DICHOTOMIC GENERATORS AND THEIR PROPERTIES

Igor A. Kulakov

Random Art Labs Limited
chief@random-art.com

Abstract. In this paper we consider the foundations for the construction of dichotomic generators, which form the core of stochastic systems. The ways of the formation and properties of simple and multiplex (one- and multidimensional) dichotomic generators in a modulo-2^n residue field $Z/2^n$ are considered. The generalization for compound algebraic structures is presented. Practical examples of the algorithm realizations of single- and multi-digit parametric counters and generators allowing parallel processing are listed. A preliminary analysis of the functional and statistic reliability of truncated and non-truncated dichotomic generators is presented. The conditions for attaining their functional insolubility in essence are noted.

The report continues the review of the results obtained in the field of stochastic systems and cryptography [1]. The results obtained considerably affect the parts of the theory of number and of algebraic systems, conceptions of the functional and statistic analysis, system analysis and the theory of dynamic systems. Taking into account the big amount and novelty of the accumulated theoretical material as well as the fact that the practical results are ahead of the theory, at first much attention is paid to practical aspects of the realization of constituent elements of dichotomic systems. The theoretical results will be presented in proportion as the theory is developed, mathematical concepts are worked out and the materials are published.

Not going into detail, by *stochastic systems* are meant statistic and dynamic systems of a special kind, which possess dual, more or less pronounced non-deterministic and deterministic properties inherent in Chaos. One can point out the following priority directions for the development of these systems:

The first direction connected with the dynamics, determines the principles of the formation of *dichotomic generators*, which form the new core of stochastic systems and cryptography.

The second direction involves the parts of *stochastic* and *network cryptography* and is conditioned by a strongly pronounced non-deterministic character of the stochastic system behavior.

The third direction, due to a strongly pronounced deterministic, and harmonic character of the behavior of such systems, gives rise to new possibilities in the field of *representation of abstract images* and *compositions*.

The report focuses on dichotomic generators, which are the most important constituent elements of cryptographic systems of new generation.

By definition, dichotomic or *Dh*-generators are used to form sequences of a special kind, which posses a variety of properties inherent in the binary representation of natural sequence, the so-called *dichotomic sequences* [2].

Let us consider the main aspects of the formation of *Dh*-generators, the formation of dichotomic sequences and the estimation of their properties by way of their priority, i.e.:

1. Method of formation and properties of *Dh*-generators in the residue field $\boldsymbol{Z}/2^n$.

2. Generalization of the formation method of *Dh*-generators for the compound algebraic structures, i.e., the fields $\boldsymbol{Z}/2^n$, the fields $\boldsymbol{Z}/2^{n-1}$ and then to the fields $\boldsymbol{Z}/2$.

3. Method of formation of multidimensional and parametric *Dh*-generators.

4. Method of formations of single- and multi-digit parametric *Dh*-counters and *Dh*-generators, which are oriented at the simplest binary parallel processing.

5. Analytic and statistic analysis of the functional and statistic reliability of the main implementation schemes of *Dh*-generators.

The binary sequence $D = \{d_i: i = \overline{1,T_n}\}$ composed of $T_n = 2^n$ non-negative integers d_i, which consist of n of significant bits $b_{ij} \in d_i$ $(j = \overline{1,n})$ with a dichotomic order fixed in this sequence is called a *dichotomic sequence* [2].

The dichotomic order can be easily illustrated by means of the binary representation of the first numbers of the natural sequence:

00	0000	04	0100	08	1000	12	1100
01	0001	05	0101	09	1001	13	1101
02	0010	06	0110	10	1010	14	1110
03	0011	07	0111	11	1011	15	1111

One can see from the formed binary sequence that the repetition period T_1 of the first bit is equal to 2^1, of the second bit is equal to 2^2, of the third bit is equal to 2^3, of the forth bit is equal to 2^4, etc., and of the k-th bit is $T_k = 2^k$ and of the n-th arbitrary bit is 2^n. The mentioned property characterizes the dichotomic order of the elements of this sequence.

Besides, note that for every k-th bit, elements i and $(i+T_k/2)$ belonging to adjacent half-cycles of this sequence are complementary, i.e., they are related by the complementation operation $\bar{}$ or, which is the same by the *NOT* operation (the relation being called dichotomic complement):

$$b_{ki} = \bar{b}_{k(i+Tk/2).}$$

Dichotomic sequences with complementary elements are called *perfect* or *D-sequences* [2]. Below we will only consider perfect dichotomic sequences.

Analogous dichotomic properties inherent in elements of the sequence C, which is formed on the basis of the linear binary congruent method [3, 5]; the method being based on the equation of the type:

$$x_i = a \cdot x_{i-1} + c \mod T_n, \qquad (1)$$

for $a \equiv 1 (\mod 4)$ and an odd c. In this case the number *card C* of all linear binary congruent sequences (or *D*-sequences, which is the same) is about $2^{3(n-1)}$.

In ordinary binary arithmetic or in a modulo-2^n residue field $\mathbf{Z}/2^n$, the cardinal number *card* D_Z of the set of all dichotomic sequences D_Z is about

$$card\ D_Z \approx 2^{n(n+3)/2-1}$$

and is determined accurate to the isomorphism by the recurrent expression:

$$d = \omega_o + \sum_{k=1}^{n} \omega_k\, b_k\, 2^{k-1} \mod 2^n \qquad (2)$$

with respect to the n-digit binary variable d and the bits $b_k \in d$ composing it, for all odd coefficients $\omega_o < 2^n$ and $\omega_k < 2^{(n-k)+1}$ and the condition $\omega_1 \equiv 1 (\mod 4)$. Expression (2) will be further called the *dichotomic equation in the field* $\mathbf{Z}/2^n$.

The dichotomic equation in the field $\mathbf{Z}/2^n$ is called the *linear* dichotomic equation, and the sequences formed on the basis of it is called *linear dichotomic sequences* D_Z. Note that the congruent sequences C are the special case $C \subseteq D_Z$ of the sequences D_Z.

However, the cardinal number *card D* of the set of all possible dichotomic sequences D is

$$card\ D = 2^{2^n - 1}.$$

The cardinal number is very large and considerably surpasses the number of all possible linear dichotomic sequences. The cardinal number shows the existence of an algebraic structure, which is more general than

the residue field $\mathbf{Z}/2^n$, the structure being able to generate *D*-sequences. Consider the following example for the determination of these structures.

Let us modify equation (1) of the linear congruent method in the following way:

$$z_i = a \cdot (h \oplus z_{i-1}) + c \mod 2^n, \tag{3}$$

where h is the modifier. Using the known relations

$$\alpha + \beta = 2 \cdot (\alpha \wedge \beta) + (\alpha \oplus \beta), \qquad \alpha + \beta = 2 \cdot (\alpha \vee \beta) - (\alpha \oplus \beta), \tag{4}$$

$$\alpha \oplus \beta = (\alpha + \beta) - 2 \cdot (\alpha \wedge \beta), \qquad \alpha \oplus \beta = -(\alpha + \beta) + 2 \cdot (\alpha \vee \beta), \tag{5}$$

we obtain

$$z_i = a \cdot z_{i-1} + (c + a \cdot h) - 2 \cdot a \cdot (h \wedge z_{i-1}) \mod 2^n \tag{6}$$

or

$$z_i = -a \cdot z_{i-1} + (c - a \cdot h) + 2 \cdot a \cdot (h \vee z_{i-1}) \mod 2^n. \tag{7}$$

If the conditions $h \equiv \overline{c}\ (mod\ 1)$, c is odd and $a \equiv 1 (mod\ 4)$ or c is even and $a \equiv 3 (mod\ 4)$ are fulfilled, the sequence generated by expressions (3), (6) or (7), is the *D*-sequence with the period $T_n = 2^n$. Moreover, by definition this sequence is the linear dichotomic sequence since the expansion

$$z = c_o + \sum_{k=1}^{n} c_k z_k 2^{k-1} \mod 2^n,$$

follows from expression (6),

where $z = \{ z_k : k = \overline{1,n} \}$, $h = \{ h_k : k = \overline{1,n} \}$,

$c_o = c + a h$, $c_k = a \cdot (1 - 2 \cdot h_k) \mod 2^{n-k+1}$.

At the same time, the *D*-sequence, which is recurrent to the *D*-sequence generated by expression (3), is presented by the expression inverse to it, i.e.,

$$z_{i-1} = h \oplus (a^{-1} \cdot z_i - c) \mod 2^n,$$

for $a^{-1} \cdot a \equiv 1 (mod\ 2^n)$. This expression cannot be presented in the form of expression (2), and consequently, it cannot be presented in a modulo-2^n residue field $\mathbf{Z}/2^n$, and in this respect is not the linear dichotomic sequence.

Note other properties, which are typical for expression (3). Note also that for nonzero values of the modifier h expressions (6) and (7) being equivalent to it contain linear and non-linear components. Thereby, this equation shows the dual character, i.e. the so-called *lined* character, according to which linear changes in some values of the argument are accompanied by jumpwise (non-linear) changes in other values. In this case the modifier action leads to the changes of the bits $z_k \in z$ statuses of the binary variable z and do not change the correlations between them. Further, depending on the state z of the variable, the multiplier a and the increment c cause fast and respectively slow redistribution of values and unidirectional correlation of bits of this variable from low-order to high-order bits.

Thus, from the algebraic point of view, the presented expression is characterized by the dual (the so-called lined) properties, i.e., by linear properties inherent in the field $\mathbf{Z}/2^n$ on the one hand, and by discrete properties inherent in the field $\mathbf{Z}/2$ on the other hand.

In the most general case the algebraic structures, which have in part or in whole linear properties inherent in the field $\mathbf{Z}/2^n$ on the one hand, and discrete properties inherent in the field $\mathbf{Z}/2$ on the other hand, and both linear and discrete properties in the fields $\mathbf{Z}/2^{n-1}$, $\mathbf{Z}/2^{n-2}$ and so on, will be called *lined structures*.

Based on these structures, there was developed the so-called *randomization method*, which is used to form ordinary, one- and multi-parametric, simple and multiplex multidimensional dichotomic generators with any repetition period being not smaller than the one given in advance. The generators possess relatively good statistic properties and a high functional complexity [1].

Dichotomic generators are easily adapted to any platforms of computing devices and allow to organize highly efficient sequential and multi-channel parallel, single- and multi-digit (including processorless) processing. They are capable of forming structural compositions of any complexity and can be functionally insoluble in essence and at the same time preserve unrepeated and other dichotomic properties inherent in their elements.

The formation of functionally multiplex dichotomic sequences and structural compositions is implemented by means of complexation of dichotomic generators and by means of multidimensional *Dh*-generators.

The simplest complexation of *Dh*-generators can be expressed by the lined function, which is given depending on the dichotomic variables *{z,x}* by the expression:

$$r = (h \oplus z) + 2\cdot(g \oplus x) \bmod 2^n, \qquad (8)$$

where *{h,g,r}* are binary *n*-digit vectors; *{h,g}* are arbitrary fixed modifiers; and *r* is the resultant dichotomic quantity.

The dichotomic generator can be multiplex, multidimensional and can be specified by a system of equations defined on a set of variables. One of the variants of the generator realization can be presented by a binary two-dimensional, so-called dual *Dh*-generator, given for two *n*-digit dichotomic variables *{u,v}* by the system of equations

$$u_i = (h_u \oplus u_{i-1}) + 2\cdot(g_u \oplus v_{i-1}) \bmod 2^n, \qquad (9)$$
$$v_i = (h_v \oplus v_{i-1}) + 2\cdot(g_v \oplus u_{i-1}) \bmod 2^n$$

where $\{h_u,h_v\}$ are fixed odd values and $\{g_u,g_v\}$ are arbitrary values of the modifier *{h,g}*.

Due to complexation and functional complexity dichotomic generators are capable of forming holistic structural compositions of any complexity. Based on the above mentioned randomization method, there were developed synthesis tools for such complex dichotomic systems [1].

The considered above ways of implementation of dichotomic generators work rather well under efficient realization of arithmetic operations and conditions provided that the digit capacity of registers used in computing devices is sufficient to perform machine commands. Otherwise, inefficient and complicated arithmetic of high numbers is required, which adversely affects the efficiency and prime cost of such devices.

The mentioned drawbacks can be eliminated with the help of vector *(segment)* generators. In this case, the generator platform composed of n bits, where $n = N \cdot m$, is divided into *N* equal *m*-digit segments (sub-blocks), whose length m coincides with the digit capacity of registers of the applied computing devices. The segments formed this way are linked with each other by their own result criterion formed using the calculation results so that the resultant output sequence generated by the generator is the dichotomic sequence with the common period $T_n = 2^{N \cdot m}$.

Below, we present the system of equations of the realization of *N*-segment *Dh*-generator; the equations being defined on a set of fixed modifiers $H = \{H_k\}$, $G = \{G_k\}$, $Q = \{Q_k\}$ and a vector dichotomic variable $Z = \{z_k\}$:

$$z_{ki} = z_I - z_{II} \bmod 2^m \qquad (k = \overline{1,N}), \qquad (10)$$
$$z_I = (2\cdot(G_k \oplus z_{k(i-1)})) \oplus p_{i-1} \bmod 2^m, \qquad z_{II} = H_k \oplus z_{k(i-1)},$$
$$p_i = \{Q_k:\ z_I < z_{II},\ \bar{Q}_k:\ z_I \geq z_{II}\},$$

at $p_0 = 1$ and an odd H_1. The presented algorithm is characterized by a mixed algebraic structure in the residue field and differs from the known methods by the way of p result criterion assignment. The analysis

shows that strongly pronounced correlation properties are inherent in elements of the dichotomic sequence formed on the basis of the mentioned equation. To overcome this drawback, it is sufficient to increase rate of the influence distribution of low-order bits on the high-order bits of this sequence. For example, it can be achieved using the following system of equations required for the realization of the *N*-segment *Dh*-generator:

$$z_{ki} = z_I - z_{II} \mod 2^m \qquad (k = \overline{1, N}), \tag{11}$$
$$z_I = (2\cdot(G_k \oplus z_{k(i-1)})) \oplus q_{i-1} \mod 2^m, \quad z_{II} = H_k \oplus z_{k(i-1)},$$
$$q_i = q_{i-1} \oplus z_{ki} \oplus \{Q_k:\ z_I < z_{II},\ \overline{Q}_k:\ z_I \geq z_{II}\}.$$

The above dichotomic generators are designed for the sequential processing. The efficiency of *Dh*-generators can be increased many times by using multi-channel generators. Multi-channel (multi-processor), parallel processing is provided by the *parameterization* of generators.

The idea of the division of the addition operation into simple component parts performed during the generator iteration lies in the heart of parameterization. Thus, for example, if the result criteria $\{p,q\}$ formed during calculations in (10) and (11) are used not at once but at the next generator iteration, then this generator can operate as a multi-channel generator.

The realization variant of an *N*-channel one-parametric *Dh*-generator from the set of parameters $P = \{r_k\}$ and the output dichotomic vector variable $R = \{r_k\}$ at an odd $p|_{k=1} = p_0$ fixed for every iteration can be presented by the following equation:

$$z = z_{k(i-1)}, \quad r_{ki} = (p \oplus z) + H_k \mod 2^m \quad (k = \overline{1, N}), \tag{12}$$
$$q = z \oplus \{Q_k:\ z < p,\ \overline{Q}_k:\ z \geq p\}, \quad z_{ki} = z - p \mod 2^m, \quad p = p_{k(i-1)}, \quad p_{ki} = q.$$

Among the peculiarities of the behavior of parametric dichotomic generators, note the presence of a short transient non-stationary interval τ, inherent in a wide class of dynamic systems. The interval being passed, these generators independently and phenomenally proceed to the stable state and everywhere within the period $T_n = 2^{N\cdot m}$ behave as unrepeated generators. Depending on the method of the generator realization and on the number of parameters p composing it (usually *2-3*), the length of the transient interval τ can reach the value of $p\cdot n$. This drawback is not an obstacle for the practical usage of these generators, since the drawback can be either easily eliminated or depending on the maximum length of the statistic sampling L_S in bits be set equal to $p\cdot log_2 L_S$ [2].

All the above-mentioned ways of dichotomic generator realizations provide the presence of a specialized arithmetic device or a processor, which affects the final cost of such generators, while the presence of the addition (subtraction) operation and moreover the presence of the multiplication operation affect the efficiency of these devices.

The parametric generators with simplest binary, one- and multi-digit parallel processing do not have these drawbacks. This processing is based on the idea of recurrent development of the addition (subtraction) operation into a finite number of the elementary binary operations performed step by step during the generator iteration or any other similar stochastic systems. In the residue field **Z***/2,* resulting from expression (4) and the complement-on-two operation $-\beta = \overline{\beta} + 1$, one can obtain the following expressions for the realization of additive arithmetic operations:

$$\alpha + \beta = 2\cdot(\alpha \wedge \beta) \oplus (\alpha \oplus \beta), \qquad \alpha - \beta = 2\cdot(\overline{\alpha} \wedge \beta) \oplus (\alpha \oplus \beta), \tag{13}$$

which can be realized using the half-adders of the necessary type.

Consider the optimal realization variants for the construction of parametric dichotomic generators. Let us focus on the simplest and analytically insoluble *Dh*-generators possessing the highest efficiency,

which can be compared only with the performance rate of one *XOR* operation; the number of n of bits composing the platform of such generators being insignificant.

The simplest *Dh*-generator given by the two-parametrical *{P,D}* randomization operator $R_C(H,P_{i-1},D_{i-1})$: $B_{i-1} \to \{B_i,P_i,D_i\}$, at $H \equiv 1(\ mod\ 2\ )$ being an odd fixed value of the modifier H and output $r_i = B_{i-1} \oplus D_{i-1}$, can be presented by the following composition of operators:

$$B_i = B_{i-1} \oplus P_{i-1},\ P_i = H\ \oplus D_{i-1},\ D_i = 2\cdot(B_{i-1} \wedge P_{i-1})\ \ mod\ 2^n. \qquad (14)$$

The generators of this type are characterized by a slow change of bits, which is typical of ordinary counters. These generators are hereafter called *dichotomic counters (Dh-counters)*.

Dichotomic variables *{B,D}* characterizing the internal generator state can be expressed through the known output generator state determined by the dichotomic variable r in the following form:

$$B_i = H\ \oplus B_{i-1} \oplus B_{i-2} \oplus \mathbf{r}_{i-1},\quad D_i = 2\cdot((\mathbf{r}_i \oplus D_{i-1}) \wedge\cdot(H\ \oplus D_{i-2}))\ \ mod\ 2^n.$$

The analytic insolubility of the generator equations (14) follows from the expressions, i.e., at any iteration, the changes in the internal generator state cannot be unambiguously expressed even through all known external states of this generator. Otherwise, it is impossible to solve analytically one of the following values and every preceding value of output variables of parametric generators using all their known external states, if changes of the variables characterizing their internal state are unknown and hidden from external access.

To reduce the essentially pronounced correlation inherent in dichotomic counters, it is necessary to the influence distribution of low-order bits on the high-order bits, which is realized consecutively during the generator iteration.

These, the so-called *dissipative Dh-generators of the first type*, can be represented by an auto-synchronous two-parametric *{P,D}* randomization operator $R_I\ (P_{i-1},D_{i-1})$: $B_{i-1} \to \{B_i,P_i,D_i\}$, composed of operators:

$$B_i = B_{i-1} \oplus P_{i-1},\quad P_i = (4\cdot B_{i-1})\ \oplus\ \bar{D}_{i-1}\ mod\ 2^n,\quad D_i = 2\cdot(B_{i-1} \wedge P_{i-1})\ mod\ 2^n. \qquad (15)$$

As in the previous case, the *Dh*-generator output can be represented by a similar equation of the type $r_i = B_{i-1} \oplus D_{i-1}$. Dichotomic variables *{B,D,P}* characterizing the internal state of the generator can be expressed through its known output state r_i in the following form:

$$B_i = B_{i-1} \oplus\ \bar{B}_{i-2} \oplus (4\cdot B_{i-2}) \oplus \mathbf{r}_{i-1}\ \ mod\ 2^n,$$

$$D_i = 2\cdot((\mathbf{r}_i \oplus D_{i-1}) \wedge ((4\cdot(\mathbf{r}_{i-1} \oplus D_{i-2}))\ \oplus\ \bar{D}_{i-2})\ \ mod\ 2^n,$$

$$P_i = (4\cdot B_{i-1})\ \oplus\ \bar{B}_{i-1} \oplus \mathbf{r}_i\ \ mod\ 2^n,\quad P_i = (4\cdot(\ \mathbf{r}_i \oplus D_{i-1}))\ \oplus\ \bar{D}_{i-1}\ \ mod\ 2^n.$$

The analytic insolubility of equation (15) follows from these expressions.

Despite the essentially pronounced avalanche properties inherent in the above-considered dissipative generators due to the influence distribution of low-order bits onto the high-order bits, these generators have essentially pronounced linear properties. The imparting of essentially pronounced non-linear properties to dichotomic sequences, formed on the basis of *Dh*-generators, can be realized using catenation of low-order bits with the high-order bits; the catenation being implemented consecutively during the iteration of these generators. Dissipative generators with the essentially pronounced non-linear properties will be called dissipative *Dh*-generators of the *second type*.

Dh-generators of the second type with the output $r_i = B_{i-1} \oplus D_{i-1}$, can be represented by an auto-synchronous three-parametric *{P,D,Q}* randomization operator $R_{II}(P_{i-1},D_{i-1},Q_{i-1})$: $B_{i-1} \to \{B_i,P_i,D_i,Q_i\}$, composed of operators:

$$B_i = B_{i-1} \oplus P_{i-1},\ \ P_i = (4\cdot B_{i-1})\ \oplus\ \bar{D}_{i-1}\ \ mod\ 2^n,\ \ Q_i = 2\cdot(B_{i-1} \wedge P_{i-1})\ mod\ 2^n, \qquad (16)$$

$$D_i = Q_{i-1} \oplus (4\cdot D_{i-1})\ mod\ 2^n.$$

Dichotomic variables $\{B,D,P,Q\}$ characterizing the internal state of this generator can be expressed through its known output state r_i in the following form:

$$B_i = B_{i-1} \oplus \overline{B}_{i-2} \oplus (4 \cdot B_{i-2}) \oplus \mathbf{r}_{i-1} \mod 2^n,$$
$$D_i = (2 \cdot ((\mathbf{r}_i \oplus D_{i-1}) \wedge ((4 \cdot (\mathbf{r}_{i-1} \oplus D_{i-2})) \oplus \overline{D}_{i-2})) \oplus (4 \cdot D_{i-1}) \mod 2^n,$$
$$P_i = (4 \cdot B_{i-1}) \oplus \overline{B}_{i-1} \oplus \mathbf{r}_i \mod 2^n, \quad P_i = (4 \cdot (\mathbf{r}_i \oplus D_{i-1})) \oplus \overline{D}_{i-1} \mod 2^n,$$
$$Q_i = 2 \cdot (B_{i-1} \wedge ((4 \cdot B_{i-2}) \oplus \overline{B}_{i-2} \oplus \mathbf{r}_{i-1})) \mod 2^n,$$
$$Q_i = 2 \cdot ((r_i \oplus D_{i-1}) \wedge (((4 \cdot (\mathbf{r}_{i-1} \oplus D_{i-2})) \oplus \overline{D}_{i-2})) \mod 2^n.$$

The analytic insolubility of equation (16) follows from these expressions.

Parametric generators can be multiplex, multidimensional and can be represented by a system of equations defined on a set of variables. One of realization variants of these generators can be represented by a two-dimensional, four-parametric $\{P_u,D_u,P_v,D_v\}$ autosynchronous dual *Dh*-generator with many outputs $r_{ui} = B_{u(i-1)} \oplus D_{u(i-1)}$ and $r_{vi} = B_{v(i-1)} \oplus D_{v(i-1)}$, which is represented by a system of equations consisting of randomization operators

$$R_D(P_{u(i-1)},D_{u(i-1)}): \{U_{i-1},V_{i-1}\} \to \{U_i,P_{ui},D_{ui}\}, \qquad R_D(P_{v(i-1)},D_{v(i-1)}): \{V_{i-1},U_{i-1}\} \to \{V_i,P_{vi},D_{vi}\},$$

which are presented by analytically insoluble compositions of operators of the type:

$$U_i = U_{i-1} \oplus P_{u(i-1)}, \quad P_{ui} = (4 \cdot V_{i-1}) \oplus \overline{D}_{u(i-1)} \mod 2^n, \quad D_{ui} = 2 \cdot (U_{i-1} \wedge P_{u(i-1)}) \mod 2^n, \qquad (17)$$
$$V_i = V_{i-1} \oplus P_{v(i-1)}, \quad P_{vi} = (4 \cdot U_{i-1}) \oplus \overline{D}_{v(i-1)} \mod 2^n, \quad D_{vi} = 2 \cdot (V_{i-1} \wedge P_{v(i-1)}) \mod 2^n.$$

Parametric *Dh*-generators can be represented not only by a relatively simple system of equations given above, but also by a more complicated system of equations for a set of variables possessing the dichotomous properties. Using the developed formal tools of synthesis of such systems [1], it is possible to create different stochastic and cryptographic distributed systems, which will be of any functional and structural complexity than the one given in advance.

The considered above theoretical and technical aspects of realization of dichotomic generators show the possibility of obtaining the analytic insolubility of the dichotomic sequences formed on their basis. At the same time, the analytic insolubility, obtained due to multidimensionality and parameterization of *Dh*-generators, is necessary but not sufficient to form efficient cryptographic devices and systems. Based on the general requirements to generators of random numbers [2, 5], as a case of sufficient conditions of achieving the cryptographic reliability of *Dh*-generators are the statistic properties of the sequences formed on their basis with the distribution law being close to *ideal* uniform.

Following these conditions, consider the most characteristic statistic properties of dichotomic sequences and quantities. First, let us define the term "slice" of the binary sequence $Z = \{z_i: i = \overline{1,L}\}$ formed of L non-negative integers z_i, composed of n significant bits $b_{si} \in z_i$ $(s = \overline{1,n})$.

The binary sequence $Z_s = \{b_{si}: i = \overline{1,L}\}$, composed of all $b_{si} \in \{0,1\}$ bits of the binary sequence Z initial to it is called the *slice* s. The slice $\Delta Z_s = \{b_{s(i-1)} \oplus b_{si}\}$ for $b_{so} = 0$, formed over the slice Z_s will be called the *difference slice* s.

Due to essentially pronounced deterministic behavior of low-order bits of dichotomic quantities and complementation of dichotomic classes generated by them, strong statistic dependence is inherent in bits belonging to low-order slices of realization of these quantities. Depending on the influence distribution rate of low-order bits onto the high-order bits and their catenations, which are provided by the equations of generation of dichotomic sequences, the correlation between slice bits can be preserved or either rapidly or

can slowly decrease from slice to slice.

As the first example, consider the variant of realization of the N-channel two-parametric $\{P,D\}$ dissipative dichotomic generator of the first type, otherwise, the Δ_N -generator, which is given by the randomization operator $R_\Delta(P_{i-1},D_{i-1})$: $B_{i-1} \to \{B_i,P_i,D_i\}$, composed of operators:

$$B_{ki} = B_{k(i-1)} \oplus P_{k(i-1)}, \quad P_{ki} = (4 \cdot B_{k(i-1)}) \oplus \overline{D}_{k(i-1)} \bmod 2^m \quad (k = \overline{1,N}), \tag{18}$$
$$D_{ki} = (2 \cdot (B_{k(i-1)} \wedge P_{k(i-1)})) \vee Q \bmod 2^m, \quad Q = Q_{k(i-1)}, \quad Q_{ki} = (B_{k(i-1)} \wedge P_{k(i-1)})/2^{m-1},$$

with the output $r_{ki} = B_{k(i-1)} \oplus D_{k(i-1)}$, for $Q|_{k=1} = 0$. The analytic insolubility of equations (18) follows from the analytic insolubility of equations (15).

The statistic analysis of slices, which was performed using the statistical test package DIEHARD [6], shows the presence of an essential correlation between bits of low-order channel slices $s = (k-1) \cdot m + 1$ for any m. For $m = 32$, note an inessential correlation between bits of high-order channel slices $s = k \cdot m - 1$. The essential correlation between slice bits is provided by low digit capacity of registers on the one hand, and the absence of the mechanisms of the influence distribution of bits between blocks, on the other hand.

High statistic characteristics can be achieved using generators, which provide the influence distribution between channel bits. As an example of such a generator, consider the variant of realization of an N-channel three-parametric $\{P,D,G\}$ dissipative dichotomic generator of the first type, otherwise, the ∇_N -generator, which is given by a randomization operator $R_\Delta(P_{i-1},D_{i-1},G_{i-1})$: $B_{i-1} \to \{B_i,P_i,D_i,G_i\}$, composed of operators:

$$B_{ki} = B_{k(i-1)} \oplus P_{k(i-1)}, \quad P_{ki} = (4 \cdot B_{k(i-1)}) \oplus D_{k(i-1)} \bmod 2^m \quad (k = \overline{1,N}), \tag{19}$$
$$D_{ki} = G \oplus G_{k(i-1)}, \quad G_{ki} = (2 \cdot (B_{k(i-1)} \wedge P_{k(i-1)})) \vee Q \bmod 2^m,$$
$$G = \mathbf{rot}_L(B_{k(i-1)},S_G), \quad Q = Q_{k(i-1)}, \quad Q_{ki} = \cdot (B_{k(i-1)} \wedge P_{k(i-1)})/2^{m-1},$$

with the output $r_{ki} = B_{k(i-1)} \oplus D_{k(i-1)}$ for $G|_{k=1} = G_o$ and $Q|_{k=1} = G_o \bmod 2$. Here, $\mathbf{rot}_L$ is the operation of the cyclic shift $\mathbf{rot}_L(B_{k(i-1)},S_G)$ of the binary m-bit variable B_k by S_G bits to the left, which is equal to the nearest prime for $m/3$ and aliquant with m. Similarly to the above-mentioned cases, the analytic insolubility of equation (19) follows from analytic insolubility of equation (18).

According to the statistic analysis results [6], no noticeable correlation of slice bits and difference slices (starting with 27) formed on their basis, is revealed under any initial conditions.

While testing the dichotomic sequences of ∇_N -generators, note the following results. For a short length $n = N \cdot m$ of the generator platform, there exists an essential correlation between the elements of dichotomic sequences formed by the ∇_N -generator. For an average length 256-512 bits of the generator platform, the statistics is unstable. The correlation slowly decreases with increasing n. The statistics is stable and satisfactory for $24 \times 32 = 768$ bits $(N=24, m=32)$, for $64 \times 16 = 964$ bits and for $162 \times 8 = 1296$ bits and more in the platform.

The situation changes drastically when 32 low-order correlated slices are truncated. For the $\nabla_{(N-32/m)}$ -generators truncated this way, the statistics is satisfactory for $5 \times 32 = 160\ (160 - 32 = 128)$ bits $(N=5, m=32)$, for $6 \times 16 = 96\ (48)$ bits and for $9 \times 8 = 72\ (40)$ bits and more in the platform; the brackets denoting the length of the generator output block.

Note the improvement of statistic characteristics of sequences of the difference type $\Delta r_{ki} = r_{k(i-1)} \oplus r_{ki}$ for $r_{ko} = 0$; the sequences are formed from truncated D-sequences initial to them.

In contrast to non-truncated dichotomic sequences, truncated *D*-sequences within the repetition period 2^n are not unrepeated sequences. The average estimates of the repetition number for the above ∇_N-generator performed for 500 statistical samples of different length are shown below in the Table.

Testing of repetition number

Statistical sample	**65536**	**32768**	**16384**	**8192**	**4096**	**2048**	**1024**	**512**	**256**
Truncation ∇_N	**non-truncated *D*-sequence is unrepeated**								
1	16379	4096	1021	255	65	16	4	0.96	0.15
2	20738	5646	1473	376	94	24	6	1	0.31
4	23343	6662	1785	463	118	30	7	2	0.37
8	24063	6962	1879	490	125	31	8	2	0.39
16	24112	6985	1886	491	125	31	8	2	0.43
Empiric Law	**24109**	**6981**	**1895**	**495**	**127**	**32**	**8**	**2**	**0.53**
RC4	24107	6979	1887	491	126	31	8	2	0.47
GOST 28147-89	24107	6981	1886	492	125	31	8	2	0.44

The estimates presented in the Table do not depend on the length of the registers being used and quickly converge in to surjective, the so-called *gamma generators* of the RC4 type, and in to block ciphers which function in the output feedback regime.

The performed statistic analysis would be incomplete without the estimate of reachability of statistic uncertainty of high-order bits of dichotomic *n*-bit quantities, which are formed by *Dh*-generators. As this estimate, we take the factor of $0 \le \rho \le n$, which is comparable with the value of 2^{ρ} and characterizes on average the depth of the possible enumeration of bits of the mentioned dichotomic quantity, this depth being necessary for predicting every of the next realization elements of this quantity.

The calculation of the estimate ρ is performed over all slices Z_s $(s = \overline{1,n})$, which belong to the statistic sampling formed by the *Dh*-generator in the following way.

Over all slices of the length equal to L_S bits, there are calculated the repetition number R_{1L} of the 1-series of the length $L = \{1,2,\ldots L_S\}$, which consists only of unities, and the repetition number R_{0L} of the 0-series of length *L*, which consists only of zeros. Consequently, the identity

$$1\cdot(R_{11} + R_{01}) + 2\cdot(R_{02} + R_{02}) + \ldots L\cdot(R_{0L} + R_{0L}) + \ldots L_S\cdot(R_{0Ls} + R_{0Ls}) \equiv L_S.$$

takes place.

From this identity, following Golomb's second postulate [7], let us calculate the heuristic evaluations P_{BL} of non-determinacy of bits of series

$$P_{BL} = (1 - |2\cdot Q_{BL}^{\,1/(L+2)} - 1|)^q, \qquad q = 1 + log_2(1 + L_S / T) \qquad (0 \le P_{BL} \le 1),$$

where $B = \{1,0\}$ is the series type and $Q_{BL} = R_{BL} / L_S$ and *T* is the repetition period of *s*-slice.

The non-determinacy factor ρ_S of the corresponding *s*-slice

$$\rho_s = -\log_2\left(1 - k_\rho \sum_{L=1}^{L_S} \frac{L}{2^L}(P_{1L} + P_{0L})\right), \qquad k_\rho = 0.5 / \sum_{L=1}^{L_S} \frac{L}{2^L} \qquad (0 \le \rho_s \le 1)$$

can be calculated using the results of the evaluations P_{BL}.

Hence, the depth factors ρ of the complete enumeration of bits of the dichotomic quantity concerned with the *Dh*-generator output is determined on a set of *E* statistical samples by the expression

$$\rho_e = \sum_{s=1}^{n} \min\{\rho_{s(e-1)}, \rho_{se}\} \qquad (e = \overline{1,E},\ 0 \le \rho_e \le n), \tag{20}$$

by summing in the direction from low-order significant bits to high-order bits and for all $\rho_{s0} = 1$.

The table showing calculations of non-determinacy factors ρ_S for 16 (32) slices and the depth factors ρ_{150} of the complete enumeration of bits is presented below. The values are calculated using 150 statistical samples, which comprise 131970 non-negative 32-digit binary numbers for the RC4 generator of random numbers and a multi-channel 8-digit ∇_N -generator under the different number of low-order significant bits truncating (*TRN*) it.

TRN	**1**/17	**2**/18	**3**/19	**4**/20	**5**/21	**6**/22	**7**/23	**8**/24	**9**/25	**10**/26	**11**/27	**12**/28	**13**/29	**14**/30	**15**/31	**16**/32	ρ_{150}
0	0.000	0.000	0.000	0.019	0.024	0.120	0.189	0.307	0.387	0.268	0.515	0.262	0.461	0.408	0.647	0.426	**16.001926**
	0.539	0.726	0.663	0.810	0.724	0.806	0.691	0.803	0.823	0.743	0.798	0.746	0.861	0.705	0.839	0.691	
32	0.766	0.864	0.804	0.838	0.807	0.823	0.799	0.845	0.864	0.814	0.878	0.825	0.845	0.804	0.875	0.814	**26.396966**
	0.836	0.867	0.858	0.896	0.836	0.895	0.845	0.883	0.897	0.835	0.901	0.808	0.912	0.846	0.924	0.861	
64	0.875	0.901	0.882	0.917	0.865	0.926	0.852	0.918	0.924	0.873	0.921	0.878	0.945	0.884	0.932	0.875	**28.298560**
	0.884	0.945	0.885	0.938	0.903	0.942	0.911	0.944	0.942	0.918	0.946	0.924	0.942	0.919	0.945	0.917	
128	0.958	0.979	0.952	0.977	0.957	0.979	0.953	0.976	0.981	0.963	0.979	0.960	0.982	0.966	0.983	0.960	**30.189417**
	0.960	0.973	0.966	0.984	0.974	0.983	0.971	0.984	0.985	0.974	0.987	0.974	0.989	0.978	0.987	0.973	
224	0.993	0.992	0.992	0.992	0.992	0.993	0.993	0.994	0.993	0.994	0.993	0.993	0.993	0.993	0.993	0.993	**30.782163**
288	0.993	0.993	0.993	0.993	0.993	0.993	0.993	0.994	0.994	0.993	0.993	0.993	0.993	0.993	0.994	0.992	**30.787265**
RC4	0.993	0.993	0.993	0.993	0.993	0.994	0.993	0.993	0.993	0.994	0.994	0.992	0.993	0.993	0.994	0.993	**30.787472**

One can see from the results of the testing that the statistic properties of the ∇_N-generator slices approximate to the statistic properties of the RC4 generator slices. At the same time, beginning somewhat with the 224th bit, one can observe the equalization of their properties. In the general case, note that 40-channel 8-digit *(ρ_{150} = 30.787265)* ∇_N-generators truncated on 288 bits and 13-channel 16-digit *(ρ_{150} = 30.786975)* ∇_N -generators truncated on 164 bits as well as 4-channel 32-digit *(ρ_{150} = 30.787333)* ∇_N -generators truncated on 90 bits and so on do not differ from the RC4 generator *(ρ_{150} = 30.787472)* chosen as standard in the statistic properties of all output bits.

Consequently, one can conclude that the high-order bits of the above-mentioned ∇_N -generators in their statistic properties can be on par with binary sequences formed on the basis of the most advanced and investigated generators of random numbers. Thereby, it is possible to assert about the possibility of reachability of statistic non-determinacy of random number sequences formed on the basis of dichotomic generators, the statistic non-determinacy being virtually identical.

As a result, taking into account the facts as

(i) the proved above analytic insolubility of the equations of operation of parametric and multidimensional *Dh*-generators,

(ii) the performed statistic analysis [6], which confirms the distribution of bits of high-order slices close to ideal uniform (including their difference slices),

(iii) the presented analysis of statistic properties [6] and of distribution of the repetition number of truncated *Dh*-generators as well as the analysis on the basis of equation (20), which show the possibility of reachability of statistic uncertainty of bits close to ideal

We can speak about the possibility of attaining the functional insolubility in essence of random sequences from the high-order significant bits, where the sequences are formed using the mentioned *Dh*-generators. Moreover, as the analysis shows, it is achieved independently of the initial generation conditions of these sequences.

.

In the most general case, based on the dichotomic generators possessing the functional insolubility in essence, one can rather simply create cryptographically powerful unrepeated Running Key Generators and equirepeated Gamma Generators. It can be achieved by bijective and surjective transformation of dichotomic sequences, which means the influence distribution of high-order bits onto the low-order bits, and vice versa and bit catenation as well as confusion of the transformed bits due to efficient techniques. Using these transformations, higher statistic factors of the sequences being formed can be achieved and a more reliable hiding of dichotomic properties inherent in initial *D*-sequences is provided.

As a rule, the practical result is optimal if the tasks of the dichotomic sequence formation and their transformations are mutually specified and superadditive, they are uniquely irreversible, they supplement each other and are in harmony with each other. The solution of these problems is the topic of the next part, i.e., stochastic cryptography, which will be presented in future.

By generalizing the aforesaid, we come to the following conclusions:

1. Dichotomic generators in their statistic properties, functional complexity and efficiency, surpass the most commonly used linear recurrent generators, which operate using the linear feedback shift registers (LFSRs). Thus, as for the hardware design, the operation rate of such generators can be comparable with the performance rate of one XOR operation, the length of the generator platform being insignificant.

2. The realization schemes of dichotomic generators are very simple, allow parallel single-digit and multi-digit (including processorless) hardware processing on any platforms of computing devices, they require small storage capacity and they are designed to use keys of variable length.

3. The realization schemes are transparent for analysis, they are algebraically complicated and closed, they are of highly dynamic and parametric, hidden from the environment, simple or multiplex, multidimensional, essentially pronounced constrained and nonlinear character. As a result, they can possess sufficient for practical applications statistic and functional reliability. In software realizations, they have no match among the most perfect samples. As for the hardware, they are distinguished high efficiency and low prime cost.

4. Dichotomic generators can have any repetition period that is not smaller than the one given in advance. They are capable of forming structural compositions of any complexity. They can be functionally insoluble in essence from the high-order significant bits and at the same time preserve the unrepeated properties inherent in their elements.

5. The above-mentioned properties of dichotomic sequences allow, using simple and transparent for analysis ways, to obtain simply and efficiently statistically and functionally reliable, for practical applications, unrepeated and equirepeated sequences of uniformly distributed numbers.

6. Dichotomic generators and methods of their formation lay the foundations of stochastic cryptography, which is intended for the construction of one- and multi-round parametric and non-linear binary stochastic converter of one-sided functions and operators. Within the framework of this direction, there were developed unrepeated Running Key Generators, equirepeated Gamma Generators, non-linear adders and integrators, hash functions of different applications and a symmetric iterative RACH block cipher with the variable number of rounds, based on special controlled operations.

7. Dichotomic generators lay the basis of the network cryptography. The latter consists of protocols, tools and technologies for the formation of distributed multidimensional, parametric, holistic, and

structurally multiplex dichotomic generators, cryptographic means and security systems of new generation, oriented at network solutions of any complexity, super-high-speed and highly reliable processing.

8. Dichotomic generators and the methods of their formation provide a high level unification and standardization due to universal and uniform character of the cryptographic modules and components being used.

9. The presented technologies retain the succession and they are permanent due to the fundamental character of the theoretical base and its conceptual connection with the processes and phenomena inherent in complicated dynamic systems and real nature. This is verified by investigations of behavior of stochastic systems and devices based on them, by the presence of peculiar dichotomic, lined and dual properties, attractors and transient processes in them, after which they independently and phenomenally proceed in a stable state. Note also miraculous similarities with the processes happening in the micro world.

10. The multidimensional and parametric structure of dichotomic generators and essentially pronounced non-linear character of behavior of dichotomic generators and similar stochastic devices and systems caused by this structure, as well as the properties which they exhibit allow speaking about the anticipatory character of calculation physics. This is especially urgent on the threshold of the revolution in the field of nano-technologies, holographic and quantum processing.

Keywords. Dynamic system. Attractor. Functional insolubility. Chaos. Stochastic system. Symmetric cryptography. Network cryptography. Random-number generator. Dichotomic order. Dichotomic sequence. Dichotomic generator. Randomization method. Randomization system.

References

1. I. A. Kulakov "A Method of the Randomization Properties Imparting to a Real Object and a Randomization System" Application for the International Patent.

2. I. A. Kulakov "Dichotomic sequences and their properties",
Article based on the materials of the report presented at the 3rd Central-European Conference in Bratislava, TATRACRYPT 2003, 26-28 June, 2003, Slovakia

3. D. Knuth "The Art of Computer Programming",
Volume.2, Seminumerical Algorithms, 2nd edition Addison-Wesley, 1981

4. R. Lidl, H. Niederreiter "Finite Fields,"
Encyclopedia of Mathematics and its Applications, v.20, Addison-Wesley, 1983

5. B. Schneier APPLIED CRYPTOGRAPHY. Protocols, Algorithms, and Source Code in C,
John Wiley & Sons, Inc, 1996

6. G. Marsaglia DIEHARD Statistical Test Package,
1997, geo@stat.fsu.edu

7. S.W. Golomb Shift Register Sequences,
San Francisco: Holden-Day, 1967. (Reprinted by Aegean Park Press, 1982.)