УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО УНИВЕРСИТЕТА.
СЕРИЯ ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

2017, Т. 159, кн. 2 ISSN 2541-7746 (Print)
С. 246–262 ISSN 2500-2198 (Online)

UDK 531.19+681.326

# THEORY OF TERNARY JITTER-BASED TRUE RANDOM NUMBER GENERATORS COMPOSED OF IDENTICAL GATES

*R.Kh. Latypov, E.L. Stolov*

*Kazan Federal University, Kazan, 420008 Russia*

## Abstract

In this paper, we continue to study of a novel family of generators producing true uniform random numbers. The generator consists of a number of identical ternary logic combinational gates. In our previous work, the main attention was dedicated to the schemes composed of the gates in a ring. Other circuits are taken into consideration in this paper. All the units are characterized by time delays that are random and independent. If this time delay has an exponential distribution, then the theory of generator's behaviour is based on the Erlang equations. Some other models are also considered. The features of the multidimensional random vectors produced by the generator are discussed. They can be used for identification of the generator. This article is an extended version of the report presented by the authors at conference [Latypov R.Kh., Stolov E.L. Ternary jitter-based true random number generator. *IOP J. Phys.: Conf. Ser.*, 2017, vol. 783, art. 012064. doi: 10.1088/1742-6596/783/1/012064].

**Keywords:** ternary logic, true random number generator, jitter

## Introduction

Random numbers are important for cryptographic applications, lotteries, stochastic modelling, randomized algorithms, online gambling, etc. [1, 2]. The problem of generating true random numbers lies in the fact that computers are basically predictable devices that perform calculations and bring answers based on mathematical algorithms. True random number generator (TRNG) is a type of random number generators that produces unpredictable random number sequence using a random source. Any TRNG must introduce an unpredictable element from the real world into the algorithm, i.e., use a non-deterministic physical phenomenon [3–5]. One of such phenomenons is jittering in digital circuits [6–14]. The TRNG we propose in this paper is an asynchronous circuit utilizing jittering as a source of entropy. It results from feedback in an asynchronous schema consisting of identical gates, while each gate is a combinational circuit.

Delay modelling is among the most difficult topics in asynchronous circuit analysis. Because of its peculiarities, asynchronous circuit components have to be assigned with probabilistic delays for accurate timing analysis. Statistical static timing analysis is a method of computing statistical distribution for the output arrival time based on the statistical input arrival time and the statistical input-to-output pin delay [15–21]. In the present paper, we propose a statistical method for delay estimation in generator. The effectiveness of the proposed method will be analyzed theoretically. Our numerical evaluations show that this method provides an efficient way to model the dynamic behavior of TRNG.

Most of cited papers concern binary schemes. Development of ternary logic devices seems to be prospective in providing a higher speed of arithmetic operations; hence,

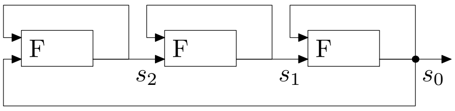

Fig. 1. Version of the ring-like generator containing three ternary units

development of such circuits becomes an urgent problem [22–24]. In our paper, we present a new family of TRNGs that can be implemented by using only ternary logic gates. The purpose of the work is to theoretically study the behavior of such devices.

The main body of the paper is organized as follows: In Section II, the basic scheme of the ring-like TRNG (and also its mathematical theory) is given; in Section III, functions suitable for generator design are described; in Section IV, statistical properties of the basic generator are studied; in Section V, an alternative generator design is proposed; Section VI is dedicated to implementation of the generator; Conclusions are given in Section VII.

Throughout this paper, while dealing with matrices, the following notation is used:

A. $A[i, j]$ represents an element of matrix A standing at $i$-th row and $j$-th column .

B. $A[i, *]$ represents the $i$-th row of matrix A, $A[*, j]$ is the $j$-th column of this matrix.

C. $\theta$ represents the zero matrix.

D. Bold symbols, such as $\mathbf{P}$, are used for vector designations.

## 1. Preliminaries and basic scheme

Since this paper continues our previous research [25], some of the already obtained results must be recalled. The balanced ternary logic is a special case of ternary logic where the digits have the values –1, 0, and 1. Here, we will focus on two-input single-output functions or gates.

### 1.1. Ring-like TRNG.

Consider the scheme shown in Fig. 1, where F stands for a ternary combinational gate. It realizes the function $c = F(a, b), \quad a,\, b,\, c \in \{-1, 0, 1\}$. Generally, the scheme consists of $N$ gates. Renumber all the units via numbers in the interval $[0, N-1]$. The output of the unit which uses the number $k$ is connected to one of the inputs of the same unit and to the input of the unit with the number $k-1 \bmod N$ (see Fig. 1). After one input signal of the gate changes, the output signal of the gate changes tool; but it takes a delay time $DT$. In the paper, a statistical delay model is considered.

According to this model, the following assumptions are accepted:

A. $DT$ is a stochastic value having an exponential distribution for all units with the same parameter $T$. The latter means that $P(DT < d) = 1 - \exp(-Td)$. In what follows, we will assume that, for exponential distribution, $T = 1$; it does not limit the generality of the arguments.

B. At any time, only one unit can change its output; all those events are independent.

### 1.2. Basic function.

To guarantee good properties of the TRNG, some restrictions on the function $F$ are imposed. First of all, the TRNG must have no stable states. Suppose that the following formula takes place:

$$c = F(a, b), \quad \forall\, (a, b), \quad c \neq a,\, b. \tag{1}$$

Table 1. Basic function $F(a,b)$

| Name | $F(0,0)$ | $F(1,1)$ | $F(-1,-1)$ |
|---|---|---|---|
| $F_1$ | 1 | –1 | 0 |
| $F_2$ | 1 | –1 | 1 |

It means that only the values of $F(a,a)$, $a \in \{-1,0,1\}$, must be defined. It was proved that there exist only two different functions, which obey (1). These are the functions defined by the Table 1 [25].

**1.3. Erlang equations.** All the restrictions imposed on the system allow us to implement the Erlang theory [26] to the generator. Let $s_k(t)$ be the output signal of the unit with the number $k$ at the time $t$. Denote the state of the TRNG at the time $t$ by vector $\mathbf{S}(t) = \langle s_0(t), \ldots, s_{N-1}(t)\rangle$. Hence, the system has $M = 3^N$ states, which are also indexed by the numbers from 0 to $M-1$. Let $i_1, \ldots, i_m$ for each $n \in [0, M-1]$ be a list of all indices of the states, for which it is possible to transfer the TRNG to the state $\mathbf{S}_n$ from the states $\mathbf{S}_{i_k}$, $k = 1, \ldots, m$, as a result of a change of the output signal of one of the units. This list of the states depends on n. Create a system of differential equations of the Erlang type describing the dynamics of the TRNG. Let $P_n(t)$ be the probability that the TRNG is in a state number n at the time $t$. The following equation describes the dynamics of the generator

$$\frac{dP_n}{dt} = -NP_n(t) + \sum_{k=1}^{m} P_{i_k}(t), \tag{2}$$

where $m$, $i_1, \ldots, i_m$ depend on $n$. This Erlang type equation is usually used in description of Queueing Systems.

**1.4. Dynamics of generator states.** As far as the type of $F$ has been defined, all parameters can be found in (2). Using a matrix form, rewrite the system as follows:

$$\frac{d\mathbf{P}}{dt} = \mathrm{Matr} \cdot \mathbf{P}. \tag{3}$$

Here $\mathbf{P} = \langle P_0, P_1, \ldots, P_{M-1}\rangle^T$.

First of all, one has to index all states of the TRNG. Let $\mathbf{S} = \langle s_0, s_1, \ldots, s_{N-1}\rangle$ be a state of TRNG, $s_k \in \{-1,0,1\}$. Index of $\mathbf{S}$ is a number

$$\mathrm{Ind}(\mathbf{S}) = \sum_{k=0}^{N-1} 3^k (s_k + 1). \tag{4}$$

It is convenient to present the matrices as tables. The rows and columns of the matrix are numbered using the index calculated by the formula (4). In accordance with the definition, $\mathrm{Matr}[i,j] = 1$, $i \neq j$ if and only if it is possible to transfer to the state with index $i$ from the state with index $j$. $\mathrm{Matr}[k,k] = -N$ $\forall\, k$. Matr is presented in Table 2 for $N = 1$ and in Table 3 for $N = 2$.

Formally, knowing matrix $Matr$ and differential equations (3), it is possible to find vector $\mathbf{P}(t)$ for any $t$, if $\mathbf{P}(0)$ is known, where $\mathbf{P}(0)$ is a stochastic vector defining initial distribution of states of the TRRG [28]. Our goal is to obtain properties of this vector without searching an exact solution of the system.

Table 2. Matrix for $N = 1$

| $R\backslash C$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | –1 | 0 | 1 |
| 1 | 1 | –1 | 0 |
| 2 | 0 | 1 | –1 |

Table 3. Matrix for $N = 2$

| $R\backslash C$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | –2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | –2 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| 2 | 0 | 1 | –2 | 0 | 0 | 1 | 0 | 0 | 1 |
| 3 | 1 | 0 | 0 | –2 | 0 | 1 | 1 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | –2 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 1 | 1 | 1 | –2 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 1 | 0 | 0 | –2 | 1 | 1 |
| 7 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | –2 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | –2 |

**1.5. Asymptotic properties of $\mathbf{P}(t)$.** It can be easily seen that, for $N = 2$, there are lines in Matr that have no 1's. They are Matr$[0, :]$, Matr$[4, :]$, Matr$[8, :]$. It means that there are no transfers of the TRNG to the states with such indices; in other words, these states are unattainable. It is proved in [25] that the states of form $\langle x, x, \ldots, x\rangle$ with $x \in \{-1, 0, 1\}$ are the only unattainable states of the generator with $N > 1$.

In general case, exclude from consideration the states of the form $\langle x, x, \ldots, x\rangle$ for $N > 1$. It means that one should exclude three items from vector $\mathbf{P}$ and three rows and three columns from matrices $Matr$. We keep the previous notation for new $\mathbf{P}$ and $Matr$. Since the matrix $Matr$ in (3) is constant, the solution of the equation can be presented as follows

$$\mathbf{P}(t) = \exp(\mathrm{Matr} \cdot t) \cdot \mathbf{P}(0). \tag{5}$$

According to the definition, we have

$$\mathrm{Matr} = Q - N \cdot I, \tag{6}$$

where $I$ represents the identity matrix, while $Q$ is a binary matrix containing either 1 or 0. Both the matrices have the size $M' \times M'$, $M' = M - 3$. The following proposition is proved in [25]

**Proposition 1.** *Let $e_0, e_1, \ldots, e_{M'-1}$ be all eigenvalues of $Q$ and*

$$|e_0| \geq |e_1| \geq \cdots \geq |e_{M'-1}|. \tag{7}$$

*Then $e_0 = N$.*

Let $m_0, m_2, \ldots, m_{M'-1}$ be all eigenvalues of Matr. We have

$$m_i = e_i - N \quad \forall i. \tag{8}$$

Hence $m_0 = 0$ and inequalities $\mathrm{Real}(m_j) \leq 0$, $j = 1, \ldots, M' - 1$, are fulfilled. Suppose that we have the strong inequalities

$$\mathrm{Real}(m_j) < 0, \quad j = 1, \ldots, M' - 1. \tag{9}$$

It means that matrix $E(t) = \exp(t{\cdot}\mathrm{Matr})$, $t \geq 0$ with eigenvalues $\exp(t{\cdot}m_i)$ has a single characteristic root 1, while all other characteristic roots of this matrix have absolute values lesser than 1. If $t \to \infty$, then $E(t)$ converges to a stable matrix. The same is true for the vector $\mathbf{P}(t)$, and

$$\frac{d\mathbf{P}(t)}{dt} \to 0, \quad t \to \infty. \tag{10}$$

Following [26], one can find a stochastic vector $\overline{\mathbf{P}} = \mathbf{P}(\infty)$ by solving the system

$$Q \cdot \overline{\mathbf{P}} = N\,\overline{\mathbf{P}}. \tag{11}$$

**The case** $N = 1$. There are three states of the TRNG: $\langle -1\rangle$, $\langle 0\rangle$, $\langle 1\rangle$. The eigenvalues of $Matr$ are 0, –1.5, –1.5, thus (9) is fulfilled, and $\overline{\mathbf{P}} = \langle 1/3,\ 1/3,\ 1/3\rangle$. The latter means that stable vector $\overline{\mathbf{P}}$ possesses the uniform distribution.

**The case** $N = 2$. Here the eigenvalues of Matr are 0, –1, –4, –3, –3, –1, and the stable vector is $\langle 0.17,\ 0.17,\ 0.17,\ 0.17,\ 0.17,\ 0.17\rangle$; hence, in this case, we have the uniform distribution as well, excluding three unattainable states.

**The case** $N = 3$. In this case (9) is fulfilled, but the stable vector $\overline{\mathbf{P}}$ has components

$$\begin{array}{cccccc} 0.037 & 0.037 & 0.037 & 0.037 & 0.074 & 0.037 \\ 0.037 & 0.037 & 0.037 & 0.037 & 0.037 & 0.037 \\ 0.037 & 0.074 & 0.037 & 0.037 & 0.037 & 0.074^{\cdot} \\ 0.037 & 0.037 & 0.037 & 0.037 & 0.037 & 0.037 \end{array} \tag{12}$$

Hence, we have a nonuniform final distribution of states. The reason is the existence of special states of the generator: $\langle -1, 0, 1\rangle$, $\langle 1, -1, 0\rangle$, $\langle 0, 1, -1\rangle$. In fact, it is the same state, because every state is a result of cyclic transform of other states (see Fig. 1).

## 2. General case

Let us recall some facts relating to the matrix theory [27]. Matrix $Q$ is a decomposable matrix if there exists a permutation matrix $Pr$ such that

$$Pr^T \cdot Q \cdot Pr = \begin{pmatrix} A & 0 \\ B & C \end{pmatrix}$$

where $A$, $C$ represent square matrices. Non-negative matrix $Q$ is an indecomposable matrix if for any of two indexes $i$, $j$ there exists integer $k$ (dependent on these indexes) such that

$$Q^k[i, j] > 0. \tag{13}$$

In our case, the matrix $Q$ is a binary matrix, and it can be considered as a transfer matrix of the TRNG. Condition (13) is equivalent to the following one: for any two states $\mathbf{S}$, $\mathbf{S}'$ of the TNRG there is a chain of states $\mathbf{S}_0 = \mathbf{S}$, $\mathbf{S}_1, \ldots, \mathbf{S}_k = \mathbf{S}'$ such that the transfer of state $\mathbf{S}_i \to \mathbf{S}_{i+1}$ is a result of the change of one of the inputs of the TRNG.

**Proposition 2.** *Matrix* $Q$ *in* (6) *is an indecomposable matrix.*

**Proof.** We assume that $N > 2$ and all the states of the form $\langle x, x, \ldots, x\rangle$, $x \in \{-1, 0, 1\}$ are excluded. Our goal is to prove that the matrix $Matr$ is an indecomposable one. It is sufficient to state that each state $\mathbf{S}$ of the TRNG is attainable from any other state $\mathbf{U}$ via a finite number of steps. We divide the proof into two parts.

First of all, show that any state is attainable from $\mathbf{U} = \langle 0, -1, \dots, -1 \rangle$. Let $\mathbf{S}' = \langle s_0, \dots, s_{N-1} \rangle$. Recall that the states, where the generator can transfer to from $\mathbf{S}'$ after one gate changes its output, have the form

$$\langle p_0, p_1, \dots, p_{N-1} \rangle.$$

Here

$$p_k = F(s_k, s_{k+1}), \quad k < N-1, \quad p_{N-1} = F(s_{N-1}, s_0) \tag{14}$$

and inequality $p_k \neq s_k$ is true just for one index k. Let the generator be in state $\mathbf{U}$. After output $s_1$ changed, we obtain state $\mathbf{U}_1 = \langle 0, 1, -1, \dots, -1 \rangle$. After signal $s_1$ changed again, the TRGN transfers to state $\mathbf{U}_2 = \langle 0, 0, -1, \dots, -1 \rangle$. It means that all states of the form $\langle 0, a, -1, \dots, -1 \rangle$, $a \in \{-1, 0, 1\}$ are attainable from $\mathbf{U}$. In the same way one can establish that all states of the form

$$\langle 0, s_1, \dots, s_{N-2}, -1 \rangle \tag{15}$$

are attained from $\mathbf{U}$ as well. If signal $s_0$ changes in state $\mathbf{U}$, the next state of the TRNG is $\mathbf{U}_1 = \langle 1, -1, \dots, \rangle$. Repeating the previous arguments, one can see that all states of the form

$$\langle 1, s_1, \dots, s_{N-2}, -1 \rangle \tag{16}$$

are attained from $\mathbf{U}$. Let $\mathbf{S} = \langle -1, 0, s_2, \dots, s_{N-2}, -1 \rangle$ be arbitrary state of the TRNG. Changing signal $s_0$ in (16), where $s_2 = 0$, one establishes attainability of $\mathbf{S}$. In the same way it can be proved that all states of the form

$$\langle -1, s'_1, s_2, \dots, s_{N-2}, -1 \rangle, \quad s'_1 \in \{0, 1\} \tag{17}$$

are also attainable from $\mathbf{U}$. Using (15),(16) and changing signal $s_{N-1}$, one gets the attainability of states $\langle 0, s_1, \dots, s_{N-2}, 1 \rangle$ and $\langle 1, s_1, \dots, s_{N-2}, 0 \rangle$. Let us show that states of the form

$$\langle -1, -1, \dots, -1, b, s_{k+1}, \dots, s_{N-2}, -1 \rangle, \quad b \in \{0, 1\} \tag{18}$$

are also attainable states. According to (16),

$$\mathbf{S} = \langle 1, 1, \dots, 1, b, s_{k+1}, \dots, s_{N-2}, -1 \rangle. \tag{19}$$

We have $F(1, b) = -1$, so by changing signals $s_0, s_1, \dots s_{k-1}$ one establishes the attainability of the sates in (18). Finally, the attainability of such states as

$$\langle 0, 0, \dots, 0, b, s_{k+1}, \dots, s_{N-2}, 0 \rangle, \quad b \in \{-1, 1\} \tag{20}$$

can be proved starting from (18), changing signal $s_{N-1}$ and by changing afterwards signals $s_0, s_1, \dots s_{k-1}$.

In the second part of the proof, we have to prove the attainability of $\mathbf{U}$ from any state $\mathbf{S}$. Let $\mathbf{S}$ have the form (15). Consider pair $s_1, s_2$. If $s_1 = 1$ or $s_1 = 0$, then we always can gain the equality $s_1 = -1$ by changing $s_1$. The same arguments can implied to state

$$\langle 0, -1, s_2, \dots, s_{N-2}, -1 \rangle. \tag{21}$$

If signal $s_{N-1} \neq -1$, then, by changing signal $s_{N-1}$, one can convert it to –1. Suppose now that $\mathbf{S} = \langle s_0, \dots s_{N-1} \rangle$ and $s_0 \neq 0$. As before, by changing this signal, one can gain the equality $s_0 = 0$; so, it is the situation considered above. □

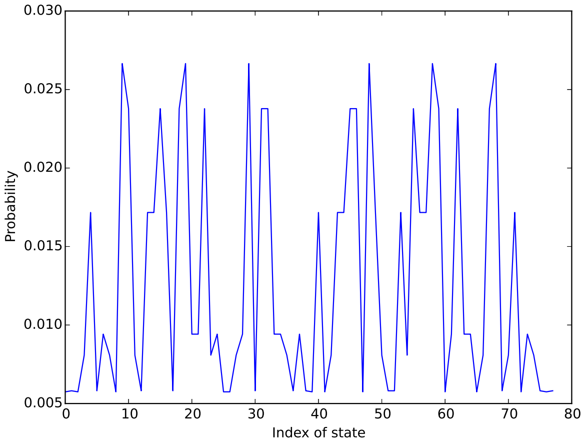

Fig. 2. $N = 4$. Components of stable vector

It is known ( [27]) from the indecomposable matrix that the maximum positive characteristic root has multiplicity equal to 1, so (9) holds. It means that the technique for calculation of the distribution of states presented above is good for any number units in the TRNG. The only problem is to find eigenvectors of a matrix of large size. The examples show that the stable distribution of states, given by the components of $\overline{\mathbf{P}}$, is not the uniform distribution for $N > 2$. Since the corresponding stable vectors are of big size, we present the components of the vector in graphical form (see Fig. 2, for example).

It means that a kind of dependence exists among different outputs of the TRNG. This feature can be used as a marker of design of the generator. On the other hand, because of the symmetry of the scheme, the output signal of any unit has the uniform distribution.

## 3. Alternative design

As was mentioned above, there is a correlation among various components of the final vector if $N > 2$. This correlation can be used for identification of the generator if one has access to all outputs of the schema. The ring-like connection of the units is not the only design that can be implemented in generator design. Two other circuits, each containing three units, are presented in Figs. 3, 5. There is an important property that holds true for all the schemes investigated in this paper, that is a kind of symmetry following from

**Proposition 3.** *Let $\sigma$ be a permutation, $\sigma(-1) = 0$, $\sigma(0) = 1$, $\sigma(1) = -1$. Then*

$$F(\sigma(x), \sigma(y)) = \sigma(F(x, y)). \tag{22}$$

**Proof.** Let $G(x, y) = F(\sigma(x), \sigma(y))$. The correctness of the proposition results from Table 4.

□

Table 4. To proof of Proposition 3

| $x$, $y$ | $F(x,y)$ | $G(x,y)$ |
|---|---|---|
| –1, –1 | 0 | 1 |
| 0, 0 | 1 | –1 |
| 1, 1 | –1 | 0 |
| –1, 0 | 1 | –1 |
| –1, 1 | 0 | 1 |
| 0, 1 | –1 | 0 |

Let $\sigma$ be as before. This permutation defines a transform $Tr_{\mathrm{ind}}$ of the set of states into itself. If $\mathbf{S} = \langle s_0, s_1, \dots, s_{N-1}\rangle$, then

$$Tr_{\mathrm{ind}}(\mathbf{S}) = \langle \sigma(s_0), \sigma(s_1), \dots, \sigma(s_{N-1})\rangle. \tag{23}$$

There is one-to-one relation between states and their indexes, so we can substitute $Tr_{\mathrm{ind}}(i)$ by $Tr_{\mathrm{ind}}(\mathbf{S})$, where $i$ is the index of $\mathbf{S}$. The following formula is an easy implication of (22)

$$Q[i,j] = Q[Tr_{\mathrm{ind}}(i), Tr_{\mathrm{ind}}(j)], \tag{24}$$

where $Q$ is defined accordingly (6).

It is difficult to suggest a theory that would be acceptable in the general case, so we restrict ourself to direct calculations. Equation (3) holds as before, but $Matr$ depends on the design. Since any state of the generator is a vector of length 3, the sum of items in each column in matrix $Q$ in (6) is 3 (mainly all non-zero items in $Q$ are ones, but it is possible that a transfer from one state to other state is a result of the change of output in two different gates). It means that 3 is an eigenvalue of $Q$, and all other eigenvalues $e_i$ of this matrix meet inequalities (7). All the arguments used above for description of asymptotic behavior $\overline{\mathbf{P}}$ are fulfilled in the cases under consideration if the multiplicity of the characteristic root 3 of the matrix $Q$ equals one. This condition will be stated via calculation. Special attention is drawn to the states having zero probabilities in the final distribution, because it is an important property of the generator. Thus, it is a very important feature of the generator that can be used for its identification, because some known vectors will not be observed on its output. All results of the calculations are presented in graphical mode in what follows.

**3.1. Case Design 1, Fig. 3.** lists of eigenvalues and components of the final vector are presented in Fig. 4. It can be seen that here is only one characteristic root equal to 3, and all other roots meet (9), so the final vector $\overline{\mathbf{P}}$ exists. We see that a part of components of $\overline{\mathbf{P}}$ are zeros. It means that a set of vectors can not be produced if the time after the onset of work is long.

**3.2. Case Design 2, Fig. 5.** Let us examine the property of the circuit in Fig. 5. In Fig. 6, graphical representation of the eigenvalues and the component of the final vector are shown. As before, there is only one eigenvalue that is equal to 3, and the final vector $\overline{\mathbf{P}}$ exists. Some of the components are zeros again, but they have indices, which do not coincide with those for Design 1. Thus, we have a possibility to distinguish between both generators.

## 4. Implementation of generator and its efficiency

Standard implementation of the generators described above is presented in Fig. 7. The clock line denotes a series of impulses with interval $D$. The efficiency of the circuit

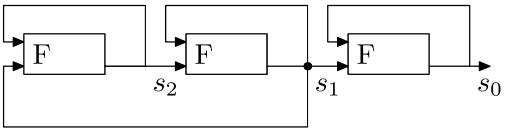

Fig. 3. Design 1

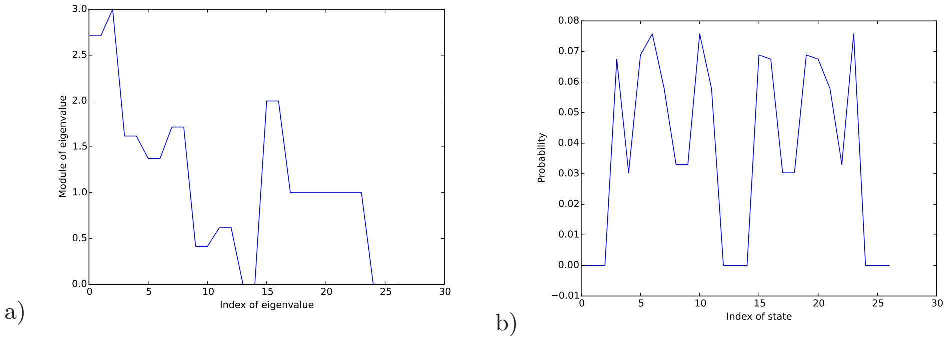

Fig. 4. Design 1: a) eigenvalues , b) final distribution

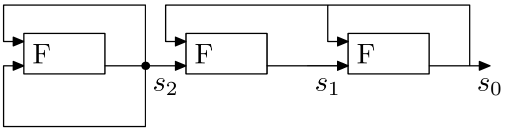

Fig. 5. Design 2

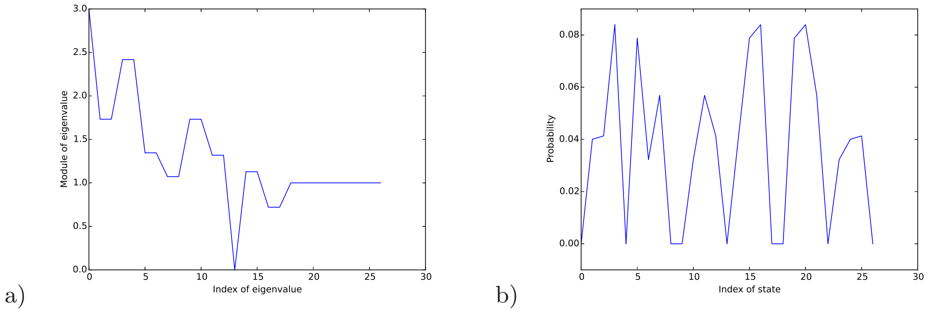

Fig. 6. Design 2: a) eigenvalues, b) final distribution

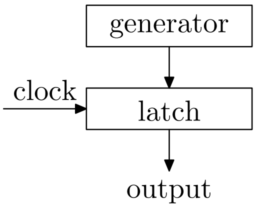

Fig. 7. Implementation. Generator's outputs are controlled by clock

Table 5. $\delta$ criteria of quality of TRNG for various $N$ and $D$

| $N\backslash D$ | 2 | 4 | 8 | 16 |
|---|---|---|---|---|
| 1 | 3.1e–2 | 1.6e–3 | 3.9e–6 | 2.1e–7 |
| 2 | 4.6e–2 | 6.1e–3 | 1.1e–4 | 3.8e–8 |
| 3 | 3.6e–2 | 6.9e–3 | 2.4e–4 | 3.2e–7 |
| 4 | 2.1e–2 | 3.7e–3 | 1.4e–4 | 2.6e–7 |
| 5 | 9.8e–3 | 2.1e–3 | 9.2e–5 | 2.0e–7 |
| 6 | 6.0e–3 | 9.4e–4 | 3.6e–5 | 7.1e–8 |

depends on the value of $D$ – the less is $D$, the more numbers will be produced in the given time interval $t_0$. As a rule, independent signals are needed on the output of the generator, so $D$ cannot be an arbitrary value. The generator must "forget" the previous state when a random number is released. That time also depends on the kind of the signal one has to obtain.

**4.1. Criteria of minimal time between two releases.** Suppose that the only generator's feature under investigation is the minimal time to reach stability of distribution of the generator's states. Formally, the generator needs infinite time to attain the distribution of the states described by vector $\overline{\mathbf{P}}$. In real situation, a condition such as(25 is used:

$$\left|\frac{d\mathbf{P}(\mathbf{t})}{dt}\right| < \epsilon, \quad t > t_0, \tag{25}$$

and $\epsilon$ is a small quantity given in advance (see (10)). In other words, $D$ is as long as the time that is enough to transfer the generator to a state that is close to the stable state. To this end, we must evaluate the difference between the matrix Stab

$$\mathrm{Stab} = (\overline{\mathbf{P}}, \overline{\mathbf{P}}, \dots, \overline{\mathbf{P}})$$

and the matrix $\mathrm{Astab}(D) = \exp(D \cdot Matr)$. Let $\mathbf{E} = \langle 1, 1, 1, \dots, 1\rangle$. Accordingly, the definition, $\mathbf{E} \cdot \mathrm{Matr} = \langle 0, 0. \dots, 0\rangle = \Theta$ is zero vector. Hence, $\mathbf{E} \cdot \mathrm{Matr}^K = \Theta$ for any natural $K$, and $\mathbf{E} \cdot \mathrm{Astab}(D) = \mathbf{E}$. In other words, the sum of the entries in any column of $\mathrm{Astab}(D)$ equals 1. Let

$$\delta = \max_{u,v} |\overline{\mathbf{P}}[u,v] - \mathrm{Astab}(D)[u,v]|. \tag{26}$$

Choose $\delta$ as a distance between two matrices and as the criteria of quality of the generator. Some results of calculation relating to TRNGs with various $N$ are presented in Table 5.

Apply the same criteria to the alternative circuits described above. Since all of them contain the same number of gates, a kind of evaluation of the quality of the design can be done without calculation of $\delta$. According to (8), all characteristic roots of Astab(t) are

$$1, e^{t \cdot m_1}, \dots, e^{t \cdot m_{26}}, \quad \mathrm{real}(m_i) < 0, \quad i > 0.$$

We have $|\exp(m)| = \exp(\mathrm{real}(m))$. If $\mathrm{real}(m) < 0$, then $|\exp(t \cdot m)| \to 0$, $t \to \infty$. Recall [28] that Jordan box $J$ is a square matrix of size $p > 1$

$$J(a) = \begin{pmatrix} a & 1 & 0 & \dots, & 0 \\ 0 & a & 1 & \dots & 0 \\ . & . & . & . & . \\ 0 & 0 & 0 & 0 & a \end{pmatrix}$$

Table 6. Values of $V$ depending on design of circuit

| | Des1 | Des2 |
|---|---|---|
| $V$ | –1 | –0.59 |

Table 7. $\delta$ criteria for various design

| Design\\$D$ | 2 | 4 | 8 | 16 |
|---|---|---|---|---|
| Des1 | 3.2e–2 | 4.7e–3 | 8.3e–5 | 2.8e–8 |
| Des2 | 6.6e–2 | 1.9e–2 | 1.7e–3 | 1.7e–5 |

If $p = 1$, then $J(a) = (a)$. It is known [28]

$$e^{J(a)} = \begin{pmatrix} e^a & e^a/1! & e^a/2! & \ldots, & e^a/(p-1)! \\ 0 & e^a & e^a/1! & \ldots, & e^a/(p-2)! \\ . & . & . & . & . \\ 0 & \ldots & 0 & 0 & e^a \end{pmatrix},$$

or

$$\exp(J(a)) = e^a \cdot B,$$

where matrix $B$ is independent of $a$. On the other hand, any matrix is similar to a Jordan form

$$\mathrm{Matr} = \mathrm{Tr}^{-1} \cdot \mathrm{diag}(J_1, \ldots J_L) \cdot \mathrm{Tr}$$

where $J_k,\ k = 0, 1, \ldots, L,$ are Jordan boxes. As a result,

$$\mathrm{Astab}(t) = \mathrm{Tr}^{-1} \cdot \mathrm{diag}(1, e^{t \cdot m_1} \cdot B_1, \ldots, e^{t \cdot m_{26}}) \cdot B_{26} \cdot \mathrm{Tr}, \tag{27}$$

where matrix Tr is independent of $t$. It follows from (27) that

$$\mathrm{Stab} = \mathrm{Tr}^{-1} \cdot \mathrm{diag}(1, 0, \cdot, 0) \cdot \mathrm{Tr},$$

and the degree of convergence $\mathrm{Astab}(t) \to \mathrm{Stab},\ t \to \infty$ depends mainly on

$$V = \max \mathrm{real}(m_i), \qquad i > 0. \tag{28}$$

The values of $V$ depending on design are presented in Table 6.

It is of interest to compare these values with analogous value $-0.84$ for the TRNG where $N = 3$. To test the hypothesis that the degree of convergence to the stable distribution depends on $V$, calculate $\delta$ for the other circuits (see Table 7).]

By comparing Tables6 and 7, one can conclude that the lesser value $V$, is the better is the degree of convergence.

**4.2. Single output criteria.** A more realistic situation is where a user needs a generator that produces random uniform distributed numbers. Because of symmetric design of ring-like TRNG, signals on any output have the same stable distribution and each value has the probability of $1/3$. The same is true for any of the circuits under consideration although is not an evident fact.

**Proposition 4.** *Let matrix $Q$ in (6) have $N$ as a characteristic root of multiplicity $1$. Then signals on each output of any circuit, which are built by means of gates with function $F$, have the uniform distribution.*

Table 8. $\overline{\mathbf{P}}$ vector for various designs

| State | Des1 | Des2 |
|---|---|---|
| 0 | 0. | 0. |
| 1 | 0. | 0.04 |
| 2 | 0 | 0.04 |
| 3 | 0.07 | 0.08 |
| 4 | 0.03 | 0. |
| 5 | 0.07 | 0.08 |
| 6 | 0.07 | 0.03 |
| 7 | 0.06 | 0.06 |
| 8 | 0.03 | 0. |
| 9 | 0.03 | 0. |
| 10 | 0.06 | 0.03 |
| 11 | 0.06 | 0.06 |
| 12 | 0. | 0.04 |
| 13 | 0. | 0. |
| 14 | 0. | 0.04 |
| 15 | 0.07 | 0.08 |
| 16 | 0.07 | 0.08 |
| 17 | 0.03 | 0. |
| 18 | 0.03 | 0. |
| 19 | 0.07 | 0.08 |
| 20 | 0.07 | 0.08 |
| 21 | 0.06 | 0.06 |
| 22 | 0.03 | 0. |
| 23 | 0.07 | 0.03 |
| 24 | 0. | 0.04 |
| 25 | 0. | 0.04 |
| 26 | 0. | 0. |

**Proof.** Let $\overline{\mathbf{P}} = \langle p_0, p_1, \ldots, p_{M-1}\rangle,\ M = 3^N$. The final probability of signal $a$ on input number $i$ is

$$P_a = \sum_{j \in U} p_j,$$

where $j \in U$ if $\mathbf{S}_j = \langle s_0, \ldots, s_j = a, \ldots, s_{N-1}\rangle$. The theorem will be proved if we demonstrate equality $p_i = p_{Tr_{\mathrm{ind}}}(i)$. According to (11), $\overline{\mathbf{P}}$ is eigenvector of $Q$. Denote

$$\mathbf{P}_{\mathbf{Tr}} = \langle p_{Tr_{\mathrm{ind}}(0)}, p_{Tr_{\mathrm{ind}}(1)}, \ldots, p_{Tr_{\mathrm{ind}}(M-1)}\rangle,$$

where $Tr_{\mathrm{ind}}$ is defined in (23). We have

$$\mathbf{P}_{\mathbf{Tr}}{}^T = Pr \cdot \overline{\mathbf{P}}^T, \tag{29}$$

where $Pr$ is a permutation matrix. Row $Pr[i,*]$ has 1 in position $Tr_{\mathrm{ind}}(i)$ and all other elements in the row are zeros. Let $B = Pr \cdot Q \cdot Pr'$. Column $Pr'[*,j]$ contains 1 in position $Tr_{\mathrm{ind}}(j)$.

$$B[i,j] = (Pr \cdot Q)[i,*] \cdot Pr'[*,j] = (Q[Tr_{\mathrm{ind}}(i), 1], \ldots,$$

$$Q[Tr_{\mathrm{ind}}(i), M-1] \cdot Pr'[*,j] = Q[Tr_{\mathrm{ind}}(i), Tr_{\mathrm{ind}}(j)]$$

Now,(24) can be rewritten in form $Pr \cdot Q \cdot Pr' = Q$. We have

$$Q \cdot \mathbf{P}_{\mathbf{Tr}}{}^T = Pr \cdot Q \cdot Pr' \cdot Pr \cdot \overline{\mathbf{P}}^T = Pr \cdot Q \cdot \overline{\mathbf{P}}^T = N \cdot Pr \cdot \overline{\mathbf{P}}^T = N \cdot \mathbf{P}_{\mathbf{Tr}}{}^T$$

It means that $\mathbf{P_{Tr}}^T$ is an eigenvector for $Q$. According to the suggestion of Theorem 4, there is only one eigenvector for $Q$ corresponding to eigenvalue $N$, so $\mathbf{P_{Tr}} = \overline{\mathbf{P}}$. In other words, state $\mathbf{S}$ and $Tr_{\text{ind}}(\mathbf{S})$ have equal final probabilities. □

The stable distributions of all designs are presented in columns of Table 8. To verify the proposition, let us obtain the probability of signal –1 on gate $S_0$. To this end, find all the states of form $\langle -1, x, y\rangle$, where $x, y$ are arbitrary values. Those states have indexes 0, 3, 6, 9, 12, 15, 18, 21, 24. Create a new table by selecting rows with these indexes from Table8 and find sum of items in each column. One reveals that all the sums equal 1/3 (all the values in the table are truncated to 2 digits after point, so some small errors can appear). The same can be done for the other gates and the values on their outputs.

## 5. Conclusions

The suggestion that delay times in different units are independent events is intrinsic, while the restriction on the form of distribution is much stronger. In practice, one has to take into account physical properties of the gates. It is desirable for all the gates to have identical electric load, otherwise the hypothesis that all units have the same delay time distribution fails. For TRNG, the condition of the same electric load is fulfilled, and this is a significant advantage of the design. On the other hand, one can obtain some special feature of the generator, which was described above, by using an alternative design. The accuracy of the results of the paper, if a deviation the the basic hypothesis exists, needs additional research.

## References

1. Asmussen S., Glynn P.W. Stochastic Simulation: Algorithms and Analysis. New York, Springer, 2007. 476 p. doi: 10.1007/978-0-387-69033-9.

2. Ferguson N., Schneie B., Kohno T. Cryptography Engineering: Design Principles and Practical Applications. Indianapolis, Wiley, 2010. 384 p.

3. Brederlow R., Prakash R., Paulus C., Thewes R. A low-power true random number generator using random telegraph noise of single oxide-traps. *IEEE Int. Solid-State Circuits Conf., Dig. Tech. Pap.*, 2006, pp. 536–537. doi: 10.1109/ISSCC.2006.1696222.

4. Buchovecka S., Lorencz R., Kodytek F., Bucek J. True random number generator based on ROPUF circuit. *Proc. 2016 Euromicro Conf. Digital Syst. Des.*, 2016, pp. 519–523. doi: 10.1109/DSD.2016.36.

5. Tokunaga C., Blaauw D., Mudge T. True random number generator with a metastability-based quality control. *IEEE Int. Solid-State Circuits Conf., Dig. Tech. Pap.*, 2007, pp. 404–405. doi: 10.1109/JSSC.2007.910965.

6. Horowitz P., Hill W. The Art of Electronics. Cambridge, Cambridge Univ. Press, 1980. 1125 p.

7. Petrie C.S., Connelly J.A. A noise-based IC random number generator for applications in cryptography. *Proc. IEEE Int.Symp. Circuits Syst., Atlanta*, 1996, vol. 4, pp. 324–327. doi: 10.1109/81.847868.

8. Golic J.D. New methods for digital generation and postprocessing of random data. *IEEE Trans. Comput.*, 2006, vol. 55, no. 10, pp. 1217–1229. doi: 10.1109/TC.2006.164.

9. 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.*, 2007, vol. 56, no. 1, pp. 109–119. doi: 10.1109/TC.2007.250627.

10. Kuznetsov V.M, Pesoshin V.A., Stolov E.L. Markov model of a digital stochastic generator. *Autom. Remote Control*, 2008, vol. 69, no. 9, pp. 1504–1509. doi: 10.1134/S0005117908090051.

11. Wieczorek P.Z., Gołofit K. Dual-metastability time-competitive true random number generator. *IEEE Trans. Circuits Syst.*, 2014, vol. 61, no. 1, pp. 134–145. doi: 10.1109/TCSI.2013.2265952.

12. Robson S., Leung B., Gong G. Truly random number generator based on a ring oscillator utilizing last passage time. *IEEE Trans. Circuits Syst., II: Express Briefs*, 2014, vol. 61, no. 12, pp. 937–941. doi: 10.1109/TCSII.2014.2362715.

13. Amaki T., Hashimoto M., Onoye T. An oscillator-based true random number generator with jitter amplifier. *Proc. IEEE Int. Symp. Circuits Syst.*, 2011, pp. 725–728. doi: 10.1109/ISCAS.2011.5937668.

14. Guo C., Zhou Y., Liu H., Zhu N. On the jitter and entropy of the oscillator-based random source. *Proc. 6th Int. Conf. Comput., Commun. Networking Technol.*, 2015, pp. 1–5. doi: 10.1109/ICCCNT.2015.7395169.

15. Weigandt T.C., Kim B., Gray P.R. Analysis of timing jitter in CMOS ring oscillators. *Proc. IEEE Int. Symp. Circuits Syst.*, 1994, pp. 27–30. doi: 10.1109/ISCAS.1994.409188.

16. Liu B. On VLSI statistical timing analysis and optimization. *Proc. IEEE 8th Int. Conf. on ASIC*, 2009, pp. 718–721. doi: 10.1109/ASICON.2009.5351306.

17. Liu T., Rabaey J. Statistical analysis and optimization of asynchronous digital circuits. *Proc. IEEE 18th Int. Symp. on Asynchronous Circuits Syst.*, 2012, pp. 1–8. doi: 10.1109/ASYNC.2012.21.

18. Yahya E., Fesquet L., Ismail Y., Renaudin M. Statistical static timing analysis of conditional asynchronous circuits using model-based simulation. *Proc. IEEE 19th Int. Symp. on Asynchronous Circuits Syst.*, 2013, pp. 67–74. doi: 10.1109/ASYNC.2013.12.

19. Xiao R., Chen C. Statistical delay modeling for single-electron-based circuits. *IEEE Trans. Nanotechnol.*, 2014, vol. 14, no. 4, pp. 676–686. doi: 10.1109/TNANO.2014.2315502.

20. Islam A., Nakai T., Onodera H. Statistical analysis and modeling of Random Telegraph Noise based on gate delay variation measurement. *Proc. Int. Conf. Microelectron. Test Struct.*, 2016, pp. 82–87. doi: 10.1109/ICMTS.2016.7476179.

21. Kim J., Kim W., Kim Y. Efficient statistical timing analysis using deterministic cell delay models. *IEEE Trans. Very Large Scale Integr. Syst.*, 2015, vol. 23, no. 11, pp. 2709–2713. doi: 10.1109/TVLSI.2014.2364736.

22. Wu X.W., Prosser F.P. CMOS ternary logic circuits. *IEE Proc.-G.: Circuits, Devices Syst.*, 1990. vol. 137, no. 1, pp. 21–27. doi: 10.1049/ip-g-2.1990.0005.

23. Gaikwad V.N., Deshmukh P.R. Design of CMOS ternary logic family based on single supply voltage. *Proc. IEEE Int. Conf. on Pervasive Comput., Sydney*, 2015, vol. 9, pp. 1–6. doi: 10.1109/PERVASIVE.2015.7087114.

24. Lisa N.J., Babu H.Md.H. Design of a compact ternary parallel adder/subtractor circuit in quantum computing. *Proc. IEEE Int. Symp. on Mult.-Valued Logic*, 2015, pp. 36–41. doi: 10.1109/ISMVL.2015.23.

25. Latypov R.Kh., Stolov E.L. Ternary jitter-based true random number generator. *IOP J. Phys.: Conf. Ser.*, 2017, vol. 783, art. 012064. doi: 10.1088/1742-6596/783/1/012064.

26. Kleinrock L. Queueing Systems. Vol. I: Theory. New York, Wiley-Intersci., 1980. 417 p.

27. Marcus M., Mink H. A Survey of Matrix Theory and Matrix Inequalities. Boston, Allys and Bacon, 1964. 232 p.

28. Bellman R. Introduction to Matrix Analysis. New York, Macgrow-Hill, 1960. 365 p.

Recieved
March 21, 2017

**Latypov Roustam Khafizovich**, Doctor of Technical Sciences, Head of Department of System Analysis and Information Technologies

Kazan Federal University
ul. Kremlevskaya 18, Kazan, 420008 Russia
E-mail: *Roustam.Latypov@kpfu.ru*

**Stolov Evgeny L'vovich**, Doctor of Technical Sciences, Professor, Department of System Analysis and Information Technologies

Kazan Federal University
ul. Kremlevskaya 18, Kazan, 420008 Russia
E-mail: *ystolov@kpfu.ru*

УДК 531.19+681.326

# Теория физических генераторов случайных чисел, использующих джиттер в схемах, составленных из одинаковых комбинационных схем, работающих в трехзначной логике

*Р.Х. Латыпов*[*], *Е.Л. Столов*[**]

*Казанский (Приволжский) федеральный университет, г. Казань, 420008, Россия*
E-mail: [*]*Roustam.Latypov@kpfu.ru*, [**]*ystolov@kpfu.ru*

Поступила 21.03.17

### Аннотация

В статье предлагается теория нового семейства генераторов случайных чисел, построенных из комбинационных логических блоков. Каждый блок реализует одну и ту же функцию трехзначной логики. Генератор состоит из нескольких таких блоков, и если схема содержит обратные связи, то в результате возникает явление, получившее название джиттер, или джиттеринг. Оно проявляется как случайное изменение сигнала на выходах блоков, а вся схема превращается в физический генератор случайных чисел. Основное внимание уделяется схемам, имеющим кольцевую структуру, но наряду с ними изучаются и другие схемы. В основе математической модели положено предположение, что все блоки срабатывают с некоторой случайной задержкой, имеющей экспоненциальное распределение, и эти задержки для разных блоков являются независимыми случайными величинами. Показано, что при указанных предположениях динамика генератора описывается дифференциальными уравнениями типа уравнений Эрланга в теории массового обслуживания. Рассматриваются также некоторые другие модели. Предложена процедура, превращающая указанное устройство в генератор независимых случайных величин, имеющих равномерное распределение. Обсуждаются свойства генерируемых многомерных случайных векторов, зависящие от способа соединения блоков в схеме. Статья является расширенной версией доклада, сделанного авторами на конференции [*Latypov R.Kh., Stolov E.L.* Ternary jitter-based true random number generator // IOP J. Phys.: Conf. Ser. – 2017. – V. 783. – Art. 012064. – doi: 10.1088/1742-6596/783/1/012064].

**Ключевые слова:** трехзначная логика, физический генератор, случайные числа, джиттер

**Литература**

1. *Asmussen S., Glynn P.W.* Stochastic Simulation: Algorithms and Analysis. – N. Y.: Springer, 2007. – 476 p. – doi: 10.1007/978-0-387-69033-9.
2. *Ferguson N., Schneie B., Kohno T.* Cryptography Engineering: Design Principles and Practical Applications. – Indianapolis, Wiley, 2010. – 384 p.
3. *Brederlow R., Prakash R., Paulus C., Thewes R.* A low-power true random number generator using random telegraph noise of single oxide-traps // IEEE Int. Solid-State Circuits Conf., Dig. Tech. Pap. – 2006. – P. 536–537. – doi: 10.1109/ISSCC.2006.1696222.
4. *Buchovecka S., Lorencz R., Kodytek F., Bucek J.* True random number generator based on ROPUF circuit // Proc. 2016 Euromicro Conf. Digital Syst. Des. – 2016. – P. 519–523. – doi: 10.1109/DSD.2016.36.
5. *Tokunaga C., Blaauw D., Mudge T.* True random number generator with a metastability-based quality control // IEEE Int. Solid-State Circuits Conf., Dig. Tech. Pap. – 2007. – P. 404–405. – doi: 10.1109/JSSC.2007.910965.
6. *Horowitz P., Hill W.* The Art of Electronics. – Cambridge, Cambridge Univ. Press, 1980. – 1125 p.
7. *Petrie C.S., Connelly J.A.* A noise-based IC random number generator for applications in cryptography // Proc. IEEE Int.Symp. Circuits Syst., Atlanta. – 1996. – V. 4. – P. 324–327. – doi: 10.1109/81.847868.
8. *Golic J.D.* New methods for digital generation and postprocessing of random data // IEEE Trans. Comput. – 2006. – V. 55, No 10. – P. 1217–1229. – doi: 10.1109/TC.2006.164.
9. *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. – 2007. – V. 56, No 1. – P. 109–119. – doi: 10.1109/TC.2007.250627.
10. *Kuznetsov V.M, Pesoshin V.A., Stolov E.L.* Markov model of a digital stochastic generator // Autom. Remote Control. – 2008. – V. 69, No 9. – P. 1504–1509. – doi: 10.1134/S0005117908090051.
11. *Wieczorek P.Z., Gołofit K.* Dual-metastability time-competitive true random number generator // IEEE Trans. Circuits Syst. – 2014. – V. 61, No 1. – P. 134–145. – doi: 10.1109/TCSI.2013.2265952.
12. *Robson S., Leung B., Gong G.* Truly random number generator based on a ring oscillator utilizing last passage time // IEEE Trans. Circuits Syst., II: Express Briefs. – 2014. – V. 61, No 12, P. 937–941. – doi: 10.1109/TCSII.2014.2362715.
13. *Amaki T., Hashimoto M., Onoye T.* An oscillator-based true random number generator with jitter amplifier // Proc. IEEE Int. Symp. Circuits Syst. – 2011. – P. 725–728. – doi: 10.1109/ISCAS.2011.5937668.
14. *Guo C., Zhou Y., Liu H., Zhu N.* On the jitter and entropy of the oscillator-based random source // Proc. 6th Int. Conf. Comput., Commun. Networking Technol. – 2015. – P. 1–5. – doi: 10.1109/ICCCNT.2015.7395169.
15. *Weigandt T.C., Kim B., Gray P.R.* Analysis of timing jitter in CMOS ring oscillators // Proc. IEEE Int. Symp. Circuits Syst. – 1994. – P. 27–30. – doi: 10.1109/ISCAS.1994.409188.
16. *Liu B.* On VLSI statistical timing analysis and optimization // Proc. IEEE 8th Int. Conf. on ASIC. – 2009. – P. 718–721. – doi: 10.1109/ASICON.2009.5351306.
17. *Liu T., Rabaey J.* Statistical analysis and optimization of asynchronous digital circuits // Proc. IEEE 18th Int. Symp. on Asynchronous Circuits Syst. – 2012. – P. 1–8. – doi: 10.1109/ASYNC.2012.21.

18. *Yahya E., Fesquet L., Ismail Y., Renaudin M.* Statistical static timing analysis of conditional asynchronous circuits using model-based simulation // Proc. IEEE 19th Int. Symp. on Asynchronous Circuits Syst. – 2013. – P. 67–74. – doi: 10.1109/ASYNC.2013.12.

19. *Xiao R., Chen C.* Statistical delay modeling for single-electron-based circuits // IEEE Trans. Nanotechnol. – 2014, V. 14, No 4. – P. 676–686. – doi: 10.1109/TNANO.2014.2315502.

20. *Islam A., Nakai T., Onodera H.* Statistical analysis and modeling of Random Telegraph Noise based on gate delay variation measurement // Proc. Int. Conf. Microelectron. Test Struct. – 2016. == P. 82–87. – doi: 10.1109/ICMTS.2016.7476179.

21. *Kim J., Kim W., Kim Y.* Efficient statistical timing analysis using deterministic cell delay models // EEE Trans. Very Large Scale Integr. Syst. – 2015. – V. 23, No 11. – P. 2709–2713. – doi: 10.1109/TVLSI.2014.2364736.

22. *Wu X.W., Prosser F.P.* CMOS ternary logic circuits // IEE Proc.-G.: Circuits, Devices Syst. – 1990. – V. 137, No 1. – P. 21–27. – doi: 10.1049/ip-g-2.1990.0005.

23. *Gaikwad V.N., Deshmukh P.R.* Design of CMOS ternary logic family based on single supply voltage // Proc. IEEE Int. Conf. on Pervasive Comput., Sydney. – 2015. – V. 9. – P. 1–6. – doi: 10.1109/PERVASIVE.2015.7087114.

24. *Lisa N.J., Babu H.Md.H.* Design of a compact ternary parallel adder/subtractor circuit in quantum computing // Proc. IEEE Int. Symp. on Mult.-Valued Logic. – 2015. – P. 36–41. – doi: 10.1109/ISMVL.2015.23.

25. *Latypov R.Kh., Stolov E.L.* Ternary jitter-based true random number generator // IOP J. Phys.: Conf. Ser. – 2017. – V. 783. – Art. 012064. – doi: 10.1088/1742-6596/783/1/012064.

26. *Kleinrock L.* Queueing Systems. V. I: Theory. – N. Y.: Wiley-Intersci., 1980. – 417 p.

27. *Marcus M., Mink H.* A Survey of Matrix Theory and Matrix Inequalities. – Boston: Allys and Bacon, 1964. – 232 p.

28. *Bellman R.* Introduction to Matrix Analysis. – N. Y.: Macgrow-Hill, 1960. – 365 p.

Поступила в редакцию
21.03.17

**Латыпов Рустам Хафизович**, доктор технических наук, заведующий кафедрой системного анализа и информационных технологий

Казанский (Приволжский) федеральный университет
ул. Кремлевская, д. 18, г. Казань, 420008, Россия
E-mail: *Roustam.Latypov@kpfu.ru*

**Столов Евгений Львович**, доктор технических наук, профессор кафедры системного анализа и информационных технологий

Казанский (Приволжский) федеральный университет
ул. Кремлевская, д. 18, г. Казань, 420008, Россия
E-mail: *ystolov@kpfu.ru*

***For citation***: Latypov R.Kh., Stolov E.L. Theory of ternary jitter-based true random number generators composed of identical gates. *Uchenye Zapiski Kazanskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki*, 2017, vol. 159, no. 2, pp. 246–262.

***Для цитирования***: *Latypov R.Kh., Stolov E.L.* Theory of ternary jitter-based true random number generators composed of identical gates // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. – 2017. – Т. 159, кн. 2. – С. 246–262.