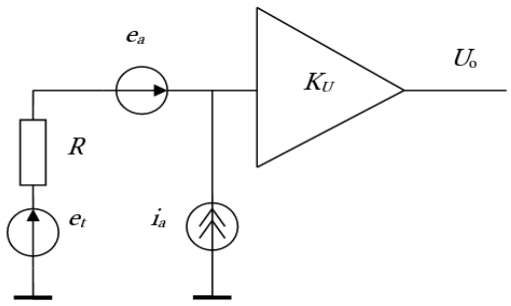

Figure 1: Equivalent circuit of a noise generator

In this figure, R is the active component of the circuit resistance, generating the EMF e_t; e_a is the source of the amplifier's noise voltage; i_a is the source of the amplifier's noise current; K_U is the amplifier's voltage gain (we assume the input resistance of the amplifier to be infinite); U_o is the amplifier's output voltage. For the noise at the output to be as random as possible, one needs to minimize the noise figure (*NF*), which determines the contribution of the amplifier's noise to the output signal:

$$NF = 1 + \frac{P_a}{P_t},$$

where P_a is the amplifier's noise power, P_t is the thermal noise power generated by the active component of the input circuit resistance. Considering the bandwidths of all the noises and the gain for all the noises to be the same, we can express NF through the parameters of the noise sources as follows:

$$NF = 1 + \frac{\frac{e_a^2}{R} + i_a^2 R}{4kT}.$$

And, if we choose the value of R that minimizes NF for given e_a and i_a, then knowing the required value of U_o, we can calculate the required gain factor K_U.

Let's consider a numerical example: an amplifier with e_a = 1.1 nV/Hz$^{1/2}$ and i_a = 8.8 pA/Hz$^{1/2}$. We assume that we take a larger R to generate more noise. We substitute a 10 kOhm resistor into the formula and get NF = 49.4. That is too high a number. For the internal noise to be at least no greater than the useful noise, NF = 2 is necessary. Using the iteration method, we get R = 120 Ohm and NF = 2.2.

This is a good result, especially since there are also sources of thermal noise inside the amplifier, which will not distort the original quality (random) noise of the resistor.

If it is required to obtain the effective value of U_o = 100 mV (for normally distributed noise this is about 0.8 V peak-to-peak), then at T = 290 K and a bandwidth of 500 MHz, we obtain:

$$K_U = \frac{U_o}{\sqrt{4kTRB}} =$$

$$= \frac{0.1}{\sqrt{4 \cdot 1.38e-23 \cdot 290 \cdot 120 \cdot 500000000}} =$$

$$= \frac{0.1}{30.98e-6} = 3227.$$

3. Circuitry of an analog noise generator based on thermal noise sources

It is important to consider several possible options and, as a result, to choose the best practical realization among them for the equivalent circuit shown in Fig. 1. Let us remind ourselves here that e_t in this figure is formed by the active component of the complex resistance of the amplifier input circuit, regardless of its configuration.

One should consider several circuit diagrams of a generator based on thermal noise. In all of them hereinafter, R is the noisy resistor, R_f is the resistor in the op-amp feedback circuit, e_t is the source of thermal noise EMF, and U_o is the op-amp output voltage. The first circuit diagram is shown in Fig. 2.

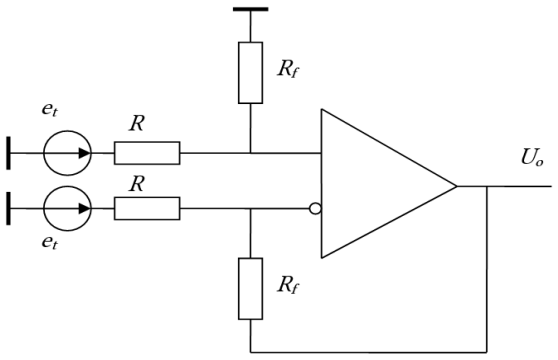

Figure 2: Circuit diagram of the first noise generator

For this circuit, we consider the resistance R_f to be significantly higher than the resistance of the noisy resistors and, since the EMFs of the resistor's noise e_t are independent, then

$$U_o = \frac{\sqrt{2} e_t R_f}{R}.$$

By doubling the resistance value of resistors R we get

$$U_o = \frac{2\sqrt{2} e_t R_f}{2R} = \frac{\sqrt{2} e_t R_f}{R}.$$

In this case, U_o remains unchanged.

Let us consider the second circuit, shown in Fig. 3.

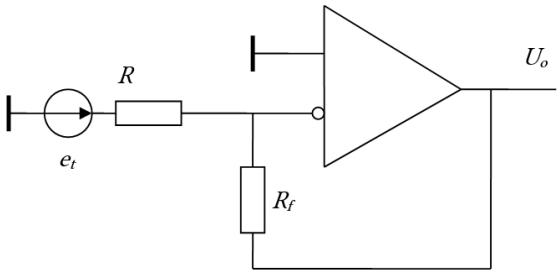

Figure 3: Circuit diagram of the second noise generator

In this diagram, the output voltage of the op-amp will be equal to

$$U_o = \frac{e_t R_f}{R}.$$

By doubling the resistance value of resistors R we get:

$$U_o = \frac{\sqrt{2} e_t R_f}{2R},$$

that is, U_o will decrease by the root of 2 times.

In the third circuit, shown in Fig. 4, the output voltage of the op-amp can be expressed as follows:

$$U_o = \frac{e_t R_f}{R_i}.$$

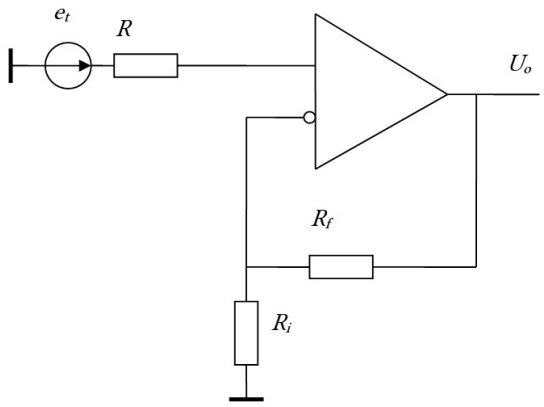

Figure 4: Circuit diagram of the third noise generator

In this case, by doubling the value of the resistor R, we obtain the following:

$$U_o = \frac{\sqrt{2} e_t R_f}{R_i},$$

that is, U_o will increase by the root of 2 times.

Let us consider the fourth option, in the form of the circuit diagram shown in Fig. 5.

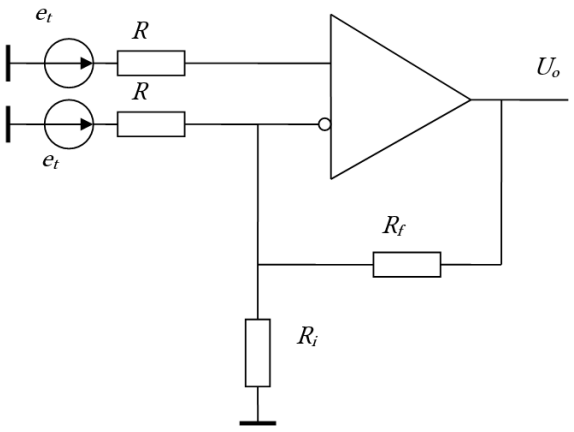

Figure 5: Circuit diagram of the third noise generator

The output voltage of the op-amp in Fig. 5 can be expressed in the following way:

$$U_o = \frac{\sqrt{2} e_t R_f}{R_i}.$$

By doubling the resistance value of resistor R, one can obtain:

$$U_o = \frac{2\sqrt{2} e_t R_f}{R_i},$$

that is, U_o will increase by 2 times.

Let us consider once again the equivalent circuits of the noise generators taken with account of the amplifier noise. There are two possible options. The first one is shown in Fig. 6.

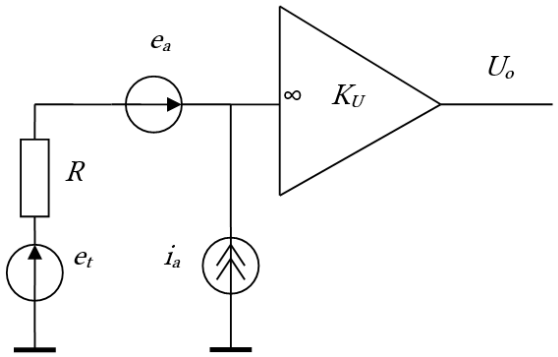

Figure 6: First variant of the equivalent circuit

In this circuit, R is the active component of the circuit resistance, generating the EMF e_t; e_a is the source of the amplifier's noise voltage; i_a is the source of the amplifier's noise current; K_U is the amplifier's voltage gain (it is assumed that the amplifier's input resistance to be infinite), and U_o is the amplifier's output voltage.

For the noise at the output to be as random as possible, that is, so that the amplifier's noise is represented in the output voltage of the op-amp to a minimum degree, one needs to minimize the noise factor *NF*, which determines the contribution of the amplifier's noise to the output signal in the following way:

$$NF = 1 + \frac{P_a}{P_t},$$

where P_a is the amplifier's noise power, P_t is the thermal noise power generated by the active component of the input circuit resistance.

Considering the bandwidths of all noises and the gain for all noises to be the same, we can express *NF* through the parameters of the noise sources as follows:

$$NF = 1 + \frac{\frac{e_a^2}{R} + i_a^2 R}{4kT}.$$

And if, given e_a and i_a, we have chosen the value of R that minimizes *NF*, then knowing the required value of U_o, we can calculate the required gain coefficient K_U.

Let us consider the second variant of the equivalent circuit that is shown in Fig. 7.

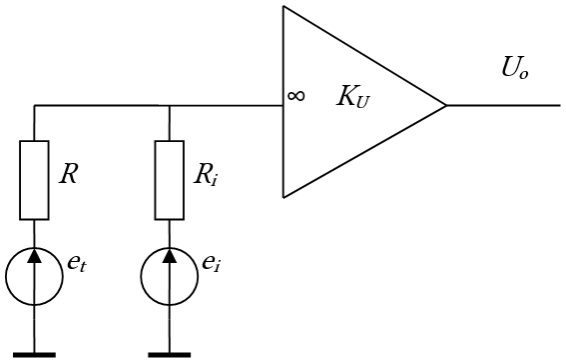

Figure 7: Second variant of the equivalent circuit

In Fig. 7, R is the resistance of the noisy resistor generating the EMF e_t, R_i is the input resistance of the amplifier generating the EMF e_i.

According to Ohm's law for the complete circuit, the maximum power from the source R can be received under the condition $R_i = R$.

Thus, the circuit of the noise generator shown in Fig. 2 should be considered the best option, in which (with sufficiently large values of the resistance of the resistors R_f) the equality of the active impedances of the source and the receiver of the noise signal is observed. This is true because the resistors R in the circuit of each input simultaneously represent the output resistances of the thermal noise sources and the input resistances of the amplifier.

4. Violation of the sampling theorem

At a sampling frequency of F_s, the sampling theorem is valid not only for signals whose spectrum is limited by frequencies from 0 to $F_s/2$, but also for signals in bands from $F_s/2$, to F_s, from F_s to $3F_s/2$, and so on. These bands are called Nyquist zones: 1st zone, 2nd zone, 3rd and so on.

Modern analog-to-digital converters (ADCs) are technologically catching up with this capability and allow working not only in the 1st zone but also in zones with much higher numbers. For example, assume that we need to process a signal with a bandwidth of 30 MHz, in the frequency range from 450 to 480 MHz. To achieve this, we need to install a bandpass filter at the ADC input that selects the required frequency range of 450–480 MHz, and this filter has to operate at a sampling frequency of 60 MHz in the 16th Nyquist zone as if this range lies in the region from 0 to 30 MHz. It is only necessary to remember that for odd Nyquist zones, the signal spectrum remains unchanged, and for even ones it is mirrored, that is, when the frequency of the original signal changes from the lower boundary to the upper boundary of the zone, the frequency of the resulting signal presented in the first zone will change from the upper boundary to the lower. In this case, a one-to-one correspondence is maintained between the analog signal as a continuous function and the signal presented (restored from) by digital samples (with an accuracy of up to the Nyquist zone).

Now we will violate the sampling theorem. Let us take a signal with a band from 0 to 480 MHz and digitize it without any filters with a frequency of F_s = 60 MHz. We will obtain the sum of the signals in 16 Nyquist zones, and the components of the sum from the even zones will be mirror-reflected. This phenomenon is called the aliasing effect and is considered harmful.

The power of the resulting signal will be equal to the sum of the power of the components of all Nyquist zones, and the one-to-one correspondence between the analog signal and the sample values will be irreversibly lost.

Fig. 8 and Fig. 9 show the graphs of a continuous noise signal with a bandwidth of 30 MHz and a signal with a bandwidth of 480 MHz, respectively (the bold dots show the samples with a sampling frequency of 60 MHz).

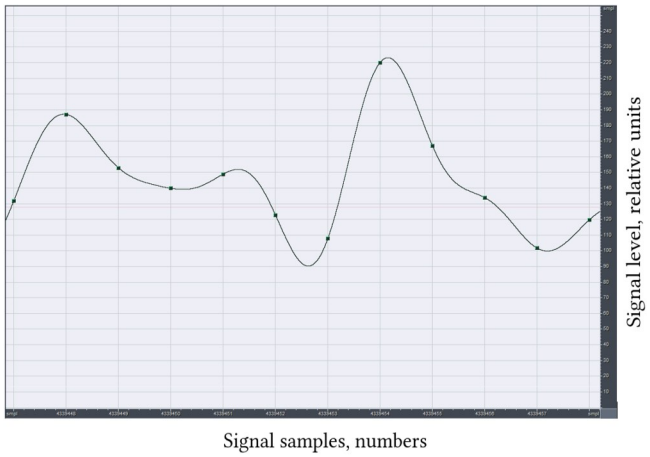

Figure 8: Noise signal with a bandwidth of 30 MHz

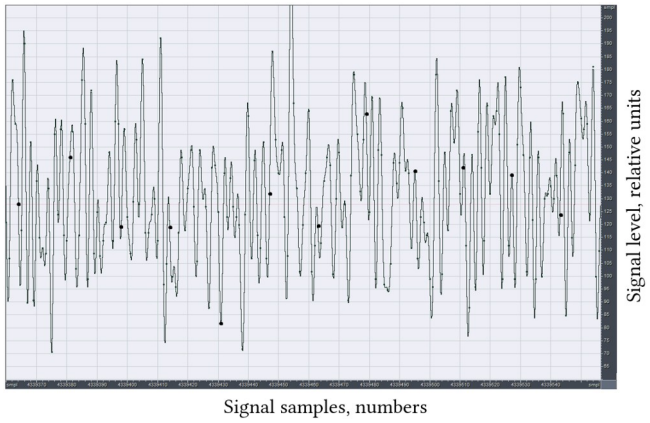

Figure 9: Noise signal with a bandwidth of 480 MHz

5. Sampling of broadband noise

If we take a broadband signal from a physical noise source and subject it to analog-to-digital conversion with a sampling frequency significantly lower than the upper frequency of the noise signal, we get the aliasing effect.

What it gives one is as follows:

1. Everything is normalized, that is, summing up many independent random variables, even not quite normal ones, leads to a normal distribution of the probability density of the resulting signal.
2. Not quite white noise is whitened to the degree of averaging.

3. The noise power increases by n times compared to using a narrow-band analog filter in the 1st Nyquist zone.
4. The correlation between the original signal samples decreases to a power of times.

The main inference is that the signal, possibly not ideal, is idealized to a power corresponding to the number of steps of averaging. In practice, 16 of them is more than enough.

6. Vanishing difference

Let us there be two independent binary sequences a and b with probabilities of zero and one, respectively, p_0, p_1 and bias $d = |p_0 - p_1|$. Then, when summing modulo 2 sequences a and b, the bias of the probability of zero and one for the summed sequence will be equal to $2d^2$. In the general case, the expectation of the bias of the sum of m independent sequences with the same biases will have the order of the m-th power of the expectation of the bias of one sequence.

For the confidence probability β and the number of elements in the sequence N, we define the admissible interval ε, into which the bias d must fall when $p_0 = p_1$, as,

$$\varepsilon = \frac{1}{2\sqrt{N}} \arg\Phi * \left(\frac{1+\beta}{2} \right).$$

To secure that with probability β the shift dm of the sum of m sequences of length N does not go beyond the permissible interval ε, i.e. to satisfy the condition $dm<\varepsilon$, we can define the minimum required number m of summed sequences as

$$m = \lceil \frac{\ln d}{\ln \varepsilon} \rceil.$$

Below are the values of m for a range of values of β, d, and N.

Table 1
Values of m for different values of β, d, and N

N			d=30%	d=10%	d=1%	d=0.1%
10^6	0.99	0.00135	m=8	m=4	m=2	m=2
10^6	0.999	0.00165	m=6	m=3	m=2	m=1
10^6	0.9999	0.002	m=5	m=3	m=2	m=1
10^{12}	0.99	0.00000135	m=12	m=6	m=3	m=2
10^{12}	0.999	0.00000165	m=12	m=6	m=3	m=2
10^{12}	0.9999	0.000002	m=11	m=6	m=3	m=2

Individual ADC digits can be selected as independent sequences for summation (to eliminate possible correlations between digits, we will delay the values of different digits by a different number of clock cycles). If an m-digit ADC is used, then the estimate of the value of the permissible interval ε for a given value of d will be:

$$\varepsilon = \exp(m \cdot \ln d).$$

For example, for an 8-bit ADC with m = 8 and d<1%, we obtain an interval estimate of ε = 1e−16.

According to the law of the iterated logarithm (the limit law of probability theory), the following condition may be violated for some sufficiently large n if the sequence differs from the ideal Bernoulli sequence

$$x_n < \sqrt{(2 \ln\ln n)/n}.$$

Here x_n is the estimate of the deviation of the probability of the sequence values from the expectation value of 0.5 in n experiments, equal to

$$x_n = \frac{\sum_{k=0}^{n-1} (b_k - 0.5)}{n},$$

where b_k is the k-th bit of the sequence.

Our degree of difference is the value x_n, comparable with the boundaries of the interval ε = 1e–16, by the value of which we can easily calculate n = 1.0e33.

If our generator produces random bits at a rate of 60 Mbit/s, then the time to detect the difference between our sequence and the ideal Bernoulli sequence will be:

1.0e33/60000000/3600/24/366=5e18 years.

It looks like the result is more than sufficient.

Even for m = 8 and d<5%, we get an interval estimate of ε = 4e–11, for which we calculate n = 1e22 and 1.0e22/60000000/3600/24/366 = 5.2 million years.

7. The generator block diagram

So, our proposed entropy source consists of a noise generator in the form of a resistor with an amplifier and an ADC, part of bits of which are delayed for a different number of cycles and modulo 2 added, forming an output sequence of random bits, as is shown in Fig. 10. This is enough, no additional or other elements are required for the entropy source, they will be superfluous.

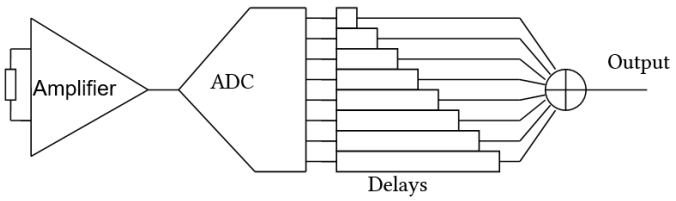

Figure 10: Block diagram of the entropy source

Conclusions

We have built a block diagram of an entropy source with characteristics close to the ideal ones. Such a source can become the basis of a truly random bit generator, close to an ideal one.

To complete the generator, it is necessary to add power nodes (the power supply of the noise generator must be especially stable (filtered), or without fluctuations; power node control circuits; a noise source quality control node; nodes implementing tests for switching on, initialization, periodic and on-demand operator tests, continuous tests of primary sequences, tests of the output random sequence; nodes for blocking the generator operation in the case of violation of the conditions for its correct functioning; a controller for exchange with the computer (technician). It is also necessary to implement electrical and mechanical requirements for preventing external electromagnetic interference and other possible adverse effects on the generator.

In addition, the generator must be equipped with drivers, a library of application programming interface functions for creating applications, and test software.

Then it will be a fully-fledged non-deterministic generator of truly random bit sequences. These sequences can be used for spread-spectrum techniques in modern robust electronic communication links and cryptographic applications as well.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] D. C. Schleher, Electronic warfare in the information age, Artech House, Inc., Norwood, 1999.

[2] Electronic warfare: Handbook 2008, Ed. Peter Donaldson, The Shephard Press Ltd, Berkshire, UK, 2008.

[3] R. A. Poisel, Introduction to communication electronic warfare systems, Artech House Inc., Norwood, MA, 2008.

[4] V. Sokolov, P. Skladannyi, A. Platonenko, Jump-stay jamming attack on Wi-Fi systems, in: IEEE 18th International Conference on Computer Science and Information Technologies (2023) 1–5. doi:10.1109/CSIT61576.2023.10324031

[5] V. Sokolov, P. Skladannyi, V. Astapenya, Bluetooth low-energy beacon resistance to jamming attack, in: IEEE 13th International Conference on Electronics and Information Technologies (2023) 270–274. doi:10.1109/ELIT61488.2023.10310815

[6] O. Pliushch, B. Zhurakovskyi, M. Kyryk, Adaptive algorithm for four-element antenna array for GNSS, in: IEEE 17th Int. Conf. on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, 2024, 564–569. doi:10.1109/TCSET64720.2024.10755781

[7] V. Sokolov, P. Skladannyi, V. Astapenya, Wi-Fi interference resistance to jamming attack, in: IEEE 5th International Conference on Advanced Information and Communication Technologies (2023) 1–4. doi:10.1109/AICT61584.2023.10452687

[8] V. Sokolov, P. Skladannyi, N. Korshun, ZigBee network resistance to jamming attacks, in: IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics (2023) 161–165. doi:10.1109/UkrMiCo61577.2023.10380360

[9] A. J. Viterbi, CDMA: Principles of spread spectrum communication, Addison-Wesley Publishing Company, Reading, Massachusetts, 1995.

[10] M. A. Abu-Rgheff, Introduction to CDMA wireless communications, Elsevier Ltd, 2007.

[11] F. Ouyang, Digital communication for practicing engineers, John Wiley & Sons, Ltd., Hoboken, New Jersey, 2020.

[12] G. Baumslag, et al., A course in mathematical cryptography, Walter de Gruyter GmbH, Berlin, 2015.

[13] K. Wesołowski, Introduction to digital communication systems, John Wiley & Sons, Ltd., West Sussex, United Kingdom, 2009.

[14] K. Fazel, S. Kaiser, Multi-carrier and spread spectrum systems: From OFDM and MC-CDMA to LTE and WiMAX, John Wiley and Sons, Ltd, Chichester, United Kingdom, 2008.

[15] L. Hanzo, T. Keller, OFDM and MC-CDMA: A primer, John Wiley & Sons, Chichester, 2006.

[16] D. Torrieri, Principles of spread-spectrum communication systems, Springer, Switzerland, 2022. doi:10.1007/978-3-030-75343-6

[17] O. Pliushch, B. Zhurakovskiy, M. Klymash, Robust control channel of unmanned aerial vehicle, in: IEEE 5th International Conference on Advanced Information and Communication Technologies (AICT), 2023, 1–4. doi:10.1109/AICT61584.2023.10452677

[18] O. Pliushch, et al., Performance Study of Spread Spectrum Systems with Hard Limiters, Int. J. Comput. Netw. Inf. Secur. 5 (2020) 1–15. doi:10.5815/ijcnis.2020.05.01

[19] V. Sokolov, P. Skladannyi, N. Mazur, Wi-Fi repeater influence on wireless access, in: IEEE 5th International Conference on Advanced Information and Communication Technologies (2023) 33–36. doi:10.1109/AICT61584.2023.10452421

[20] V. Girardin, N. Limnios, Applied probability: From random experiments to random sequences and statistics, Springer, Switzerland, 2022. doi:10.1007/978-3-030-97963-8