ДИХОТОМИЧЕСКИЕ ГЕНЕРАТОРЫ И ИХ СВОЙСТВА

Кулаков Игорь Анатольевич

Random Art Labs Limited
chief@random-art.com

Рассматриваются основы построения дихотомических генераторов, составляющих ядро стохастических систем. Рассматриваются способы построения и свойства простых и сложных (одномерных и многомерных) дихотомических генераторов в поле вычетов $\boldsymbol{Z}/2^n$ по модулю 2^n. Производится обобщение на случаи смешанных алгебраических структур. Приводятся практические примеры алгоритмов реализации одно- и многоразрядных, допускающих параллельную обработку параметрических счетчиков и генераторов. Дается предварительный анализ функциональной и статистической надежности усеченных и неусеченных дихотомических генераторов. Отмечаются условия достижения их функциональной неразрешимости по существу.

В статье продолжается обзор результатов, полученных в области стохастических систем и криптографии [1]. Полученные результаты существенно затрагивают разделы теории чисел и алгебраических систем, положения функционального и статистического анализа, системный анализ и теорию динамических систем. Учитывая большой объем и новизну накопленного в этой части теоретического материала, а также и то, что практические результаты несколько опережают теорию, на первых шагах основное внимания уделяется практическим аспектам реализации составляющих элементов дихотомических систем. Теоретические результаты будут представляться последовательно по мере становления теории, отработки математических понятий и публикации фактического материала.

Не вдаваясь в детали, под *стохастическими системами* будем понимать статические или динамические системы особого рода, обладающие двойственными, существенно или менее сильно выраженными недетерминированными и детерминированными свойствами присущими Хаосу. Можно выделить следующие приоритетные направления развития этих систем.

Первое направление, связанное с динамикой, определяет принципы построения *дихотомических генераторов*, закладывающих новое ядро стохастических систем и криптографии.

Второе направление включает в себя разделы *стохастической и сетевой криптографии* и обусловлено сильно выраженным недетерминированным характером поведения стохастических систем.

Третье направление, в силу сильно выраженного детерминированного, гармоничного характера поведения таких систем, открывает новые возможности в области *представления абстрактных образов и композиций*.

В докладе основное внимание уделяется дихотомическим генераторам, как одним из наиболее важных составляющих элементов криптографических систем нового поколения.

По определению, дихотомические или *Dh*-генераторы предназначены для формирования последовательностей специального вида, обладающих комплексом свойств присущим двоичному представлению чисел натурального ряда, так называемых *дихотомических последовательностей* [2].

Рассмотрим основные аспекты построения *Dh*-генераторов, формирования дихотомических последовательностей и оценки их свойств, в порядке их очередности. К ним относятся:

1. Способы построения и свойства *Dh*-генераторов в поле вычетов $\boldsymbol{Z}/2^n$.

2. Обобщение способов построения *Dh*-генераторов на случаи смешанных алгебраических структур - поля $\boldsymbol{Z}/2^n$, поля $\boldsymbol{Z}/2^{n-1}$ и далее, до поля $\boldsymbol{Z}/2$.

3. Способы построения многомерных и параметрических *Dh*-генераторов.

4. Способы построения, ориентированных на простейшую двоичную параллельную обработку, одно- и многоразрядных параметрических *Dh*-счетчиков и *Dh*-генераторов.

5. Аналитический и статистический анализ функциональной и статистической надежности основных схем реализаций *Dh*-генераторов.

Двоичная последовательность $D = \{d_i: i = \overline{1, T_n}\}$ из $T_n = 2^n$ неотрицательных целых чисел d_i, составленных из n значащих бит $b_{ij} \in d_i$ $(j = \overline{1, n})$, с установленным в ней *дихотомическим порядком*, называется *дихотомической последовательностью* [2].

Дихотомический порядок, можно наглядно продемонстрировать на основе двоичного представления первых чисел натурального ряда.

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

Из образованной таким образом двоичной последовательности видно, что период повторения T_1 первого бита равен 2^1, второго 2^2, третьего 2^3, четвертого 2^4 и так далее, k-го $T_k = 2^k$, а n-го 2^n, для произвольного n. Указанное свойство характеризует *дихотомический порядок* элементов данной последовательности.

Кроме этого, можно заметить, что для каждого k-го бита, i и $(i+T_k/2)$ элементы принадлежащие соседним полупериодам этой последовательности комплементарны, т.е. посредством операции комплементации $\bar{}$ *(операции НЕ)*, связаны соответствием

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

именуемым *дихотомическим комплементом*.

Дихотомические последовательности, с комплементарными элементами, называются *совершенными* или *D-последовательностями* [2]. Далее рассматриваются совершенные дихотомические последовательности и это специально не оговаривается.

Аналогичные дихотомические свойства присущи элементам последовательностей C, формируемым на основе линейного двоичного конгруэнтного метода [3, 5], задаваемым уравнением, вида:

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

при $a \equiv 1 (mod\ 4)$ и нечетном c. При этом число *card C* всех различных таких линейных двоичных конгруэнтных или тоже, что *D*-последовательностей, составляет величину, около $2^{3(n-1)}$.

В ординарной двоичной арифметике или тоже, что в поле вычетов $\mathbf{Z}/2^n$ по модулю 2^n, кардинальное число $card\ D_Z$ множества всех различных дихотомических последовательностей D_Z, приблизительно равно

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

и с точностью до изоморфизма определяется рекуррентным выражением:

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

относительно n-разрядной двоичной переменной d и составляющих ее бит $b_k \in d$, при любых нечетных коэффициентах $\omega_o < 2^n$ и $\omega_k < 2^{(n-k)+1}$ и условии $\omega_1 \equiv 1 (mod\ 4)$, именуемым *дихотомическим уравнением в поле* $\mathbf{Z}/2^n$.

Дихотомическое уравнением в поле $\mathbf{Z}/2^n$ будем также называть *линейным* дихотомическим уравнением, а формируемые на его основе последовательности - *линейными дихотомическими после-*

довательностями D_Z. Легко показать, что конгруэнтные последовательности C, есть частный случай $C \subseteq D_Z$ последовательностей D_Z.

Между тем, кардинальное число $card\, D$ множества всевозможных различных дихотомических последовательностей D, равно:

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

Кардинальное число очень велико и существенно превосходит число всевозможных различных линейных дихотомических последовательностей. Кардинальное число указывает, на существование более общей алгебраической структуры, чем поле вычетов $\mathbf{Z}/2^n$, способной порождать D-последовательности. Для определения свойств этих структур, рассмотрим следующий пример.

Модифицируем уравнение (1) линейного конгруэнтного метода следующим образом:

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

где h - модификатор. Используя известные соотношения

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

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

получим

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

или

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

При выполнении условий $h \equiv \overline{c}\ (mod\ 1)$, c - нечетно и $a \equiv 1 (mod\ 4)$ или c - четно и $a \equiv 3 (mod\ 4)$, порождаемые этими уравнениями (3), (6) или (7), последовательность, есть D-последовательность с периодом $T_n = 2^n$. Более того, эта последовательность по определению, есть линейная дихотомическая последовательность, так как из уравнения (6) следует разложение

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

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

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

Вместе с тем, D-последовательность, рекуррентная к D-последовательности порождаемой уравнением (3), как следует из обратного к нему уравнения:

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

при $a^{-1} \cdot a \equiv 1 (mod\ 2^n)$, не представима в виде (2), а следовательно и в поле вычетов $\mathbf{Z}/2^n$ по модулю 2^n, и в этом отношении не является линейной дихотомической последовательностью.

Отметим другие особенности, характерные для уравнения (3). Заметим, что при значении модификатора h отличным от нуля, эквивалентные ему представления (6) и (7), содержат линейную и нелинейную компоненты. В силу этого, данное уравнение проявляет двойственный характер, так называемый *линейчатый* характер, в соответствии с которым линейные изменения при одних значениях аргумента, сопровождаются ее скачкообразными (нелинейными) изменениями при других. При этом действие модификатора приводят лишь к изменению состояния битов $z_k \in z$ двоичной переменной z и не меняют корреляционных отношений между ними. Далее, в зависимости от состояния z переменной, множитель a и приращение c этого уравнения, вызывают быстрое и соответственно медленное перераспределение значений и однонаправленную от младших к старшим корреляцию битов этой переменной.

Таким образом, с алгебраической точки зрения, представленное уравнение характеризуется двойственными, так называемыми линейчатыми свойствами, а именно линейными свойствами при-

сущими полю $\mathbf{Z}/2^n$ с одной стороны и дискретными свойствами, присущими полю $\mathbf{Z}/2$ с другой.

В самом общем случае алгебраические структуры, обладающие в целом или части, линейными свойствами присущими полю $\mathbf{Z}/2^n$, с одной стороны и дискретных свойств, присущих полю $\mathbf{Z}/2$ с другой, а также линейных и дискретных свойств присущих полям $\mathbf{Z}/2^{n-1}$, $\mathbf{Z}/2^{n-2}$ и далее, будем именовать - *линейчатыми структурами*.

На основе этих структур разработан, так называемый *рандомизационный способ*, предназначенный для построения ординарных, одно и много параметрических, простых и сложных многомерных дихотомических генераторов с любым, не меньшим наперед заданного периодом повторения, обладающих относительно хорошими статистическими свойствами и высокой функциональной сложностью [1].

Дихотомические генераторы легко адаптируются под любые платформы вычислительных устройств, допускают организовать высокоэффективную последовательную и многоканальную параллельную, одно и много разрядную, включая и беспроцессорную обработку. Они способны образовывать структурные композиции любой сложности, могут быть функционально неразрешимыми по существу и при этом сохранять присущие составляющим их элементам бесповторные и другие дихотомические свойства.

Формирование функционально сложных дихотомических последовательностей и структурных композиций осуществляется на основе комплексирования дихотомических генераторов, а также на основе многомерных *Dh*-генераторов.

Простейший вариант комплексирования *Dh*-генераторов, может быть выражен линейчатой функцией, задаваемой в зависимости от дихотомических $\{z,x\}$ переменных:

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

где $\{h,g,r\}$ - двоичные n-разрядные вектора, $\{h,g\}$ - произвольные фиксированные модификаторы, а r - результирующая дихотомическая величина.

Дихотомический генератор может быть сложным, многомерным и задаваться системой уравнений определенной на множестве переменных. Один из вариантов реализации таких генераторов может быть представлен двумерным, так называемым дуальным *Dh*-генератором, задаваемым системой уравнений, для двух n-разрядных дихотомических переменных $\{u,v\}$, следующего вида:

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

при фиксированных нечетных $\{h_u,h_v\}$ и произвольных $\{g_u,g_v\}$ значениях модификаторов $\{h,g\}$.

Дихотомические генераторы за счет комплексирования и функциональной сложности, способны образовывать целостные структурные композиции любой сложности. На основе упомянутого выше рандомизационного способа, разработан аппарат синтеза таких сложных дихотомических систем [1].

Рассмотренные выше способы реализации дихотомических генераторов, работают достаточно хорошо при эффективной реализации арифметических действий и условии, что разрядность регистров используемых вычислительных устройств достаточна для выполнения машинных команд. Иначе требуется привлечение малоэффективной и сложной в исполнении арифметики больших чисел, что многократно сказывается на производительности и себестоимости подобных устройств.

Указанные недостатки можно устранить на основе векторных *(сегментарных)* генераторов. Для этого платформа генератора, составленная из n бит, разбивается $n = N \cdot m$ на N равных m-разрядных сегментов (подблоков), обычно по длине m совпадающих с разрядностью регистров используемых вычислительных устройств. Образованные таким образом сегменты связываются между собой, своим собственным, формируемым по результатам вычислений признаком результата, так что результирующая выходная последовательность, порождаемая генератором, есть дихотомическая последовательность, с общим периодом $T_n = 2^{N \cdot m}$.

Ниже представлена система уравнений варианта реализации N-сегментарного *Dh*-генератора, определенная на множестве фиксированных модификаторов $H = \{H_k\}$, $G = \{G_k\}$, $Q = \{Q_k\}$ и векторной $Z = \{z_k\}$ дихотомической переменной:

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

при $p_o = 1$ и четном H_1. Представленный алгоритм характеризуется смешанной алгебраической структурой в поле вычетов и отличается от известных методов способом задания признака результата p. Как показывает анализ, элементам дихотомической последовательности, формируемой на основании указанного уравнения, присущи сильно выраженные корреляционные свойства. Для преодоления этого недостатка, достаточно увеличить скорость распространения влияние младших битов на старшие биты этой последовательности. Например, это достигается на основе следующей системы уравнений реализации N-сегментарного *Dh*-генератора:

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

Рассмотренные дихотомические генераторы рассчитаны на последовательную обработку. Производительность *Dh*-генераторов может быть многократно увеличена за счет использования многоканальных генераторов. Многоканальная (многопроцессорная), параллельная обработка обеспечивается за счет *параметризации* генераторов.

В основе параметризации лежит идея разделения операции сложения на простые составные части, исполняемые по ходу итерации генераторов. Так, например, если признаки результата $\{p,q\}$, формируемые по ходу вычислений в (10) и (11) использовать не сразу, а на последующей итерации генератора, то такой генератор сможет работать как многоканальный генератор.

Вариант реализации N-канального однопараметрического *Dh*-генератора, от множества параметров $P = \{r_k\}$ и выходной дихотомической векторной переменной $R = \{r_k\}$, при фиксированном на каждой итерации нечетным $p|_{k=1} = p_o$, может быть представлен следующими уравнениями:

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

Среди особенностей поведения дихотомических генераторов параметрического типа, следует отметить наличие, обычно небольшого, переходного нестационарного участка τ, присущего широкому классу динамических систем, после которого указанные генераторы самостоятельно, феноменальным образом переходят в устойчивое состояние и далее в пределах периода $T_n = 2^{N \cdot m}$, ведут себя всюду как бесповторные генераторы. В зависимости от способа реализации генератора и числа входящих в его состав параметров p, обычно это *2-3*, длина переходного участка τ может достигать

величины $p{\cdot}n$. Этот недостаток не является препятствием к практическому использованию представленных генераторов, так как может быть легко устранен, либо в зависимости от максимально используемой длины статистической выборки L_S, в битах, принят равным $p{\cdot}log_2 L_S$ [2].

Все представленные выше варианты реализации дихотомических генераторов предусматривают наличие специализированного арифметического устройства или процессора, что существенно сказывается на конечной стоимости таких генераторов, а наличие операций сложения (вычитания), а тем более операции умножения - на общей производительности соответствующих устройств.

Указанных недостатков лишены параметрические генераторы ориентированные на простейшую двоичную, одно- и многоразрядных параллельную обработку. В основе такой обработки лежат идеи рекуррентной развертки операции сложения (вычитания) на конечное число составляющих ее элементарных двоичных операций, выполняемых последовательно по ходу итерации генераторов или других подобных им стохастических систем. В поле вычетов $\mathbf{Z}/2$, исходя из формулы (4) и операции дополнения до двух $-\beta = \overline{\beta} + 1$, можно получить следующие выражения для реализации таких аддитивных арифметических действий:

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

аппаратно элементарно реализуемых на основе полусумматоров соответствующего типа.

Рассмотрим оптимальные с точки зрения реализации, варианты построения параметрических дихотомических генераторов. Основное внимание уделим наиболее простым, аналитически неразрешимым *Dh*-генераторам, обладающих, при аппаратной реализации, предельно высокой производительностью соизмеримой со скоростью выполнения одной операции *XOR*, вне зависимости от числа бит n входящих в состав платформы таких генераторов.

Простейший *Dh*-генератор, задаваемый двухпараметрическим *{P,D}* рандомизационным оператором $R_C(H,P_{i-1},D_{i-1})$: $B_{i-1} \to \{B_i,P_i,D_i\}$, при $H \equiv 1 (mod\ 2)$ нечетном фиксированном значении модификатора H и выходом $r_i = B_{i-1} \oplus D_{i-1}$, может быть представлен следующей композицией операторов:

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

Генераторы данного типа характеризуются медленным изменением битов, характерным для ординарных счетчиков и именуется в дальнейшем *дихотомическими* или *Dh-счетчиками*.

Дихотомические переменные *{B,D}*, характеризующие внутреннее состояние генератора, могут быть выражены через известное выходное состояние генератора, определяемое дихотомической переменной r, в следующем виде:

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

Из выражений следует аналитическая неразрешимость уравнений генератора (14), т.к. на любой итерации, изменения внутреннего состояния генератора не могут быть однозначно выражены даже через все известные его внешние состояния. Иначе, при неизвестном и скрытом от внешнего доступа изменении переменных характеризующих внутреннее состояние параметрических генераторов, по всем известным внешним его состояниям невозможно аналитически вычислить одно из последующих и каждое из предшествующих значений их выходных переменных.

Для уменьшения существенно выраженной корреляции присущей дихотомическим счетчикам, необходимо осуществить распространение влияния младших битов на старшие, выполняемое последовательно по ходу итерации генератора.

Такие, так называемые *диссипативные Dh-генераторы первого рода*, могут быть заданы самосинхронизирующимся двухпараметрическим $\{P,D\}$ рандомизационным оператором $R_I(P_{i-1},D_{i-1})$: $B_{i-1} \to \{B_i,P_i,D_i\}$, составленным из операторов:

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

Так же, как и в предыдущем случае, выход *Dh*-генератора может быть задан аналогичным уравнением $r_i = B_{i-1} \oplus D_{i-1}$. Дихотомические переменные $\{B,D,P\}$, характеризующие внутреннее состояние этого генератора, могут быть выражены через известное его выходное r_i состояние, в следующем виде:

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

Из этих выражений следует аналитическая неразрешимость уравнений (15).

Не смотря на существенно выраженные лавинные свойства присущие рассмотренным выше диссипативным генераторам за счет распространения влияния младших битов на старшие, данным генераторам присущи достаточно сильно выраженные линейные свойства. Придание дихотомическим последовательностям, формируемым на основе *Dh*-генераторов существенно выраженных нелинейных свойств, может быть осуществлено на основе катенации (связывания) младших битов со старшими, осуществляемое последовательно по ходу итерации этих генераторов. Диссипативные генераторы с существенно выраженными нелинейными свойствами, будем называть диссипативными *Dh*-генераторами *второго рода*.

Dh-генераторами второго рода с выходом $r_i = B_{i-1} \oplus D_{i-1}$, могут быть заданы самосинхронизирующимся 3-х параметрическим $\{P,D,Q\}$ рандомизационным оператором $R_{II}(P_{i-1},D_{i-1},Q_{i-1})$: $B_{i-1} \to \{B_i,P_i,D_i,Q_i\}$, составленным из операторов:

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

Дихотомические переменные $\{B,D,P,Q\}$, характеризующие внутреннее состояние этого генератора, могут быть выражены через известное его выходное r_i состояние, в следующем виде:

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

Из этих выражений следует аналитическая неразрешимость уравнений (16).

Параметрические генераторы могут быть сложными, многомерным и задаваться системой уравнений определенной на множестве переменных. Один из вариант реализации таких генераторов может быть представлен двумерным, 4-х параметрическим $\{P_u,D_u,P_v,D_v\}$ самосинхронизирующимся дуальным *Dh*-генератором с множеством выходов $r_{ui} = B_{u(i-1)} \oplus D_{u(i-1)}$ и $r_{vi} = B_{v(i-1)} \oplus D_{v(i-1)}$, задаваемым системой уравнений, составленной из рандомизационных операторов

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

представленных аналитически неразрешимыми композициями операторов, вида:

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

Параметрические *Dh*-генераторы могут задаваться, не только представленной выше относительно простой, но и более сложной системой уравнений множества, обладающих дихотомическими свойствами переменных. На основе разработанного формального аппарата синтеза таких систем [1], возможно создание различных по назначению стохастических и криптографических распределенных систем, любой наперед заданной функциональной и структурной сложности.

Рассмотренные выше теоретические и технические аспекты реализации дихотомических генераторов, показывают возможность достижения аналитическая неразрешимости формируемых на их основе дихотомических последовательностей. Вместе с тем, аналитическая неразрешимость, достигаемая на основе многомерности и параметризации *Dh*-генераторов необходима, но недостаточна для построения сильных в криптографическом отношении устройств и систем. Исходя из общих требований предъявляемым к генераторам случайных чисел [2, 5], в качестве достаточных условий достижения криптографической надежности *Dh*-генераторов, являются статистические свойства формируемых на их основе последовательностей, с законом распределения близким к *идеальному* равномерному.

Следуя этим условиям, рассмотрим наиболее характерные статистические особенности дихотомических последовательностей и величин. Для начала, введем понятие слайка (среза) двоичной последовательности $Z = \{z_i: i = \overline{1,L}\}$ из L неотрицательных целых чисел z_i, составленных из n значащих бит $b_{si} \in z_i$ $(s = \overline{1,n})$.

Слайком s, называется двоичная последовательность $Z_s = \{b_{si}: i = \overline{1,L}\}$, составленная из всех $b_{si} \in \{0,1\}$ битов исходной для нее двоичной последовательности Z. Слайк $\Delta Z_s = \{b_{s(i-1)} \oplus b_{si}\}$, при $b_{so} = 0$, образованный по слайку Z_s, будем называть *разностным слайком* s.

В силу существенно выраженного, детерминированного поведения младших битов дихотомических величин и комплементации порождаемых ими дихотомических классов, битам входящих в состав младших слайков реализаций этих величин, присуща довольно сильная статистическая зависимость. В зависимости от скорости распространения влияния младших битов на старшие и их катенации предусмотренных уравнениями генерации дихотомических последовательностей, корреляция между битами слайка может сохраняться, либо медленно или быстро убывать от слайка к слайку.

В качестве первого примера, рассмотрим вариант реализации N-канального двухпараметрического $\{P,D\}$ диссипативного дихотомического генератора первого рода, иначе $\mathbf{\Delta}_N$-генератора, задаваемого рандомизационным оператором $R_\Delta(P_{i-1},D_{i-1}): B_{i-1} \to \{B_i,P_i,D_i\}$, составленным из операторов:

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

$$D_{ki} = (2 \cdot (B_{k(i-1)} \wedge P_{k(i-1)})) \vee Q \bmod 2^m, \quad Q = Q_{k(i-1)}, \quad Q_{ki} = (B_{k(i-1)} \wedge P_{k(i-1)}) / 2^{m-1},$$

с выходом $r_{ki} = B_{k(i-1)} \oplus D_{k(i-1)}$, при $Q|_{k=1} = 0$. Из аналитической неразрешимости уравнений (15), следует и аналитическая неразрешимость уравнений (18).

Статистический анализ слайков, проведенный на основе пакета статистических тестов DIEHARD [6], показывает, при любых m, наличие существенной корреляции между битами младших канальных слайков $s = (k-1) \cdot m + 1$. При $m = 32$ отмечается несущественная корреляция между битами старших канальных слайков $s = k \cdot m - 1$. Существенная корреляция между битами слайков обусловлена малой разрядностью регистров с одной стороны и отсутствием механизмов распространения влияния битов между блоками, с другой.

Высокие статистические характеристики могут быть достигнуты на основе генераторов, предусматривающих распространение влияния между битами каналов. В качестве примера такого генератора, рассмотрим вариант реализации N-канального 3-х параметрического $\{P,D,G\}$ диссипативного дихотомического генератора первого рода, иначе ∇_N -генератора, задаваемого рандомизационным оператором $R_\Delta(P_{i-1},D_{i-1},G_{i-1}): B_{i-1} \to \{B_i,P_i,D_i,G_i\}$, составленным из операторов:

$$B_{ki} = B_{k(i-1)} \oplus P_{k(i-1)}, \quad P_{ki} = (4 \cdot B_{k(i-1)}) \oplus \bar{D}_{k(i-1)} \bmod 2^m \quad (k = \overline{1,N}), \tag{19}$$

$$D_{ki} = G \oplus G_{k(i-1)}, \quad G_{ki} = (2 \cdot (B_{k(i-1)} \wedge P_{k(i-1)})) \vee Q \bmod 2^m,$$

$$G = \mathbf{rot}_L(B_{k(i-1)},S_G), \quad Q = Q_{k(i-1)}, \quad Q_{ki} = (B_{k(i-1)} \wedge P_{k(i-1)})/2^{m-1},$$

с выходом $r_{ki} = B_{k(i-1)} \oplus D_{k(i-1)}$, при $G|_{k=1} = G_0$ и $Q|_{k=1} = G_0 \bmod 2$. Здесь $\mathbf{rot}_L$, это операция циклического сдвига $\mathbf{rot}_L(B_{k(i-1)},S_G)$ двоичной m-битовой переменной B_k влево, на число S_G бит, равное ближайшему простому к $m/3$, не кратному m. Аналогично ранее рассмотренным случаям, из аналитической неразрешимости уравнений (18), следует и аналитическая неразрешимость уравнений (19).

По результатам статистического анализа [6], для всех m, заметной корреляции битов слайков и образованных по ним разностных слайков, начиная с 27, не выявлено ни при каких начальных условиях.

При тестировании дихотомических последовательностей ∇_N -генераторов, отмечаются следующие результаты. При небольшой длине $n = N \cdot m$ платформы генератора, наблюдается существенная корреляция между элементами формируемых ∇_N -генератором дихотомических последовательностей. При средней длине платформы в 256-512 бит, статистика нестабильна. Корреляция медленно убывает с увеличением n. Статистика стабильна и удовлетворительна, при $24 \times 32 = 768$ бит $(N=24, m=32)$, при $64 \times 16 = 964$ бит и при $162 \times 8 = 1296$ бит в платформе и выше.

Ситуация кардинальным образом меняется, при усечении 32-х младших коррелированных слайков. Для усеченных таким образом $\nabla_{(N\ -32/\ m)}$ -генераторов, статистика удовлетворительна, при $5 \times 32 = 160\ (160 - 32 = 128)$ бит $(N=5, m=32)$, при $6 \times 16 = 96\ (48)$ бит и при $9 \times 8 = 72\ (40)$ бит в платформе и выше, где в скобках указана длина выходного блока генератора.

Отмечается улучшение статистических показателей у последовательностей разностного типа $\Delta r_{ki} = r_{k\{i-1)} \oplus r_{ki}$, при $r_{k0} = 0$, образованных из исходных к ним усеченных D-последовательностей.

В отличие от неусеченных дихотомических последовательностей, усеченные D-последовательности, в пределах периода повторения 2^n, уже не являются бесповторными. Средние оценки числа повторений для представленного выше ∇_N -генератора, проведенные по 500 статистическим выборкам различной длины, приведены в ниже следующей таблице.

Testing of repetition number

Statistical sample	**65536**	**32768**	**16384**	**8192**	**4096**	**2048**	**1024**	**512**	**256**
Truncation ∇_N	**non-truncated *D*-sequence is unrepeatable**								
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

Представленные в таблице оценки не зависят от длины используемых регистров и быстро сходятся к сюръективным, так называемым *генераторам гаммы* типа RC4 и блочным шифрам, функционирующим в режиме обратной связи по выходу.

Проведенный статистический анализ будет не полным, без оценки достижимости статистической неопределенности старших битов дихотомических *n*-битовых величин, формируемых *Dh*-генераторами. В качестве этой оценки примем показатель $0 \le \rho \le n$, соотносящийся с 2^{ρ}, характеризующий в среднем глубину возможного перебора битов упомянутой дихотомической величины, необходимую для предсказания каждого из очередных элементов реализации этой величины.

Вычисление этой ρ оценки осуществляется по всем Z_s $(s = \overline{1,n})$ слайкам, входящих в состав статистической выборки формируемой *Dh*-генератором, в следующей последовательности.

По каждому из слайков, длиной L_S бит, рассчитывается число повторений R_{1L} 1-серий длиной $L = \{1,2,\ldots L_S\}$, составленных из одних единиц и число повторений R_{0L} 0-серий длиной L, составленных из одних нулей. Имеет место тождество:

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

Из него, следуя второму постулату Голомба [7], вычислим эвристические оценки P_{BL} недетерминированности битов серий

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

где $B = \{1,0\}$ - тип серии, $Q_{BL} = R_{BL} / L_S$, T - период повторения *s*-слайка.

По результатам расчета оценок P_{BL}, может быть вычислен показатель недетерминированности ρ_s соответствующего *s*-слайка

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

Исходя из этого, показатели ρ глубины полного перебора битов дихотомической величины, связанной с выходом *Dh*-генератора, на множестве из *E* статистических выборок, определяется по формуле:

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

при суммировании в направлении от младших значащих битов к старшим и при всех $\rho_{s0} = 1$.

Ниже приведена таблица расчетов показателей недетерминированности ρ_s для 16-ти (32-х) слайков и показателей глубины полного перебора битов ρ_{150}, рассчитанным по 150-ти статистическим выборкам, составленных из 131970 неотрицательных 32-х разрядных двоичных чисел, для генератора случайных чисел RC4 и многоканального 8-ми разрядного ∇_N –генератора, при различном числе усекаемых *(TRN)* его младших значащих бит.

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**

Из результатов тестирования видно, что статистические свойства слайков указанного ∇_N – генератора приближаются к статистическим свойствам слайков генератора RC4. При этом, начиная где-то с 224 бита, наблюдается выравнивание их свойств. В общем случае отмечается, что усеченные на 288 бит 40-канальные 8-ми разрядные *($\rho_{150} = 30.787265$)* и усеченные на 164 бита 13-канальные 16-ти разрядные *($\rho_{150} = 30.786975$)*, а также усеченные на 90 бит 4-канальные 32-х разрядные *($\rho_{150} = 30.787333$)* и выше ∇_N –генераторы, по статистическим свойствам всех выходных его битов, практически не отличаются *($\rho_{150} = 30.787472$)* от упомянутого, выбранного в качестве эталонного, RC4 генератора.

Таким образом, можно сделать вывод, что старшие значащие биты рассмотренных ∇_N –генераторов по статистическим свойствам не уступают двоичным последовательностям формируемым на основе наиболее продвинутым и исследованным генераторам случайных чисел. Тем самым можно утверждать о возможности достижения статистической неопределенности формируемых на основе дихотомических генераторов последовательностей случайных чисел, практически не отличающейся от идеальной.

В итоге, принимая к сведению

- доказанную выше аналитическую неразрешимость уравнений функционирования параметрических и многомерных *Dh*-генераторов,

- проведенный статистический анализ [6], подтверждающий распределение битов старших слайков близкое к идеальному равномерному (включая и биты разностных слайков),

- представленный анализ статистических свойств [6] и распределения числа повторений усеченных *Dh*-генераторов, а также их анализ на основе уравнения (20), показывающие возможность достижения статистической неопределенности битов близкой к идеальной,

позволяет говорить о возможности достижения функциональной неразрешимости по существу со стороны старших значащих бит формируемых на основе указанных *Dh*-генераторов случайных последовательностей. Причем, как показывает анализ, независимо от начальных условий генерации этих последовательностей.

В самом общем случае, на основе дихотомических генераторов обладающих функциональной неразрешимостью по существу, можно достаточно просто построить криптографически сильные бесповторные генераторы ключевого потока и равноповторные генераторы гаммы. Это может быть осуществлено путем биективных или сюръективных преобразований дихотомических последовательностей, предусматривающих распространение влияния старших битов на младшие, младших битов на старшие и катенации битов, а также за счет эффективных приемов перемешивания преобразуемых битов. На основе этих преобразований достигаются более высокие статистические показатели формируемых последовательностей и обеспечивается надежное сокрытие дихотомических свойств, присущих исходным для них *D*-последовательностям.

Как правило, практический результат оптимален, если задачи формирования дихотомических последовательностей и их преобразования взаимно обусловлены и супераддитивны, однозначно необратимы, почти всюду дополняют друг друга и гармонично сочетаются между собой. Решение этих задач это тема следующего раздела - раздела стохастической криптографии.

Выводы:

1. Дихотомические генераторы, по своим статистическим свойствам, функциональной сложности и производительности, превосходят наиболее распространенные, функционирующие на основе регистров сдвига с линейной обратной связью (LFSR) линейные рекурентные генераторы. Так, при аппаратной реализации скорость функционирования таких генераторов, может быть соизмерима со скоростью выполнения одной операции *XOR*, вне зависимости от длины платформы генератора.

2. Схемы реализации дихотомических генераторов отличаются простой исполнения, допускают параллельную одно и много разрядную, включая беспроцессорную аппаратную обработку на любых платформах вычислительных устройств, требуют небольшого объема памяти и рассчитаны на использование ключей переменной длины.

3. Схемы реализации прозрачны для анализа, алгебраически сложны и замкнуты, носят высокодинамичный параметрический, скрытый от внешней среды простой или сложный, многомерный, существенно выраженный связанный и нелинейный характер. В итоге, могут обладать достаточной для практических приложений статистической и функциональной надежностью. В программном исполнении по всем показателям не уступают наиболее совершенным образцам, а при аппаратной реализации отличаются высокой производительностью и малой себестоимостью.

4. Дихотомические генераторы могут иметь любой, не меньший наперед заданного период повторения, способны образовывать структурные композиции любой сложности, могут быть функционально неразрешимыми по существу со стороны старших значащих бит формируемых ими последовательностей и при этом сохранять присущие составляющим их элементам бесповторные свойства.

5. Указанные свойства дихотомических последовательностей позволяют, используя простые и прозрачные для анализа способы, достаточно эффективно и просто получить статистически и функционально надежные для практических приложений бесповторные и равноповторные последовательности равномерно распределенных чисел.

6. Дихотомические генераторы и методы их построения закладывают основу стохастической криптографии, предназначенной для построения одно и много раундовых параметрических и нелинейных двоичных стохастических преобразователей, односторонних функции и операторов. В рамках этого направления разработаны бесповторные генераторы ключевого потока, равноповторные генераторы гаммы, нелинейные сумматоры и интеграторы, хеш-функции различного назначения и симметричный итерационный, основанный на специальных управляемых операциях блочный шифр RACH с переменным числом раундов.

7. Дихотомические генераторы закладывают основу сетевой криптографии. Последнюю составляют протоколы, инструментальные средства и технологии построения распределенных многомерных, параметрических, целостных, структурно сложных дихотомических генераторов, криптографических средств и систем безопасности нового поколения, ориентированных на сетевые решения любой сложности, сверхскоростную и высоконадежную обработку

8. Дихотомические генераторы и методы их построения обеспечивают высокий уровень унификации и стандартизации, за счет универсального и однородного характера используемых криптографических модулей и компонент.

9. Представленные технологии сохраняют преемственность и носят не проходящий по времени характер, за счет фундаментального характера теоретической базы и ее концептуальной связи с процессами и явлениям присущими сложным динамическим системам и реальной природе. Что под-

тверждается исследованиями поведения построенных на их основе стохастических устройств и систем, наличием у них особых дихотомических, линейчатых и двойственных свойств, аттракторов и переходных процессов после которых они самостоятельно, феноменальным образом приходят в устойчивое состояние. Отмечаются удивительные аналогии с процессами протекающими в микромире.

10. Многомерный, параметрический и обусловленный ими существенно выраженный нелинейный характер поведения дихотомических генераторов и подобным им стохастических устройств и систем, а также проявляемые ими свойства, позволяют говорить об опережающем характере физики вычислений. Что особенно актуально в преддверии революции в области нанотехнологий и квантовой обработки.

Ключевые слова: Динамическая система. Аттрактор. Функциональная неразрешимость. Хаос. Стохастическая система. Симметричная криптография. Сетевая криптография. Генератор случайных чисел. Дихотомический порядок. Дихотомическая последовательность. Дихотомический генератор. Рандомизационный способ. Рандомизационный оператор. Рандомизационная система.

ЛИТЕРАТУРА

1. И.А. Кулаков, “Способ придания реальному объекту рандомизационных свойств и рандомизационная система”, Заявка на международный патент.
2. И.А. Кулаков, Дихотомические последовательности и их свойства, Рукопись статьи по материалам доклада на 3-ей Центрально-европейской конференции в Братиславе, TATRACRYPT 2003, Словакия, 28 июня 2003.
3. D. Knuth, The Art of Computer Programming, Volume.2, Seminumerical Algorithms, 2nd edition Addison-Wesley, 1981.
4. R. Lidl and 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, Пакет статистических тестов DIEHARD, 1997, geo@stat.fsu.edu.
7. S.W. Golomb, Shift Register Sequences, San Francisco: Holden-Day, 1967. (Reprinted by Aegean Park Press, 1982.)