Стохастические системы и криптография*

Кулаков Игорь Анатольевич, www.random-art.ru

Излагаются математические основы стохастических систем и ее приложений – стохастической криптографии. Даются понятия регулярной и нерегулярной динамики, неполной арифметики и линейных стохастических систем. Особое внимание уделяется дихотомическим последовательностям и генераторам, в кольце вычетов неполной арифметики по модулю 2^n, составляющих ядро линейных стохастических систем. Указываются их преимущества и недостатки. Доказывается предельная криптографическая стойкость дихотомических последовательностей, показывается способ и дается оценка объема статистической выборки, необходимой для их точного воспроизведения. Приводятся примеры построения типичных, открытых для общего обсуждения генераторов гаммы и односторонних аутентификаторов.

1. Общие положения

Невозможно представить себе реальную действительность в условиях строго обусловленного, детерминированного характера происходящих в ней процессов и исчерпывающего охвата человеком всей поступающей ему информации. В зависимости от субъективного или объективного характера неопределенности, обусловленной сложностью процессов и множеством ограничений накладываемых на состав и точность доступной о них информации, законы функционирования реальных объектов можно подразделить на строго определенные – ***детерминированные*** и ***стохастические***, а именно, случайные по существу – ***недетерминированные*** и случайные по природе – ***статистические законы***.

Формально, стохастический закон может быть задан на *вероятностном пространстве* $\Pi_\Omega = \{\Omega,A,P\}$, состоящем из пространства элементарных событий Ω, с полем событий A и законом распределения вероятностей P, если в качестве меры неопределенности принять вероятность свершения связанного с этой неопределенностью события [1].

Реальные объекты, поведение которых тем или иным образом подчиняется стохастическому закону, иными словами характеризуемые заметно выраженным недетерминированным, хаотическим поведением, будем называть *стохастическими объектами*. Принимая в абсолюте субъективный характер отражения случайности, субъект, действующий в условиях неполной информации и реальный объект, образуют наделенное двойственной природой целое, именуемое ***стохастической системой***. Стохастические системы сложны, высоко подвижны и динамичны. Все это вместе взятое, усиленное неопределенностью возникающей под действием внешних факторов и, как правило, в высшей мере сложным взаимодействием ее элементов, делает этот объект чрезвычайно трудным для исследований.

Не смотря на достижения и предпринимаемые усилия в этой области (нелинейная динамика, синергетика, детерминированный хаос, бинарный хаос), теория стохастических систем еще очень молода и требует своего совершенства [1,2,3].

1.1. Регулярная и нерегулярная динамика поведения систем

Трудности построения строгой теории стохастических систем кроятся не только в объективно высокой сложности этих систем. Как это не парадоксально на рубеже XXI века, оказалось, что трудности построения строгой теории также скрыты в неточности исходных посылок и в несовершенстве привлекаемого математического аппарата. Источник противоречий скрыт в операции сложения. Опираясь на физические законы, **во-первых**, из-за потенциально конечной скорости взаимодействий, операция сложения, в принципе, не может реализоваться в природе мгновенно. **Во вторых**, формально, операция сложения допускает разложение в последовательность простейших, не выводимых друг из друга параллельно исполняемых действий. Вообще существование такой простейшей операции, факт известный [8], но не получивший своего достаточного осмысления.

Следуя логике представленных фактов и предположений об исчерпывающей простоте и универсальности устройства природы, разумно положить эту простейшую операцию в основу теории построения реальных систем. Если принять это положение, то из него неминуемо сле-

дует, что операция сложения и производные от нее арифметические операции реализуются не мгновенно, а за конечное время, **в динамике развития реальных систем** и сопровождаются при этом переходными (нелинейными) процессами. По завершении этих процессов, система достигает своего равновесия и развивается далее по законам, характерным для известных в физике, так называемых регулярных систем. Условимся такое движение называть ***регулярным***.

В общем случае совершенно неочевидно и необязательно, что система будет развиваться указанным выше образом. Иное движение, по сути, означает **иную динамику и арифметику**, образно говоря, поведения системы. Такое движение будем называть ***нерегулярным***, а сами системы – *нерегулярными*. Безусловно, можно показать, что такое нерегулярное движение можно представить формально – математическим рядом, с использованием обычных арифметических действий. Но такое описание становится очень громоздким, сложно интерпретируемым и мало пригодным на практике [4].

Уточнению и развитию этих положений будет уделено ниже особое внимание.

1.2. Порядок и хаос

Траектория движения нерегулярных систем, начиная от некоторого своего начального состояния, до некоторого своего фиксированного состояния, может отличаться в малых деталях или существенно от траектории движения подобных им регулярных систем. Такие отличия проявляются на фоне регулярных систем и в детерминированных условиях воспринимаются как *неупорядоченное*, в условиях неопределенности, как *беспорядочное* изменение состояния. Нерегулярные системы, изменение состояния которых тем или иным образом подчиняется стохастическому закону, по определению, есть стохастические системы. Стохастические системы, изменение состояния которых подчиняется равномерному закону распределения случайных величин, называются ***хаотическими системами***. С общесистемных позиций хаотические системы характеризуются максимальной энтропией, достигаемой с одной стороны относительной свободой поведения ее элементов и зависимостью каждого элемента от всех других ее элементов и в силу этого в высшей степени сложно устроены. В отличие от существующих предубеждений, здесь нет места для интуитивных и других околонаучных подходов.

Для хаотических систем характерно, что даже незначительные изменения в начальных условиях, могут очень быстро привести к существенному изменению состояния системы. Стохастические системы подобного рода, в которых изменения в начальных условиях усиливаются экспоненциально во времени, представляют теоретический и практический интерес для криптографии. Действительно, если сторонний наблюдатель не сможет точно задать начальные условия, ошибка его предсказания быстро вырастет до неприемлемого уровня [5]. Вместе с тем, это положение необходимо, но далеко недостаточно для построения практически значимых криптографических систем. Сюда относятся проверки на соответствие равномерному закону распределения, а также оценки сложности формального описания и моделирование адекватного поведения этих систем. Здесь также предъявляются строгие требования к простое и прозрачности аппаратной и программной реализации, производительности алгоритмов и многое остальное. В криптологии, как ни в какой другой науке накоплен огромный практический и теоретический опыт по созданию и исследованию подобных сложных систем [6].

Подводя первые итоги, можно спорить о правомерности принятых положений. Лучший критерий – практика, а в ней, одна из передовых и востребованных областей – криптография, направленная на становление нового направления – **стохастической криптографии** и создание на ее основе высокоэффективных криптографических систем.

1.3. Элементы системного анализа

Здесь и далее, при описании стохастических систем, будем следовать известным положениям системного анализа. Система вообще и стохастическая система в частности, может быть представлена формальной моделью. Формальная модель, адекватно (т.е. с точностью до изоморфизма) отражающая закон функционирования системы, называется *функциональной моделью*. Функциональная модель, наделенная алгебраической структурой, называется *математической моделью*.

Модель и система состоят из элементов. Элементы взаимосвязаны между собой, в соответствии с отношениями, установленными между ними. Состав элементов модели и системы, а также отношения между ними могут меняться по установленным правилам посредством выполнения последовательности действий и эволюции системы. В математических моделях оперируют множествами и величинами, элементы математической модели задаются отображениями и их производными – **операторами** (функциями, преобразованиями, уравнениями), отношения – **операциями**, а правила вывода – **предикатами**.

Исходя из предполагаемого выше изоморфизма модели и системы, носители информации связанные с величинами, множество элементов (операторов) модели и множество элементов системы и отношения между ними, могут быть отождествлены. Объект, полученный в результате такого соответствия, с точностью до несущественных ошибок реализации эквивалентный системе, называют *предметной моделью*, а его элементы – операторами системы или просто операторами, если из контекста понятно о каких операторах идет речь. Операторы системы, будучи исполнительными элементами, могут быть представлены в виде отдельных устройств и систем, либо в виде элементов устройств и систем, инструкций, программ.

Очевидно, предметная модель функционирует в соответствии со своей формальной моделью и может выступать в качестве самостоятельной системы, либо в качестве подсистемы или элемента более сложных систем.

Представленные здесь общие положения будут детализироваться в достаточной мере, по ходу изложения материала. Детальное описание и строгие определения можно будет найти в [4].

1.4. Дискретные системы и способы их задания

Системы и стохастические системы в частности, можно подразделить на системы с ***дискретным*** и системы с ***непрерывным*** **временем**. Принимая общую методологию развития естествознания, от простого к сложному, от дискретного к непрерывному, не вдаваясь в обобщения, ограничимся рассмотрением вопросов, связанных с поведением систем, состоящих из конечного числа неделимых элементов, функционирующих в дискретном времени, иначе – **дискретных систем**.

Дискретная система может быть задана **конечным автоматом**, преобразующим дискретную информацию. Конечный автомат - это система (A,S,B,φ,ψ), где A, S, B – конечные, как правило непустые алфавиты, называемые, соответственно, входным алфавитом, множеством состояний и выходным алфавитом; $A_i \in A$, $B_i \in B$, $S_i \in S$ – кортежи и состояние автомата на момент времени i; $S_0 \in S$ –начальное состояние автомата;

φ – функция переходов, отображающая φ: $S_{i-1} \times A_i \rightarrow S_i$ множество $S_{i-1} \times A_i$ в S_i;

ψ – функция выходов, отображающая ψ: $S_{i-1} \times A_i \rightarrow B_i$ множество $S_{i-1} \times A_i$ в B_i.

Конечные автоматы данного типа, относятся к автоматам Мили. Конечные автоматы, с функцией выходов ψ: $S_{i-1} \rightarrow B_i$, не зависящей явно от букв входного алфавита, называется автоматом Мура [1].

Если существуют такие алфавиты, что

$$A = A_{(1)} \times A_{(2)} \ldots \times A_{(\mathrm{m})}, \quad S = S_{(1)} \times S_{(2)} \ldots \times S_{(\mathrm{k})}, \quad B = B_{(1)} \times B_{(2)} \ldots \times B_{(\mathrm{n})},$$

то говорят, что автомат имеет m входов, n выходов и k измерений.

Согласно положениям системного анализа, дискретная система может быть описана **функционально**. При функциональном описании оперируют операторами и преобразуемыми величинами.

Оператором называется отображение f: $\Gamma \rightarrow \Phi$ с областью определения Γ и областью возможных значений Φ, устанавливающее правило действий $f(P)$: $Z \rightarrow S$ от множества параметров P, согласно с которым некоторому значению $z \in \Gamma$ исходной величины Z ставится в соответствие по закону $f(P)$ вполне определенное значение $s \in \Phi$ результирующей величины S.

Оператор называется биекцией (сюръекцией, инъекцией) или биективным (сюръективным, инъективным) оператором в зависимости от свойств связанного с ним отображения [1].

Операторы модели (системы) образуют множество операторов модели (системы), являются ее исполнительными элементами и отражают закон функционирования модели (системы) на множестве связанных с ней величин. Путем композиции и декомпозиции различных операторов формируются более продуктивные и содержательные операторы [4].

В терминах функционального подхода, дискретная система – это система $(X,Z,Y, \vartheta(P_\varphi), \Psi(P_\psi))$, определенная на множестве $P = P_\varphi, \cup P_\psi$ параметров P, множестве m входных $X = \{X_{(m)}\}$ и множестве n выходных $Y = \{Y_{(n)}\}$ величин, множестве переменных $Z = \{Z_{(k)}\}$ характеризующих изменение ее внутреннего состояния, функционирующая в дискретном времени i, согласно с правилами, устанавливаемыми

- оператором перехода $\vartheta(P_\varphi)$: $\{X_i, Z_{i-1}\} \to Z_i$ в очередное i состояние,
- оператором выхода: 1. $\Psi(P_\psi)$: $\{X_i, Z_{i-1}\} \to Y_i$, либо
  2. $\Psi(P_\psi)$: $Z_{i-1} \to Y_i$.

В первом случае, оператор выхода действует над входами, в некоторой, большей или меньше мере изменяя присущие входным величинам свойства и в силу этого именуется *метрическим операторами*. В свою очередь, системы с такими выходами именуются *метрическими системами*.

Во втором случае, оператор выхода отражает особенности входов и текущее состояние и поэтому именуется *модальным оператором*, а системы – *модальными системами*.

По сравнению с языком автоматов, функциональный язык более универсален, содержателен и предметен. В связи с этими преимуществами, далее при изложении материала будем придерживаться функционального подхода.

2. Двоичные величины и операции над ними

Зададим двоичный вектор

$$B^n = B_1 B_2 \ldots B_i \ldots B_n,$$

составленный из последовательности n бит B_i $(i = \overline{1,n})$. Двоичному вектору B^n может быть поставлена в однозначное соответствие постоянная или переменная n-битовая двоичная величина

$$b^n = b_n b_{n-1} \ldots b_k \ldots b_1,$$

каждый бит $k = n - i + 1$ которой, способен принимать одно из значений $b_k \in \{0,1\}$ $(k = \overline{1,n})$, а сама величина b^n, чаще просто b, принадлежит целочисленному интервалу $b \in [0, 2^n - 1]$.

Над двоичными величинами осуществимы классические арифметические операции $\{\pm, \cdot\}$ сложения, вычитания и умножения по модулю 2^n, операции деления и умножения на 2^k, означающих СДВИГ вправо $\succ$ в сторону младших двоичных разрядов и, соответственно, СДВИГ влево $\prec$ в сторону старших двоичных разрядов) на k бит, побитовые операции $\{\bar{}, \&, |, \oplus\}$ инверсия битов, *И*, *ИЛИ* и сложение по модулю *2*.

Наравне с обозначениями операций $\{\bar{}, \&, |\}$, также используют тождественные им обозначения $\{\neg, \wedge, \vee\}$. На практике, побитовой операции $\oplus$ сложения по модулю *2* соответствует равнозначная ей операция *XOR* - *исключающее ИЛИ*. Там, где это необходимо, используется частный случай операции $\oplus$, а именно операция инверсии битов

$$\bar{z} = (2^n - 1) \oplus z$$

двоичной величины z.

Условные обозначения двоичных операций

$\neg$, $\bar{}$ – побитовое отрицание НЕ (инверсия битов),
| , $\vee$ – побитовая операция ИЛИ,
& , $\wedge$ – побитовая операция И,
$\oplus$ – побитовая операция XOR (сложение по модулю 2),
$\lhd$ k – сдвиг влево, на **k** бит (умножение на $2^{\mathbf{k}}$),
$\rhd$ k – сдвиг вправо, на **k** бит (целочисленное деление на $2^{\mathbf{k}}$),
$\mathbf{mod}_n(x)$ – выделение **n** значащих бит **x** & $(2^{\mathbf{n}} - 1)$, из двоичного числа **x**.
rotR(x,k), **rotL**(x,k) – циклический сдвиг двоичного числа **x**, вправо и влево на **k** бит.

Принимается, что величина, заданная со знаком минус - *отрицательно определена*, иначе величина *положительно определена*. Положительно и отрицательно определенные величины связаны операцией умножения на константу (2^n-1) или эквивалентной ей, так называемой операцией дополнения до двух. А именно:

$$. - z = ((2^n - 1) \cdot z) \bmod 2^n, \qquad -z = (\bar{z} + 1) \bmod 2^n.$$

В целях более простого представления формул, далее рассматриваются положительно определенные величины. Отрицательно определенные величины оговариваются особо. Кроме этого, далее везде подразумевается, что двоичная величина ограничена множеством своих значащих бит и подвергается усечению со стороны ее старших бит. В выражениях и аналогичных случаях, когда значения двоичных величин подвергаются естественному усечению со стороны старших значащих бит, знак операции ***mod*** можно опускать.

В двоичной арифметике для операции сложения двух n-битовых двоичных величин, справедливы следующие эквивалентные соотношения:

$$c = a + b = 2\cdot(a \,\&\, b) + (a \oplus b) \quad \text{или} \quad c = a + b = 2\cdot(a \mid b) - (a \oplus b). \qquad (1)$$

Первоначально положим $c_0 = a$ и $p_0 = b$. Из первого соотношения, следует, что

$$c_1 = c_0 \oplus p_0, \qquad p_1 = (c_0 \,\&\, p_0) \lhd 1, \qquad \text{при этом} \quad c_1 + p_1 \bmod 2^n = a + b,$$

так как двоичная переменная p, содержит все признаки переноса, формируемые по всем n битам, одновременно.
По индукции, действуя далее, на втором и каждом последующем i-ом шаге, получим

$$c_2 = c_1 \oplus p_1, \qquad p_2 = (c_1 \,\&\, p_1) \lhd 1, \qquad \text{при этом} \quad c_2 + p_2 \bmod 2^n = a + b;$$

. . . . . .

$$c_i = c_{i-1} \oplus p_{i-1}, \qquad p_i = (c_{i-1} \,\&\, p_{i-1}) \lhd 1, \qquad \text{при этом} \quad c_i + p_i \bmod 2^n = a + b.$$

При $p_i \bmod 2^n = 0 \;\; (i \le n)$, когда все признаки переноса нулевые, имеем, что $c_i + 0 = a + b$, т. е. двоичная переменная c, становится равной сумме двух, связанных двоичной операцией сложения величин.

Таким образом, подтверждается высказанное ранее в разделе 1.1 положение о существовании формального разложения операции сложения $c = a + b$ в последовательность простейших, не выводимых друг из друга параллельно исполняемых действий, осуществляемое согласно рекурсивному выражению:

$$c_i = c_{i-1} \oplus p_{i-1}, \qquad p_i = (c_{i-1} \,\&\, p_{i-1}) \lhd 1 \qquad (p_{i-1} \neq 0), \qquad (2)$$

при начальных условиях $c_0 = a$ и $p_0 = b$.

На языке псевдо Си, алгоритм реализации операции сложения, примет вид

```
for( p = b, c = a; p; p = (p & z) <1 ) {
   z = c; c = c ⊕ p;
}
```

Аналогично, через двойное отрицание $d = \overline{\overline{a} + b}$, согласно выражению:

$$d_i = d_{i-1} \oplus p_{i-1}, \qquad p_i = (\bar{d}_{\,i-1} \,\&\, p_{\,i-1}) \lhd 1 \qquad (p_{i-1} \neq 0), \qquad (3)$$

при начальных условиях $d_0 = a$ и $p_0 = b$, может быть вычислена разность $d = a - b$ двух величин.

На языке псевдо Си, алгоритм реализации операции вычитания, примет вид

```
for( p = b, d = a; p; p = (p & (¬z)) ≺1 ) {
  z = d; d = d ⊕ p;
}
```

С точки зрения теории динамических систем, можно провести следующую аналогию. Формально, положим, что имеется два однородных объекта A и B, вступающие в суперпозицию $A + B \to A$ и $B + A \to B$ между собой. Каждый из объектов характеризуется своим внутренним состоянием, a и b, соответственно. При этом внешнее состояние p_A объекта A, вполне характеризуется $p_A = b$ состоянием b, объекта B, а внешнее состояние p_B объекта B, вполне характеризуется $p_B = a$ состоянием a, объекта A.

Если руководствоваться этими положениями, то простейшую динамическую систему суперпозиции объектов, при начальных условиях $p_{A0} = b$ и $p_{B0} = a$, можно представить тривиальной формальной моделью из двух операторов:

$$a_i = a_{i-1} \oplus p_{A\,i-1}, \qquad p_{A\,i} = (a_{i-1} \wedge p_{A\,i-1}) \prec 1 \qquad (p_{A\,i-1} \neq 0);$$
$$b_i = b_{i-1} \oplus p_{B\,i-1}, \qquad p_{B\,i} = (b_{i-1} \wedge p_{B\,i-1}) \prec 1 \qquad (p_{B\,i-1} \neq 0).$$

Завершение суперпозиции характеризуется состоянием $(p_A \vee p_B) = 0$, при котором объекты сливаются воедино $A \equiv B$, либо наделены одинаковым свойством и отделимы $A = B$.

3. Σ-арифметика и операции

В предыдущем разделе мы рассмотрели обычные арифметические действия.

Введем ***показатель побитовой катенации*** $\Sigma \leq n$, ограничивающий максимальное число итераций $i \leq \Sigma$, совершаемых в операциях (2) и (3). В зависимости от значения этого показателя может быть вычислена полусумма $c_1 = a \oplus b$ $(\Sigma = 1)$, полная сумма $c_n = a + b$ $(\Sigma = n)$ или неполная сумма c_Σ $(1 < \Sigma < n)$. Аналогично может быть вычислена полуразность $d_1 = a \oplus b$, разность $d_m = a - b$ или неполная разность d_Σ,

Двоичную арифметику данного типа назовем *Σ-арифметикой*. *Σ*-арифметика *ординарна* при $\Sigma = n$, половинчата *(гемична)* при $\Sigma = 1$ и *неполна* при $1 < \Sigma < n$. Если биты двоичных величин перенумеровать в обратном порядке, то имеет место двойственная, эквивалентная рассмотренной *контрординарная*, *контргемичная*, неполная или *контр Σ*-арифметика. В основном будем придерживаться *Σ*-арифметики, как арифметики с более привычным порядком.

Ординарная и гемичная арифметики хорошо известны и глубоко изучены. Используемые в них операции линейны и легко обратимы. В неполной арифметике подобные утверждения уже не действуют. Неполная арифметика нелинейна и асимметрична. Нелинейность проявляется в нарушении порядка, а асимметричность в простоте выполнения прямых действий и относительной сложности их обращения. В этом вы можете непосредственно убедиться, если в качестве упражнения, попробуете обратить неполную сумму.

В неполной арифметике, особое место занимает $(\Sigma = 2)$ Σ_2-арифметика. С формальной точки зрения, Σ_2-арифметика лежит в основе всех арифметических операций. С практической точки зрения, Σ_2-арифметика позволяет достичь полного внутреннего параллелизма и максимальной скорости выполнения арифметических действий. С этих позиций Σ_2-арифметика есть *предарифметика* и оптимальна в реализации. Следующие разделы посвятим более глубокому изучению этой арифметики и рассмотрению ее приложений.

4. Бинарные системы и счетчики

Дискретные системы, определенные на множестве двоичных величин, называют *бинарными*. Бинарные системы, начиная от арифмометров до компьютеров и других сложных систем, широко распространены.

Так или иначе, основу двоичной арифметики составляют правила счета, а двоичные счетчики составляют основу бинарных систем.

В двоичной арифметике правила счета задаются единичными арифметическими счетчиками. В свою очередь, единичные арифметические счетчики подразделяются на двоичные счетчики инкрементного типа, задаваемые уравнением

$$x_i = x_{i-1} + 2^k \bmod 2^n$$

и на счетчики декрементного типа

$$x_i = x_{i-1} - 2^k \bmod 2^n,$$

при константе 2^k - именуемой двоичным шагом, с показателем $k < n$ не превосходящим разрядности счетчика - n.

Счетчики данного типа могут быть заданы в $\boldsymbol{\Sigma}_2$-арифметике однопараметрическим P рандомизационным оператором $R_C(P_{i-1})$: $X_{i-1} \to \{X_i, P_i\}$, представляемый композицией:

$$X_i = X_{i-1} \oplus P_{i-1}, \qquad P_i = (2 \cdot (\boldsymbol{inv}(X_{i-1}) \wedge P_{i-1})) \vee 2^k \bmod 2^n,$$

с операцией инверсии битов $y = \boldsymbol{inv}(z)$, соответствующего вида, для операторов

инкрементного типа – $y = z$,

декрементного типа – $y = \neg z$.

Истинное значение x двоичного единичного арифметического счетчика на любом произвольном i-ом шаге, может быть получено за конечное число итераций $e \le (n-1)$ переменных $\{x, p\}$,

$$x_e = x_{e-1} \oplus p_{e-1}, \qquad p_e = 2 \cdot (\boldsymbol{inv}(x_{e-1}) \wedge p_{e-1}) \bmod 2^n \qquad (p \neq 0),$$

первоначально равных $x_0 = X_i$, $p_0 = P_i$, завершаемое при обнулении параметра p.

Алгоритм и программа реализации счетчиков на псевдоСи	
z = **inv**(X) & P; X = X ⊕ P; P = (z ≺ 1) | **ONE**;	**ONE** = $2^{\mathbf{k}}$ (k =0,1…)

for(x = **mod**$_n$(X), p = **mod**$_n$(P); p; p = **mod**$_n$(z ≺ 1))
{
z = **inv**(x) & p; x = x ⊕ p;
}
	Вычисление истинного значения счетчика – x, при обнулении параметра p.

Далее везде будем полагать, что разрядность устройств в точности соответствует числу значащих бит платформы генерации. В этом случае усечение незначащих битов происходит естественным образом, поэтому операцию $\boldsymbol{mod}_n$ можно опускать.

С учетом сделанных предположений, в частном случае, имеет место единичный $\boldsymbol{\Sigma}_2$-счетчик инкрементного типа, с выходом $\boldsymbol{Y}_i = \boldsymbol{X}_{i-1}$:

$$X_i = X_{i-1} \oplus P_{i-1}, \qquad P_i = (2 \cdot (X_{i-1} \wedge P_{i-1})) \vee 1, \qquad (4)$$

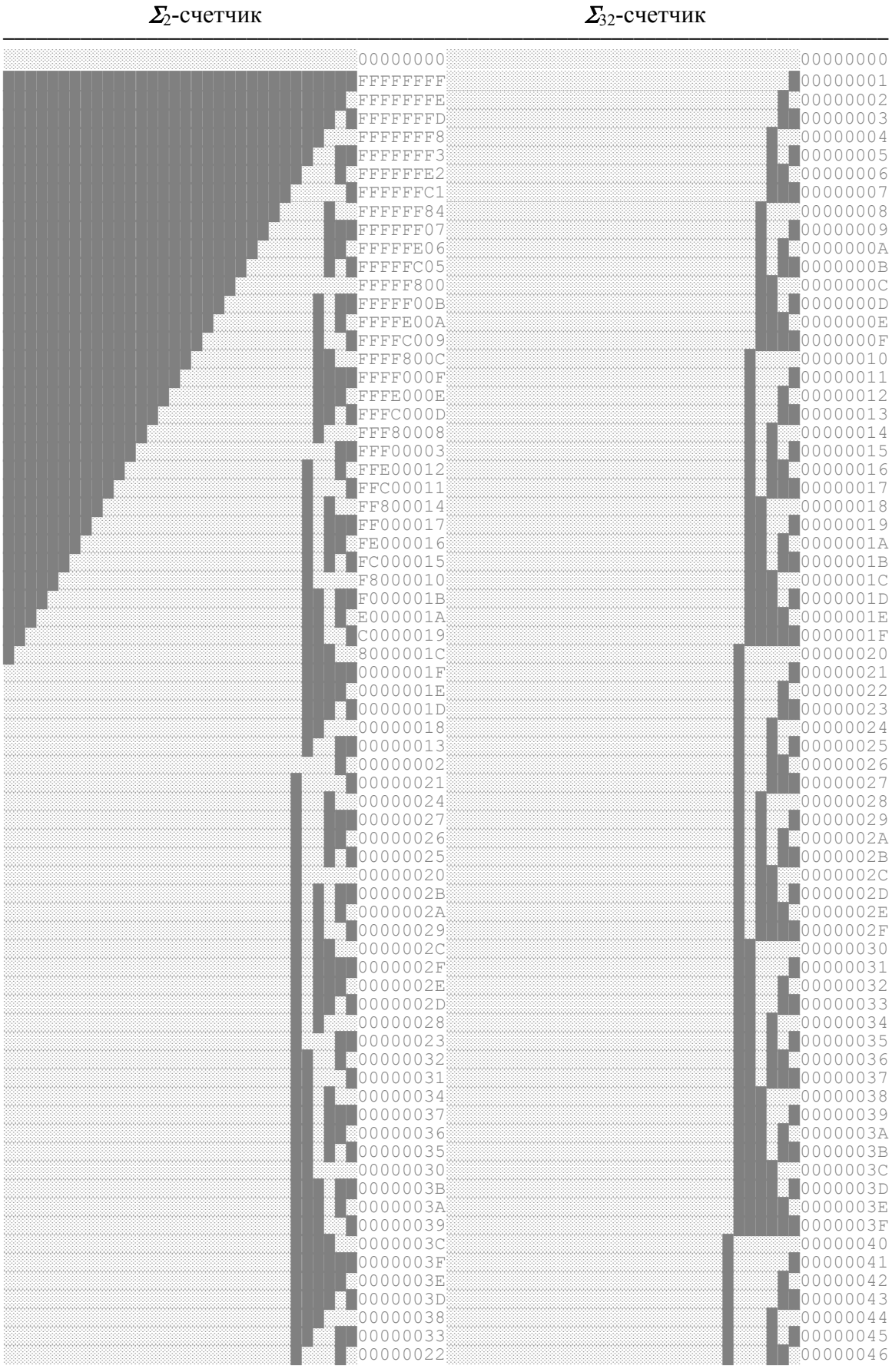
и эквивалентный ему арифметический счетчик, получаемый путем указанных выше преобразований. Алгоритм реализации единичных счетчиков представлен в нижеследующей таблице.

Алгоритм реализации единичных счетчиков: $x_i = x_{i-1} + 1 \bmod 2^n$.	
z = X & P; X = X ⊕ P; P = (z ≺ 1) | 1;	Вычисление текущего значения счетчика – X, при начальных условиях X = 0 и P = $2^n - 1$.

while(P)
{
z = X & P; X = X ⊕ P; P = z ≺ 1;
}
	Вычисление истинного значения счетчика – X, по завершению всех итераций.

На эпюре 1 представлены результаты работы 32-х разрядного Σ_2-счетчика, при начальных условиях $X = 0$ и $P = FFFFFFFF$, а также рассчитанного по указанному алгоритму, соответствующего ему единичного арифметического счетчика инкрементного типа.

Эпюра 1. 32-х битовые простейшие счетчики



По эпюре результатов видно, что в отличие от ординарных арифметических счетчиков, Σ_2-счетчики носят нерегулярный характер.

Σ_2-счетчики просты в аппаратном исполнении и обладают предельно высокой производительностью соизмеримой со скорость выполнения одной логической операции XOR, вне зависимости от длины платформы генерации, что может оказаться весьма полезным при реализации широкого класса криптографических устройств [6].

5. Дихотомические последовательности и их свойства

Двоичный единичный арифметический счетчик порождает последовательность неотрицательных целых чисел $\mathbb{Z}_n$, представленную на эпюре 1 в колонке 2, после нуля, именуемую первыми $2^n - 1$ членами натурального ряда.

Для дальнейшего изложения, введем в двоичной последовательности $B^n = \{b_i\}$, составленной из некоторого конечного числа n-битовых элементов $i \le k$, двоичную подпоследовательность $B_{\alpha/\rho}$ $(\alpha \in [1,n],\ 0 < \rho < n)$, именуемую $\boldsymbol{\alpha/\rho}$*-срезом*, иначе $\boldsymbol{\alpha}$*-срезом* составленным из $\boldsymbol{\rho}$ бит $\{b_{i(\alpha+\beta)} \in \{0,1\}, \beta = \overline{0, \rho - 1}\}$, взятых начиная с номера $\boldsymbol{\alpha}$ из каждого b_i элемента исходной для нее последовательности B^n. При срезе в один бит, срез называется единичным и обозначается просто B_α. Несколько перефразируя термин "*slice"* английского языка, срезы далее будем именовать *слайками*.

Если обратиться к Эпюре 1, колонке 2, то при внимательном рассмотрении побитового представления элементов натурального ряда, можно заметить, что период первого слайка равен 2^1, второго 2^2 и возрастает далее от α слайка к последнему $\boldsymbol{n}$- слайку по экспоненциальному закону $T_\alpha = 2^\alpha$. При этом, для каждого α единичного слайка, элементы i и $(i+T_\alpha/2)$ принадлежащие соседним полупериодам этой последовательности, комплементарно связаны инверсией между собой:

$$x_{\alpha i} = \bar{x}_{\alpha(i+T\alpha/2)}.$$

Для полупериодов каждого из α-слайков натурального ряда, также справедливо условие

$$x_{\alpha i} = x_{\alpha(i+k)} = E = \boldsymbol{const}, \qquad E \in \{0,1\}, \qquad k = \overline{0, T/2 - 1}.$$

Образно говоря, слайки натурального ряда идеально устроены и во многом подобны гармоникам разной частоты, составляющих общий для них, равномерный спектр.

Можно убедиться, что указанные дихотомические свойства присущи как счетчикам инкрементного типа (см. Эпюру 1), так и счетчикам декрементного типа. Более того, результаты расчетов показывают, что эти свойства присущи всем без исключения двоичным последовательностям максимального периода $T_n = 2^n$, формируемым на основе линейного конгруэнтного метода [7], задаваемого уравнением:

$$x_i = a \cdot x_{i-1} + b \bmod 2^n, \qquad x \in [0, 2^n - 1], \tag{5}$$

при $a \equiv 1 (mod\ 4)$ и нечетном b.

Полученные результаты позволяют сделать следующее обобщение.

Двоичная последовательность $D^n = \{d_i : i = \overline{1, T_n}\}$ неотрицательных целых чисел $d_i \in [0, 2^n - 1]$, составленных из n значащих бит, называется ***дихотомической*** или *D-последовательностью*, если любая из входящих в ее состав $D^k \in D^n$ подпоследовательностей D^k, образованная из $T_k = 2^k$ элементов исходной для нее последовательности D^n путем усечения ее старших $n - k \in [0, n-1]$ значащих бит, бесповторна в пределах периода T_k, т. е. ни для каких других пар ее элементов, кроме $d^k{}_i \in D^k$ и $d^k{}_{(i+Tk)} \in D^k$, выполняются соответствия, вида:

$$d^k{}_i = D^k{}_i \bmod T_k = d^k{}_{(i+Tk)} = D^k{}_{(i+Tk)} \bmod T_k \quad (1 \le k \le n)$$

и при этом, элементы i и $(i+T_\alpha/2)$ принадлежащие соседним полупериодам каждого α единичного слайка $D^\alpha{}_\alpha$ этой последовательности, комплиментарно связаны между собой:

$$b^\alpha{}_{\alpha i} = \bar{b}^\alpha{}_{(i+T\alpha/2)}.$$

Указанный порядок отвечает *дихотомическому порядку*. Дихотомический порядок обладает иерархической структурой типа двоичного дерева, состоящей из $k \in [1,n]$ уровней и $e_k = T_n / T_k$ взаимно непересекающихся на этих k уровнях, независимых между собой, равных $D^k{}_1 = D^k{}_2 = ... = D^k{}_j$ по значениям и числу T_k входящих в их состав элементов, так называемых *дихотомических классов* $D^k{}_j \subseteq D^n \bmod T_k$ $(j = \overline{1, e_k})$.

Указанное выше комплиментарное соответствие между элементами классов D^k, будем называть *дихотомическим комплиментом*.

Дихотомический порядок элементов натурального ряда совершенен.

Операторы, счетчики и другие объекты, включая двоичные величины, реализации которых обладают указанными дихотомическими свойствами, будем именовать *дихотомическими операторами*, *дихотомическими счетчиками*, *дихотомическими объектами* и *величинами*, соответственно.

Дихотомические последовательности D^n, в пределах периода, бесповторны. Период их повторения максимален и равен 2^n. Для изучения свойств этих последовательностей, выпишем линейное рекуррентное уравнение:

$$x_i = a_0 + \sum_{k=1}^{n} a_k x_{k\,(i-1)}\, 2^{k-1} \bmod 2^n, \qquad (6)$$

где $x_{k\,(i-1)}$ – очередной k бит двоичной n-битовой базовой переменной x, принимающий на $(i-1)$ шаге итерации уравнения, одно из значений 0 или 1,

a_0, a_k – постоянные коэффициенты, приращение и множители из интервалов $[0,2^n - 1]$ и $[0,2^{n-k+1} - 1]$, соответственно.

Известно, что при всех нечетных коэффициентах $\{a_0, a_k\}$ и условии $a_1 \equiv 1 (\bmod 4)$, уравнение (6) обратимо, а последовательность двоичных чисел составленная из $x_i \in [0,2^n - 1]$ элементов, есть M-последовательность максимальной длины с периодом повторения $T_n = 2^n$, не имеющая в пределах периода T_n равных между собой элементов.

Полученная указанным выше образом M-последовательность $X = \{x_i\}$ допускает линейное преобразование над базовой переменной:

$$y_i = c_0 + \sum_{k=1}^{n} c_k x_{k\,i}\, 2^{k-1} \bmod 2^n. \qquad (7)$$

При всех нечетных коэффициентах $\{c_k\}$ преобразование обратимо (биективно) при любых c_0. В этом случае образованная таким образом последовательность $Y = \{y_i\}$, есть последовательность максимальной длины.

Срезы и M-последовательность в целом, обладают следующими свойствами:

1. Период T_k среза k, экспоненциально нарастает $T_k = 2^k$, с ростом его номера k.
2. Все пары битов $\{b_{k\,i}, b_{k\,(i+T_k/2)}\}$ k-среза, разделенные полупериодом $T_k/2$, комплементарны между собой – $b_{k\,i} = \overline{b}_{k\,(i+T_k/2)}$.
3. Число нулевых и единичных битов в периоде слайка, равны.
4. Подпоследовательности $M_k = B \bmod T_k$, M-последовательности B, полученные путем усечения ее элементов b_i со стороны старших значащих бит, есть последовательности максимальной длины, с периодом повторения T_k.
5. M_k–последовательности бесповторны в пределах периода T_k и порождают дихотомический порядок.

Кардинальное число *card Y* множества всех различных D-последовательностей представляемых уравнением (7), вычисляется по интервалам вариации входящих в его состав коэффициентов

$$card\ Y = 2^n \cdot 2^{n-1} \cdot 2^{n-2} \cdot \ldots 2 \cdot 1 = 2^{n(n+1)/2}.$$

Кардинальное число *card D* всевозможных *D*-последовательностей, вычисляется через множество возможных состояний дихотомических классов, определяемое произведением периодов срезов

$$card\ D = T_1 \cdot T_2 \cdot \ldots T_n = 2^{n(n+1)/2}.$$

Совпадение кардинальных чисел $card\ Y = card\ D$ свидетельствует, что любая из возможных *D*-последовательностей с точностью до изоморфизма может быть единственным образом выражена через коэффициенты уравнения (7).

В свою очередь, коэффициенты c этого уравнения можно найти аналитически по выборке из n, до n^2 элементов, взятых из любой части *Y* последовательности. Для этого требуется поочередно решить n систем уравнений, сначала с размерностью 2 и далее увеличивающуюся на каждом шаге на единицу до n, над $n\cdot(n+1)/2$ двоичными неизвестными $c_{k\,i} \in \{0,1\}$, входящих в состав коэффициентов $c_k\ (k = 0, n)$. Максимальная сложность решения этой задачи невелика $O(n^4)$, что по существу не позволят серьезно говорить, о какой либо значимой с практической точки зрения криптографической стойкости *D*-последовательностей.

Между тем, срезы *D*-последовательностей будучи взятые в отдельности при больших n и коэффициентах, позволяющих достичь наиболее высокой скорости распространения младших битов на старшие, обладают высокими статистическими свойствами и могут иметь очень высокую криптографическую стойкость, соизмеримую с их достаточно большим периодом *T*.

По отношению к двоичным последовательностям, формируемым в полях Галуа, все это дает основания к более широкому практическому применению *D*-последовательностей и средств их получения, так называемых ***дихотомических Dh-генераторов***.

Учитывая комплекс требований, предъявляемый к криптосистемам, закон функционирования *Dh*-генераторов и формирования *D*-последовательностей представленных уравнениями (6) и (7), весьма сложен, что делает данный подход малопригодным для практической реализации.

Надлежащим образом разрешить эту проблему оказалось возможным на основе рандомизационных систем и неполной арифметики. Следуя этому подходу, будем ориентироваться на практическую реализацию дихотомических устройств и систем, с любым наперед заданным периодом повторения, обладающих высокими статистическими свойствами и функциональной сложностью, допускающих высокоэффективную последовательную и многоканальную всюду параллельную, одно и много разрядную беспроцессорную обработку на любых платформах вычислительных устройств.

6. Σ_2-счетчики с открытым входом. Аттракторы

Дихотомический счетчик (4), рассмотренный ранее, не имеет входов, т.е. автономен. Руководствуясь положениями раздела 3, закрепим за внутренней переменной *X*, входящей в состав этого счетчика, статус *базовой переменной*. Отношения базовой переменной с внешним параметром *P*, могут быть представлены следующим графом

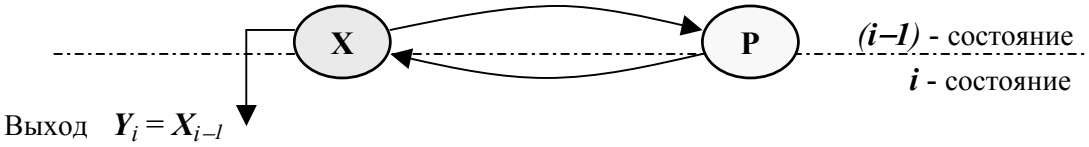


Рис. 1.

Представленный граф можно продолжить, как это показано на Рис.2.

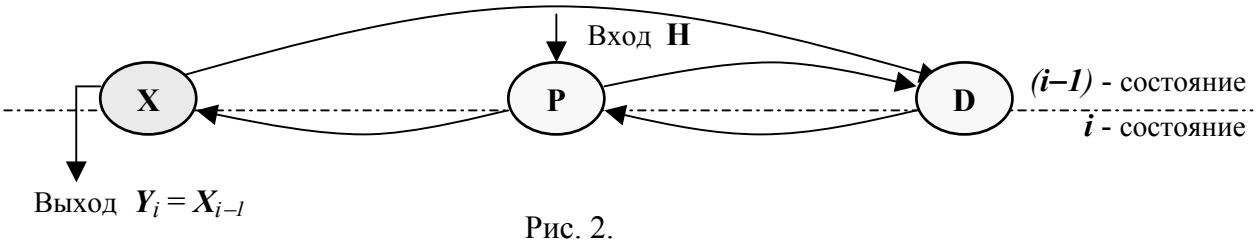


Рис. 2.

Следуя графу Рис.2, дихотомический счетчик с открытым входом $\boldsymbol{H}$ и выходом $\boldsymbol{Y_i = X_{i-1}}$, в $\boldsymbol{\Sigma_2}$-арифметике можно задать двухпараметрическим $\{P,D\}$ рандомизационным оператором $R_C\ (P_{i-1},D_{i-1})$: $X_{i-1} \to \{X_i,P_i,D_i\}$, представляемый композицией операторов:

$$X_i = X_{i-1} \oplus P_{i-1}, \quad P_i = D_{i-1} \oplus H, \quad D_i = (2\cdot(\boldsymbol{inv}(X_{i-1}) \wedge P_{i-1})) \vee P_H \bmod 2^n, \qquad (8)$$

с параметром синхронизации $P_H = (\neg H) \wedge 1$.

$\boldsymbol{\Sigma_2}$-счетчики подобного типа характеризуются относительно медленной скоростью нарастания изменений старших значащих битов. Скорость нарастания изменений можно несколько увеличить, за счет параметра синхронизации P_H. Для этого мысленно разобьем платформу счетчика на несколько равных частей. Обращаясь к уравнениям (4) и (8), можно увидеть, что слияние этих частей осуществляется за счет самых старших признаков переноса, а скорость нарастания изменений зависит от длины пробегаемых ими частей. Инвертируя значения старших признаков переноса, тем самым можно косвенно ограничить длину пробегаемых ими частей и несколько увеличить скорость нарастания изменений.

Для приложений, рекомендуется принять длину пробега Lp, равной $Lp = \lfloor log_2\ n \rfloor$, где $\lfloor\ \mu\ \rfloor$ – наибольшее целое $\le \mu$. Исходя из длины пробега, согласно приведенному ниже алгоритму, можно вычислить константу синхронизации E_n:

```
for( En = ONE, i = Lp;  i < n;  i = i + Lp )
  En = En | (ONE ≺ i);
```

С учетом сделанных замечаний, уравнения работы автономного счетчика (4) и счетчика с открытым входом (8), можно переписать следующим образом:

$$X_i = X_{i-1} \oplus P_{i-1}, \quad P_i = (2\cdot(\boldsymbol{inv}(X_{i-1}) \wedge P_{i-1})) \oplus E_n \bmod 2^n, \qquad (9)$$

$$X_i = X_{i-1} \oplus P_{i-1}, \quad P_i = D_{i-1} \oplus H, \quad D_i = (2\cdot(\boldsymbol{inv}(X_{i-1}) \wedge P_{i-1})) \oplus P_H \bmod 2^n, \qquad (10)$$

с параметром синхронизации $P_H = E_n \oplus (H \wedge 1)$.

Вводя третий, дополнительный параметр Q в уравнения (10), можно задать дихотомический $\boldsymbol{\Sigma_2}$-счетчик с двумя входами $\{\boldsymbol{H_P},\boldsymbol{H_Q}\}$:

$$X_i = X_{i-1} \oplus P_{i-1}, \quad P_i = D_{i-1} \oplus H_{\boldsymbol{P}}, \quad Q_i = B_{i-1} \oplus H_{\boldsymbol{Q}}, \qquad (11)$$
$$D_i = (2\cdot(\boldsymbol{inv}(X_{i-1}) \wedge Q_{i-1})) \oplus P_H \bmod 2^n.$$

На эпюре 2 представлены результаты работы двух 16-ти разрядных счетчиков инкрементного типа с открытым входом, описываемых уравнениями (8) и (10), с $P_H = 1$ и $P_H = 0x1111$, соответственно, при нулевых начальных условиях $X = 0$, $P = 0$, $D = 0$ и входным параметром $H = 0$.

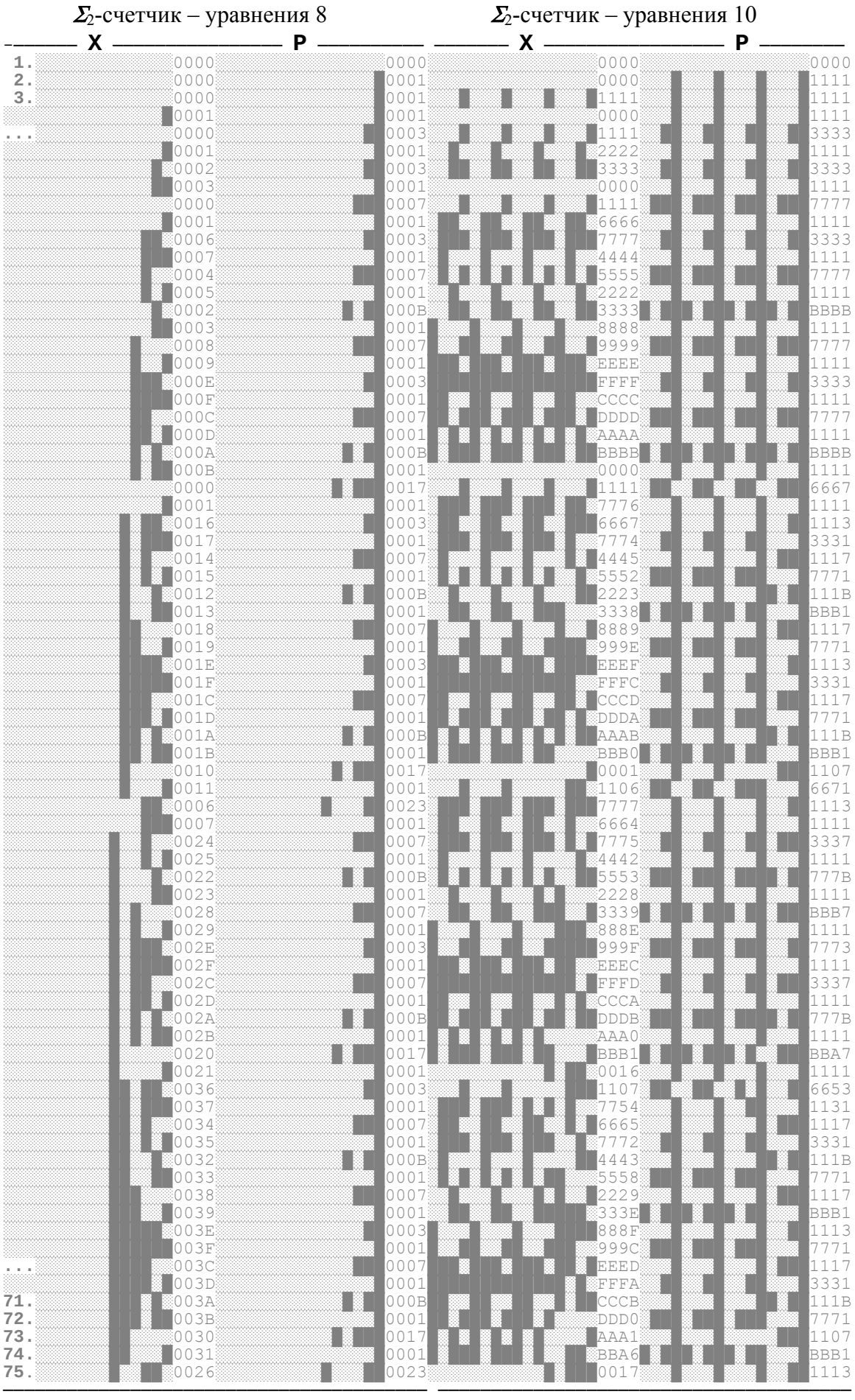
На эпюре можно заметить наличие, обычно небольшого, переходного нестационарного участка, присущего всем рассмотренным типам дихотомических $\boldsymbol{\Sigma_2}$-счетчиков, после которого они самостоятельно, феноменальным образом переходят в устойчивое состояние и далее всюду, в пределах периода 2^n, ведут себя бесповторно и от периода к периоду - идентично. Такие участки, длиной равной 32 и 24, соответственно, имеют место в представленных на эпюре вариантах.

Переходной участок складывается из строго линейной ***зоны прозрачности*** и ***аттрактора***. Наличие зоны прозрачности – эффект негативный, вынужденный и обусловлен введением конвейерных механизмов, необходимых для достижения максимальной эффективности вычислений (в один такт) и возможности организации параллельной обработки по каждому отдельно взятому биту. Ограничиваясь наиболее простыми случаями реализации счетчиков, используя уравнения (9) и (10), выпишем состояния, принимаемые ими на первых шагах итерации:

- изменение состояния 1-(одно)параметрического автономного счетчика:

1-й такт $X_{(1)} = X_0$, $P_{(1)} = P_0$;
2-й такт $X_{(2)} = X_0 \oplus P_0$, $P_{(2)} = (2\cdot(X_0 \wedge P_0)) \oplus E_n$;
3-й такт $X_{(3)} = X_0 \oplus P_0 \oplus (2\cdot(X_0 \wedge P_0)) \oplus E_n$, ... ,

Эпюра 2. 16-ти битовые счетчики с открытым входом



- изменение состояния 2-(двух)параметрического счетчика с открытым входом:

1-й такт $X_{(1)} = X_0$, $P_{(1)} = P_0$, $D_{(1)} = D_0$;
2-й такт $X_{(2)} = X_0 \oplus P_0$, $P_{(2)} = D_0 \oplus H$, $D_{(2)} = (2\cdot(X_0 \wedge P_0)) \oplus P_H$;
3-й такт $X_{(3)} = X_0 \oplus P_0 \oplus D_0 \oplus H$, $P_{(3)} = (2\cdot(X_0 \wedge P_0)) \oplus P_H \oplus H$, ... ;
4-й такт $X_{(4)} = X_0 \oplus P_0 \oplus D_0 \oplus (2\cdot(X_0 \wedge P_0)) \oplus P_H$, ...

Из представленных выше зависимостей следует, что длина линейной зоны прозрачности N_0 полностью определяется выходной переменной $\boldsymbol{Y}_i = \boldsymbol{X}_{(i)}$ и числом параметров N_P входящих в контур уравнений генерации и равна

$$N_0 = 1 + N_P. \qquad (12)$$

После прохождения линейной зоны прозрачности, счетчики переходят в нелинейное состояние, сопряженное с ***аттрактором***. Понятие аттрактора отождествляется с наличием притягивающего множества, присущего широкому классу динамических систем, характеризующего множество возможных состояний устойчивого равновесия этих систем.

В зависимости от динамики поведения в положении равновесия, будем различать системы *субаддитивного*, *аддитивного* и *супераддитивного* типа.

Системы субаддитивного типа способны вырождаться, переходить в статическое состояние или совершать в состоянии равновесия небольшие периодические колебания. В отличие от них, системы аддитивного типа в состоянии равновесия носят строго периодический и бесповторный характер.

Системы супераддитивного типа периодичны и носят равноповторный характер. Так рассмотренные нами счетчики относятся к аддитивным системам, с максимальным периодом повторения, равным $T_n = 2^n$. Для супераддитивных систем понятие периода, в некотором роде, утрачивает привычный нам смысл, так как множества их состояний образуют взаимно проникающие в друг друга скопления - *кластеры*. Отметим, что при больших n чередование этих скоплений характеризуются периодом близким к $e^n \approx 2^{1.443\,n}$, где e – число Эрмита, как одно из наиболее известных чисел в физике и математике, равное 2.71828… .

Анализ показывает, что максимальная длина переходного (нестационарного) участка L_m в $\boldsymbol{\Sigma}_2$-арифметике, для D-последовательностей формируемых на основе аддитивных систем, в нашем случае D-операторов, равна

$$L_m = N_P \cdot n \qquad (13)$$

и полностью определяется длиной платформы n и числом параметров N_P входящих в состав их уравнений. При этом фактическую длину переходного участка – L, можно вычислить через индекс

$$L = \mathbf{min}\{k : Y_k = Y_{Lm+i},\ k = \overline{0, L_m},\ i = \overline{1, T_n}\},$$

первого встретившегося выходного состояния Y_L, из числа его состояний Y_k на начальном участке длиной L_m, в точности совпадающим с одним его из состояний Y_{Lm+i} на стационарном участке $k + T_n$, такой же длины L_m, но смещенным на период T_n.

На практике, для прохождения переходного участка и получения бесповторных последовательностей ограниченных длиной статистической выборки $L_S \le T_n$, исходя из дихотомических свойств, обычно достаточно значительно меньшее $k \le L_m$ число k холостых итераций

$$k = \rceil N_P \cdot log_2 L_S \lceil .$$

Здесь $\rceil \mu \lceil$ – наименьшее целое $\ge \mu$..

Феномен перехода в стационарное состояние и связанный с этим бесповторный характер дихотомических последовательностей формируемых на основе рассмотренных выше параметрических D-операторов с одной базовой переменной X, означает существование единственной ей рекуррентной последовательности - рекурренты. Из этого следует взаимная однозначность (биективность) отображения пространства $(N_P + 1)$-измерений в одномерное про-

странство, порождаемое выходом *D*-оператора. В зависимости от структуры и числа параметров, входящих в состав *D*-оператора, данное отображение может носить более или менее сильно выраженный нелинейный характер, обусловленный отображением пространства большего числа измерений, в меньшее.

В свою очередь, бесповторность на стационарном участке и единственность рекурренты, влечет, что при H = **const**, каждому значению базовой переменной, независимо от начальных условий, ставится в строгое соответствие свой кортеж, составленный из значений параметров, входящих в состав представленных уравнений (8) и (10).

Для примера, обращаясь к формуле (8)

$$Y_i = X_{i-1}, \quad X_i = X_{i-1} \oplus P_{i-1}, \quad P_i = D_{i-1}, \quad D_i = (2\cdot(X_{i-1} \wedge P_{i-1})) \vee 1,$$

и к нижней части эпюры 2, при H = 0, после завершения очередной итерации – это будет:

$Y_{72} = X_{71} = 3B,\ X_{72} = Y_{73} = 30,\ P_{72} = 1,\ D_{72} = P_{73} = 17;$
$Y_{73} = X_{72} = 30,\ X_{73} = Y_{74} = 31,\ P_{73} = 17,\ D_{73} = P_{74} = 1;$
$Y_{74} = X_{73} = 31,\ X_{74} = Y_{75} = 26,\ P_{74} = 1,\ D_{74} = P_{75} = 23;$
$Y_{75} = X_{74} = 26,$ . . . и т.д.

Независимость от начальных условий означает, что при других начальных значениях, на стационарном участке *D*-последовательность будет той же самой, но отличающаяся только начальным смещением, т.е. всегда найдется такой элемент под номером *S*, что

$Y_S = X_{S-1} = 3B,\ X_S = Y_{S+1} = 30,\ P_S = 1,\ D_S = P_{S+1} = 17;$
$Y_{S+1} = X_S = 30,\ X_{S+1} = Y_{S+2} = 31,\ P_{S+1} = 17,\ D_{S+1} = P_{S+2} = 1;$
$Y_{S+2} = X_{S+1} = 31,\ X_{S+2} = Y_{S+3} = 26,\ P_{S+2} = 1,\ D_{S+2} = P_{S+3} = 23;$
$Y_{S+3} = X_{S+2} = 26,$ . . . и т.д.

Другими словами, показанная стабилизация параметров, вызываемая движением к стационарному состоянию, ведет к тому, что пространство различных состояний таких аддитивных систем измеряется не величиной $2^{n\cdot(Np+1+Ny)}$, как бы этого нам хотелось исходя из числа переменных (N_P+1) и имеющихся входов N_Y, а существенно ниже $2^{n\cdot(1+Ny)}$. Объективно говоря, явление негативное, собственно – расплата за неполную арифметику и используемые конвейерные механизмы.

В итоге, число различных *D*-последовательностей которые можно получить, равно $2^{n\cdot(1+Ny)}$. Между тем, путем вариации входов, как будет показано ниже, негативные последствия, связанные со стабилизацией переменных, можно заметно уменьшить, а число различных *D*-последовательностей увеличить.

Кроме всего этого, наличие нестационарного участка *(L ≠ 0)* и существование единственной рекуррентной последовательности к исходной для нее *D*-последовательности, свидетельствует, что отображение, порождаемое *D*-оператором, носит взаимно неоднозначный, сюръективный характер. В силу сюръективных свойств присущих *D*-операторам, можно говорить, что данные операторы носят ***односторонний*****,** а их последовательная итерация, иначе не что иное, как их мультипликативная композиция – ***однонаправленный*** характер.

Однонаправленный характер *D*-операторов, после некоторого числа их итераций, в известных, не менее чем $2^{n\cdot Np}$ случаях, не позволяет воспроизвести их начальное состояние.

7. Линейная стохастическая криптография

Стохастическая криптография представляет собой новое научно-практическое направление развития линейных и нелинейных стохастических систем с дискретным временем.

Основу стохастической криптографии составляют *дихотомические* и *полихотомические* операторы.

Дихотомические, иначе *D*-операторы линейны по архитектуре и относятся к классу *линейных* стохастических (рандомизационных) систем.

Полихотомические, иначе *Ð*-операторы представляются *нелинейным аналогом D*-операторов и относятся к классу *нелинейных рандомизационных систем*.. Полихотомические *Ð*-операторы

позволяют устранить существенные недостатки присущие дихотомическим операторам, существенно превосходят их в криптографическом отношении и более просты в исполнении..

Дихотомические операторы выступают в качестве строительных блоков линейных рандомизационных систем и предопределяют направления развития нелинейных систем.

Учитывая такое особое положение *D*-операторов, не вдаваясь в точные формулировки, рассмотрим более подробно этот важный класс операторов.

Рассмотренные ранее дихотомические *D*-счетчики, по сути, характеризуются медленной скоростью нарастания изменений старших значащих битов, за счет участия в распространении влияния не самих бит, а образованных в результате их катенации признаков переноса. Скорость нарастания изменений можно увеличить, за счет распространения влияния младших битов на старшие.

7.1. Дихотомические генераторы и *D*-операторы

Дихотомические *Dh*-генераторы строятся на основе *D*-счетчиков, путем распространения влияния младших битов на старшие. Даже простейший анализ показывает, что число вариантов построения счетчиков и механизмов распространения влияния битов, достаточно много.

Один из типовых вариантов реализации *Dh*-генераторов, представляется самосинхронизирующимся трехпараметрическим *{P,Q,D}* оператором $R_H(P_{i-1},Q_{i-1},D_{i-1},\boldsymbol{H})$: $B_{i-1} \to \{B_i,P_i,Q_i,D_i\}$, с коэффициентом $\boldsymbol{H}$ и косвенным выходом $\boldsymbol{r}_i = Q_{i-1} \oplus P_{i-1}$ или $\boldsymbol{r}_i = Q_{i-1} \oplus D_{i-1}$, составленным из операторов:

$$B_i = B_{i-1} \oplus P_{i-1}, \quad P_i = (2^{\boldsymbol{g}} \cdot Q_{i-1}) \oplus D_{i-1} \quad (\boldsymbol{g} \geq 2), \qquad (14)$$
$$Q_i = B_{i-1} \oplus \boldsymbol{H}, \quad D_i = (2 \cdot (Q_{i-1} \wedge P_{i-1})) \vee 1.$$

Представленный рандомизационный оператор задает дихотомический генератор с периодом $T = T_n$, являющийся естественным обобщением самосинхронизирующихся *D*-счетчиков R_C, задаваемых двухпараметрическим *{Q,D}* оператором $R_C(Q_{i-1},D_{i-1},\boldsymbol{H}_C)$: $B_{i-1} \to \{B_i,Q_i,D_i\}$, вида:

$$B_i = B_{i-1} \oplus D_{i-1}, \quad Q_i = B_{i-1} \oplus \boldsymbol{H}_C, \quad D_i = (2 \cdot (Q_{i-1} \wedge D_{i-1})) \vee 1,$$

с коэффициентом $\boldsymbol{H}_C$ и отличается от них, задаваемой показателем $\boldsymbol{g}$, более высокой скоростью распространения влияния младших битов на старшие.

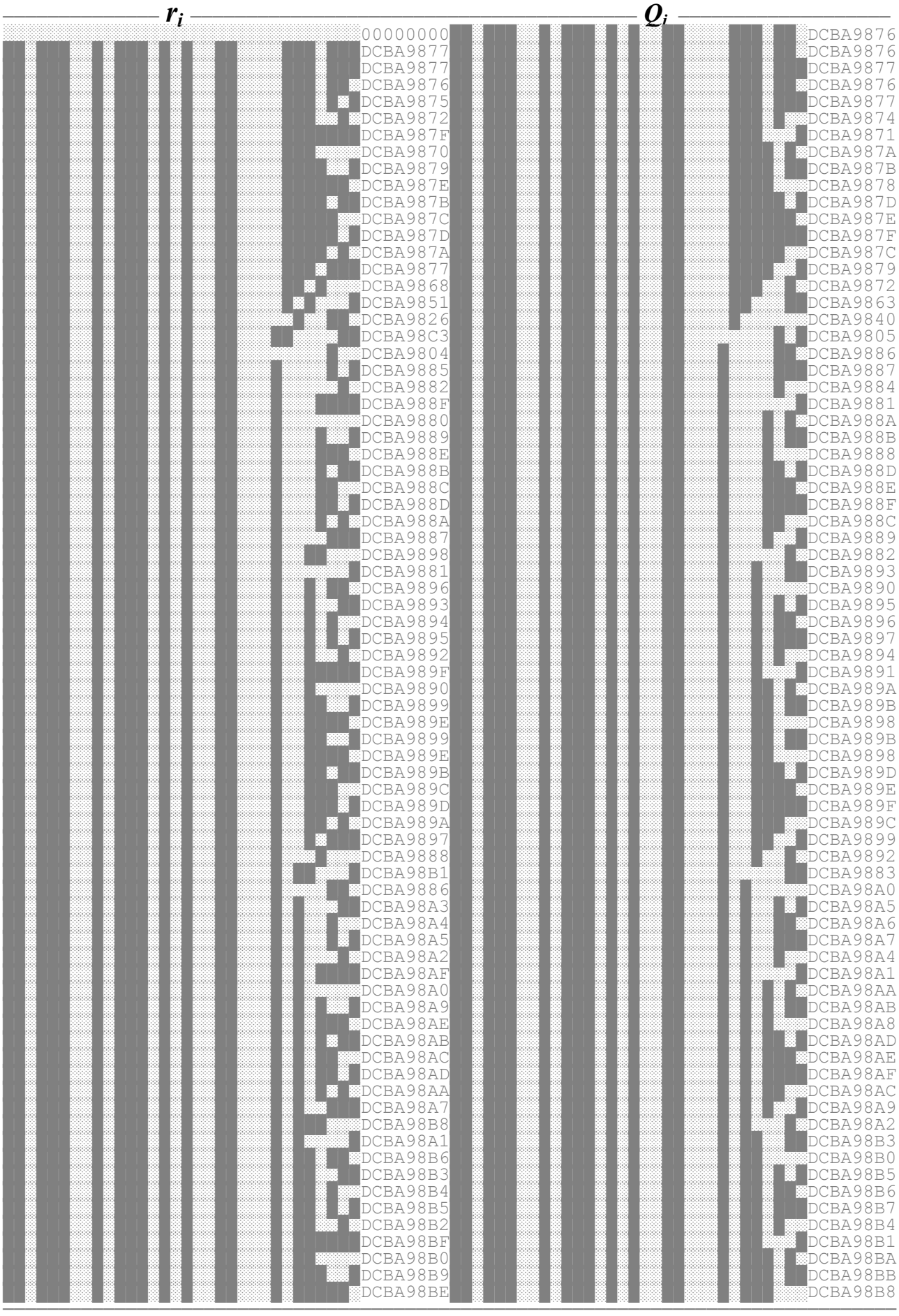
На эпюре 3 и 4 в первой и второй колонках представлены результаты работы такого 32-х разрядного счетчика и соответствующего ему *Dh*-генератора, с косвенным $\boldsymbol{r_i} = Q_{i-1} \oplus D_{i-1}$ и прямым $\boldsymbol{Q_i}$ выходом, при начальных условиях B = P = D = Q = 0, H = DCBA9876 и g = 2.

Из представленных эпюр видно, чем выше скорость распространения влияния битов, тем старшие биты *D*-последовательностей носят более сильно выраженный недетерминированный характер

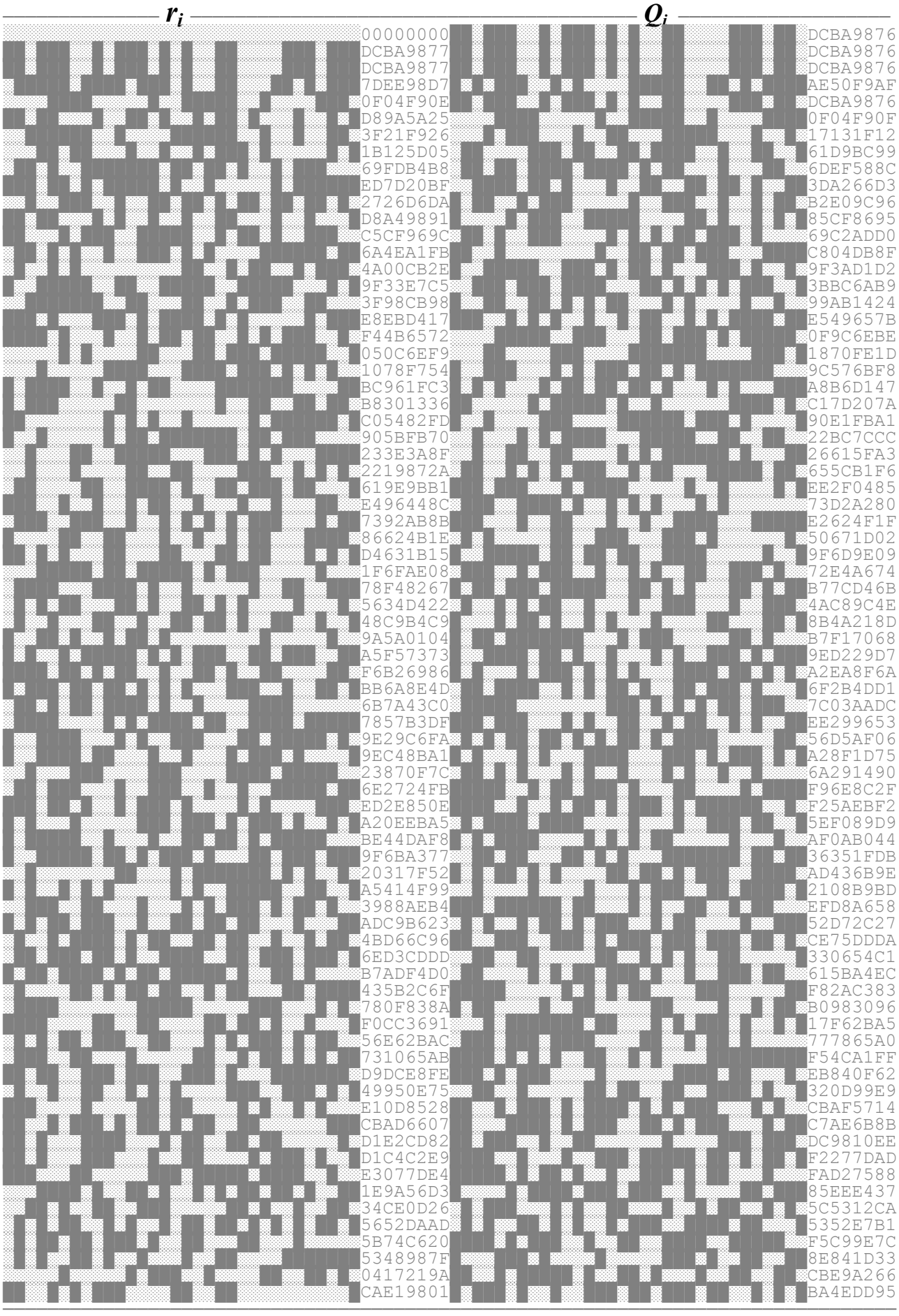
Как следует из анализа, рандомизационные операторы (4), (8-11), (14) способны порождать *D*-последовательности и по определению именуются ***дихотомическими*** или ***D-операторами***.

Для проведения статистического анализа дихотомических последовательностей, формируемых *Dh*-генератором (14), в качестве основного пакета статистических тестов, выбран широко известный пакет DIEHARD, Дж. Марсальи. Пакет тестов специально разрабатывался для исследования статистических свойств конгруэнтных последовательностей. Именно этим и обусловлен данный выбор, так как известно, что, с точностью до изоморфизма, *D*-последовательностям присущи все свойства линейных конгруэнтных последовательностей.

Эпюра 3. 32-х битовый счетчик



Эпюра 4. 32-х битовый дихотомический генератор



В целях получения более точных и объективных статистических оценок, анализ проводился

- по конкретно выделенным срезам *D*-последовательности – ***побитовое тестирование***,
- для усеченных *D*-последовательностей со стороны младших бит – ***поэлементное тестирование***.

Побитовый статистический анализ показывает, наличие существенной корреляции между битами срезов начиная с 1 по 25, включительно. Для срезов 26 по 64, заметной корреляции между битами срезов не выявлено.

Выборочные результаты поэлементного тестирования *D*-последовательностей приведены в таблице 1.

Таблица 1

Число младших усекаемых битов	**Длины выходного блока генератора (в битах) – результат тестирования**
26	32 – существенно выраженная корреляция, 38 – корреляция не выявлена
28	32 – существенно выраженная корреляция, 36 – корреляция не выявлена
32	1 – корреляция не выявлена, 2 - сильно выраженная корреляция, 3, 4, 8 – не сильно выраженная корреляция, 5, 6, 7 – слабо выраженная корреляция, 9, 10 – несущественная корреляция, 11-15 – корреляция не выявлена, 16 – существенно выраженная корреляция.
	32, 64 – существенно выраженная корреляция, 40, 94 – не сильно выраженная корреляция, 48, 128 – слабо выраженная корреляция, 56, 80, 144, 160, 176, 192, 208, 224, 250, 256 – корреляция не выявлена

Как следует из анализа результатов приведенных в таблице, элементы *D*-последовательностей, формируемые на основе указанных генераторов (14), достаточно сильно коррелированны между собой. Это обусловлено существенно выраженным, детерминированным характером поведения младших битов дихотомических величин и относительно невысокой линейной скоростью распространения влияния младших битов на старшие. Последнее приводит к образованию кластеров.

При усечении 32-х младших битов статистика стабильна и удовлетворительна, лишь при длине выходного блока генератора более 128 бит. В остальных случаях, статистика нестабильна.

Преодоление указанных недостатков возможно, за счет увеличения скорости распространения влияния младших битов на старшие. Для этих целей могут использоваться, так называемые лавинные *Dh*-генераторы.

Лавинные Dh-генераторы задаются самосинхронизирующимся 4-х параметрическим $\{A, P,Q,D\}$ *D*-оператором $R_H(A_{i-1},P_{i-1},Q_{i-1},D_{i-1},\boldsymbol{H})\colon B_{i-1} \to \{B_i,A_i,P_i,Q_i,D_i\}$, с коэффициентом $\boldsymbol{H}$ и косвенным выходом $\boldsymbol{r}_i = A_{i-1} \oplus P_{i-1}$ или $\boldsymbol{r}_i = A_{i-1} \oplus D_{i-1}$, вида:

$$B_i = B_{i-1} \oplus P_{i-1}, \quad A_i = (2^{\boldsymbol{q}}\cdot A_{i-1}) \oplus Q_{i-1}, \quad P_i = (2^{\boldsymbol{g}}\cdot A_{i-1}) \oplus D_{i-1}, \qquad (15)$$
$$Q_i = B_{i-1} \oplus \boldsymbol{H}, \quad D_i = (2\cdot(A_{i-1} \wedge P_{i-1})) \vee 1 \quad (\boldsymbol{g} \geq 2, \boldsymbol{q} = 2\cdot\boldsymbol{g}+1).$$

Побитовый статистический анализ генераторов данного типа показывает наличие существенной корреляции, между битами срезов 1 по 24, включительно. Заметной корреляции между битами срезов, начиная с 25, не выявлено.

В отличие от рассмотренных выше простых *Dh*-генераторов (14), также не выявлено заметной корреляции между элементами усеченных на 24 и более бит лавинных *Dh*-генераторов.

Для всех рассмотренных выше типов параметрических дихотомических счетчиков и генераторов, функционирующих в неполной арифметике, необходимо отметить наличие небольшого, переходного нестационарного участка *(аттрактора)*, после которого они самостоятельно, фе-

номенальным образом переходят в устойчивое состояние и далее всюду, в пределах периода 2^n, ведут себя бесповторно и от периода к периоду - идентично.

В Σ_2-арифметике, максимальная длина переходного участка составляет $Np \cdot n$, где Np – число параметров в контуре уравнений генерации. По мере прохождения переходного участка наблюдается стремление параметров к некоторому базовому состоянию, вне зависимости от начального состояния генератора. Стремление к базовому состоянию с одной стороны вызывает весьма полезный в криптографическом смысле эффект, когда по базовому состоянию, становиться невозможным, установить истинное начальное состояние, по сути, вычислить ключ, а с другой, негативный эффект, за счет сокращения пространства состояний до 2^n.

Частично устранить указанный негативный эффект возможно на основе *D*-операторов с ***переменными коэффициентами*** и ***нелинейных управляемых операций***.

7.2. *D*-операторы с переменными коэффициентами

Для *D*-операторов с ***переменными коэффициентами***, принимается, что модификатор $\boldsymbol{H}$ входящий в состав их уравнений может быть переменным.

В целях обеспечения равного вклада всех битов $\boldsymbol{H}$, уравнения (14) и (15) необходимо модифицировать, используя расщепление параметра $\boldsymbol{H} = \boldsymbol{H}^{\circ} \cup \boldsymbol{H}^{\bullet}$ на независимые между собой $(\boldsymbol{H}^{\circ} \cap \boldsymbol{H}^{\bullet} = \varnothing)$ регулярную $\boldsymbol{H}^{\circ}$ и нерегулярную $\boldsymbol{H}^{\bullet}$ компоненты, а именно:

- для *D*-оператора простого (14), 3-х параметрического типа

$$B_i = B_{i-1} \oplus P_{i-1}, \quad P_i = (2^{\boldsymbol{g}} \cdot Q_{i-1} \vee \boldsymbol{H}^{\bullet}) \oplus D_{i-1} \quad (\boldsymbol{g} \geq 2), \qquad (16)$$
$$Q_i = B_{i-1} \oplus \boldsymbol{H}^{\circ}, \quad D_i = (2 \cdot (Q_{i-1} \wedge P_{i-1})) \vee 1,$$

- для *D*-оператора лавинного (15), 4-х параметрического типа

$$B_i = B_{i-1} \oplus P_{i-1}, \quad A_i = (2^{\boldsymbol{q}} \cdot A_{i-1}) \oplus Q_{i-1}, \quad P_i = (2^{\boldsymbol{g}} \cdot A_{i-1} \vee \boldsymbol{H}^{\bullet}) \oplus D_{i-1}, \qquad (17)$$
$$Q_i = B_{i-1} \oplus \boldsymbol{H}^{\circ}, \quad D_i = (2 \cdot (A_{i-1} \wedge P_{i-1})) \vee 1 \quad (\boldsymbol{g} \geq 2, \boldsymbol{q} = 2 \cdot \boldsymbol{g} + 1),$$

при

$$\boldsymbol{H}^{\bullet} = \boldsymbol{H} \bmod 2^{\boldsymbol{g}}, \quad \boldsymbol{H}^{\circ} = \boldsymbol{H}^{\bullet} \oplus \boldsymbol{H} \quad \text{и косвенным выходом} \quad \boldsymbol{r}_i.$$

В простейшем случае закон вариации коэффициентов $\boldsymbol{H}$ дихотомических операторов, можно задать ***ламинарным генератором***, описываемым линейным уравнением:

$$\boldsymbol{H}_i = \boldsymbol{H}_{i-1} \oplus ((\boldsymbol{H}_{i-1} \lessdot 1) \vee 4),$$

при четном начальном условии $\boldsymbol{H}_0 \equiv 0 \ (mod\ 2)$, с коротким, независимым от $\boldsymbol{H}_0$, периодом $T_{\boldsymbol{H}} = 2^{[1 + log2(\boldsymbol{n}-2)]}$.

Построенные таким образом генераторы, есть *Dh*-генераторы максимального периода, а формируемые на их основе последовательности после преодоления переходного участка, есть *D*-последовательности с периодом $T = T_n$ и пространством состояний $T_{\boldsymbol{H}} \cdot T_n$.

Закон вариации коэффициентов $\boldsymbol{H}$ может носить ***регулярный*** (дихотомический, ламинарный ординарно, в нашем случае лево направленный) или ***нерегулярный*** (контрординарный дихотомический и ламинарный, *LFSR* и пр.) характер. Генераторы, построенные на основе регулярных *D*-операторов, иначе регулярные или просто *Dh*-генераторы, сохраняют присущие им дихотомические свойства. В отличие от них, генераторы, построенные на основе нерегулярных *D*-операторов, утрачивают эти свойства, вырождаются, либо приобретают равноповторные свойства. Такие генераторы именуются ***нерегулярными дихотомическими*** или ***Gh-генераторами***.

На основе вариации коэффициентов входящих в состав уравнений *D*-операторов может быть не только увеличена скорость распространения влияния младших битов коэффициентов на старшие и тем самым уменьшена их корреляция, но и существенно увеличен период и мощность пространства состояний, а также улучшены другие статистические свойства формируемых двоичных последовательностей.

Вносимая законом вариации коэффициентов неопределенность и нелинейность, по сути обусловленная вложением пространства большего числа измерений в меньшее, позволяет эффективно противостоять *линейным атакам*.

Закон вариации коэффициентов задается соответствующими операторами – ***H-конверторами*** и, как правило, носит периодический характер.

7.3. Нелинейная управляемая операция

Продолжая дальнейшее развитие, введем понятие ***нелинейной управляемой операции*** $a \wedge^{c} b$, над парой двоичных переменных $\{a, b\}$, связанных нелинейной управляемой операцией $\wedge^{c}$ по закону C, задаваемым c_k битом двоичной переменной c.

Примем, при $c_k = 0$ имеет место конъюнкция, при $c_k = 1$ – дизъюнкция. В этом случае справедливо следующее аналитическое соотношение

$$a \wedge^{c} b = (a \wedge b) \oplus (c \wedge (a \oplus b)). \qquad (18)$$

Для введения ***нелинейной управляемой операции*** в уравнения (14)-(17), достаточно входящую в них фиксированную операцию конъюнкции $\wedge$, заменить операцией $\wedge^{c}$. Допускается два вида управления:

- Внутреннее управление – $\boldsymbol{C}_i = B_{i-1} \lhd 2$ или $\boldsymbol{C}_i = P_{i-1} \lhd 1$.
- Внешнее управление

  $\boldsymbol{C_i} = E_{i-1} \lhd 2$, где E_{i-1} – внешняя дихотомическая последовательность,

либо

  $\boldsymbol{C}_i = \boldsymbol{C}_{i-1} \oplus ((\boldsymbol{C}_{i-1} \lhd 1) \vee 4)$ – внешняя ламинарная последовательность.

При указанных механизмах управления, последовательности, формируемые счетчиками и генераторами с нелинейной управляемой операцией, фактически *Dh*-генераторы с переменной структурой, есть дихотомические последовательности.

Аналогично закону вариации коэффициентов, закон управления операцией $\boldsymbol{C}$, может носить ***регулярный*** (ординарный дихотомический, ламинарный) или ***нерегулярный*** (контрординарный дихотомический и ламинарный, *LFSR* и пр.) характер. Генераторы, построенные на основе регулярных *D*-операторов, иначе регулярные или просто *Dh*-генераторы, сохраняют присущие им дихотомические свойства. Генераторы, построенные на основе нерегулярных *D*-операторов, утрачивают эти свойства, вырождаются, либо приобретают равноповторные свойства. Такие генераторы также именуются ***нерегулярными дихотомическими***, ***Gh-генераторами***.

На основе нелинейных управляемых операций включаемых в состав уравнений *D*-операторов может быть увеличена скорость распространения влияния младших битов на старшие и тем самым уменьшена корреляция, существенно увеличен период и мощность пространства состояний, а также улучшены другие статистические свойства формируемых двоичных последовательностей. Вносимая управляемой операцией неопределенность и нелинейность, при внешнем управлении характеризуемая вложением пространства большего числа измерений в меньшее, позволяет эффективно противостоять *дифференциальным атакам*.

Законы управления операциями задаются соответствующими операторами – ***C-конверторами*** и, как правило, носят периодический характер.

7.4. Регулярные дихотомические генераторы

В итоге, собирая все вместе, а именно – высокую скорость распространения влияния младших битов на старшие, косвенные выходы, переменные коэффициенты и нелинейные управляемые операции регулярного типа, выходные последовательности регулярных *Dh*-генераторов, фактически становятся в своем классе *идеально* функционально сложными и формально подчиняются закону

$$R = F + 2W, \quad \text{равно} \quad R = F \oplus (W \lhd 1), \qquad (19)$$

где F, W – две неизвестные дихотомические последовательности.

Неопределенность, вносимая законом суперпозиции (19), не позволяет по известной *D*-последовательности *R*, однозначно определить поведение составляющих ее последовательностей $\{F, W\}$, равно тому, определить ни одно из внутренних состояний одного или пары порождающих их генераторов. Вследствие возникающей такой неопределенности, при больших платформах генерации n, такие выходные последовательности *R*, по сути, оказываются функционально неразрешимыми по существу, со стороны отдельно взятых старших значащих бит.

Между тем, как это следует из уравнения (7), это не является препятствием к вскрытию таких регулярных генераторов.

Сложность решения этой задачи экспоненциально быстро растет, как 2^{w}, при ***усечении*** w младших значащих бит. Но в этом случае последовательности, формируемые на основе таких усеченных *Dh*-генераторов, утрачивают бесповторные свойства. С ростом числа усекаемых младших значащих бит, *D*-последовательности быстро стремятся к равноповторным, при сравнительно небольших $n \geq 24$, по своим статистическим свойствам практически не отличающихся от *истинно* случайных последовательностей, формируемым на основе наиболее продвинутых криптографических примитивов ***RC4***, ***AES*** и ***ГОСТ***.

По представленному обзору, можно сделать следующие выводы:

1. *Dh*-генераторы, по своим статистическим свойствам и функциональной сложности существенно, $2^{n(n+1)/2}$ против $2^{1,2n}$, превосходят наиболее распространенные, функционирующие на основе регистров сдвига с линейной обратной связью (*LFSR*) линейные рекуррентные генераторы. При аппаратной реализации скорость функционирования таких генераторов, может быть соизмерима со скоростью функционирования генераторов Галуа, сопоставимой с выполнением одной логической операции XOR, независимо от длины используемой платформы генерации.
2. *Dh*-генераторы отличаются высокой производительностью за счет использования всех битов выходного блока, а не одного бита блока, как это предписывается *LFSR*.
3. В отличие от *LFSR*, последовательности, формируемые на основе *Dh*-генераторов, содержат нулевой элемент и отличаются полнотой.
4. Схемы реализации *D*-операторов отличаются простой исполнения и настройки, требуют небольших аппаратных затрат, допускают параллельную одно и много разрядную, включая беспроцессорную аппаратную обработку на любых платформах вычислительных устройств.
5. Последовательности, формируемые на основе *D*-операторов, способны сохранять присущие составляющим их элементам бесповторные свойства, могут иметь любой, не меньший наперед заданного период повторения, характеризуются аналитически не выводимым, непредсказуемым начальным состоянием и функциональной неразрешимостью по существу, со стороны старших значащих бит.
6. *D*-операторы могут иметь открытую, наращиваемую модульную архитектуру и исходя из принципа суперпозиции, способны интегрироваться в большие системы.
7. *D*-операторы носят фундаментальный характер и закладывают основу для развития нелинейной криптографии и построения нелинейных стохастических систем.

Дихотомические генераторы имеют следующие недостатки:

1. *Dh*-генераторы не являются криптографически стойкими. Между тем, это не является препятствием для их использования в качестве эффективных строительных блоков.
2. Неравнозначный вклад битов ключа инициализации генераторов и битов входного потока, связанных с модификатором ***H***, обусловленный однонаправленным характером распространения влияния битов входящих в состав *D*-операторов. Что приводит к усложнению процедуры инициализации генераторов.
3. Стабилизации параметров относительно базовой переменной при переходе дихотомических генераторов в стационарное состояние, что предопределяет существенное сокращение пространства его внутренних состояний.

7.5. Дихотомические операторы и рандомизаторы

Концептуально, ядро линейной стохастической составляют дихотомические операторы и рандомизаторы (Рис.3). Согласно с принципом суперпозиции, в частном случае представляемым формулой (19), дихотомические величины способны порождать новые дихотомические величины.

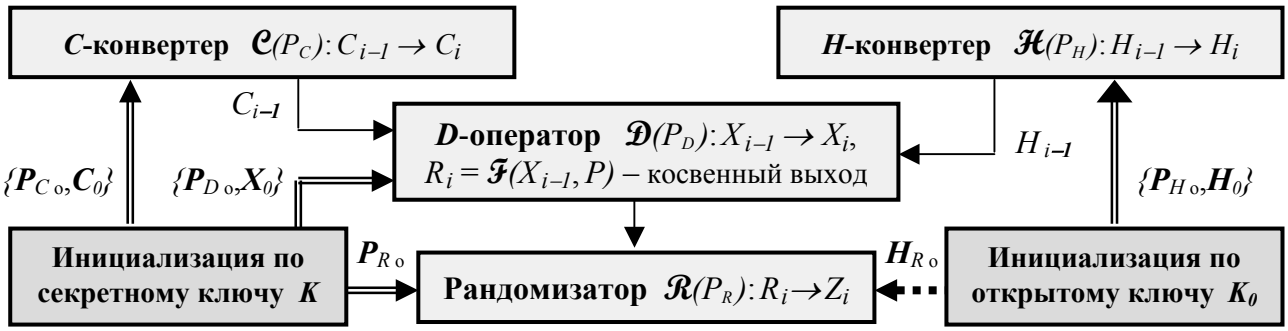


Рис. 3.

В силу свойств присущих регулярным *D*-операторам, младшим битам формируемых на их основе дихотомических последовательностей, присуща существенно выраженная корреляция. Корреляция убывает от младших битов *D*-последовательности, к старшим. По мере убывания корреляции, старшие биты дихотомических величин способны приобретать существенно выраженный недетерминированный, по существу функционально неразрешимый характер.

В этих условиях, получение надежных в статистическом и криптографическом отношении случайных последовательностей может быть осуществлено путем преобразований (усложнений), обеспечивающих на основе принципов рассеяния и перемешивания, выравнивание частотных свойств битов и функционально сложное, неразрешимое сокрытие дихотомических и корреляционных свойств исходных для них *D*-последовательностей.

Осуществление таких стохастических преобразований *D*-последовательностей, включая последовательности, полученные на основе *D*-операторов, производится на основе простых (однораундовых) и мультипликативных (многораундовых) рандомизаторов ***R***.

Как следует из практики, такие рандомизаторы должны удовлетворять следующему, сформулированному по отношению к *D*-последовательностям, ряду требований, если ставятся задачи построения криптографически сильных рандомизационных операторов:

1. Порядок катенации битов элементов преобразуемых последовательностей от раунда к раунду (от итерации к итерации), устанавливаемый оператором, должен обеспечивать равномерное выравнивание частот изменения битов исходных для них *D*-последовательностей.
2. Порядок преобразования должен обеспечивать наиболее высокую, экспоненциально нарастающую от раунда к раунду (от итерации к итерации), лавинную скорость распространения влияния старших значащих битов *D*-последовательностей, на младшие.
3. Порядок преобразования должен задавать существенно выраженное, не приводящее к кластеризации, нарастающее от раунда к раунду (от итерации к итерации) нелинейное преобразование битов. Естественно, в этих условиях, период *T* образованной таким образом последовательности должен быть не менее периода T_n исходной для нее *D*-последовательности.

В зависимости от характера осуществляемых отображений, операторы данного класса ***R*** подразделяются на ***рандомизаторы биективного*** $\boldsymbol{R}^{\circ}$ и ***сюръективного*** $\boldsymbol{R}^{\bullet}$ типа.

7.6. Генераторы ключевого потока

$\boldsymbol{R}^{\circ}$-рандомизаторы используются при построении бесповторных генераторов ключевого потока, так называемых ***RK-генераторов***. Для построения генераторов ключевого потока обычно используются *Dh*-генераторы типа (15), функционально неразрешимые со стороны старших значащих бит.

Учитывая свойства присущие регулярным *D*-операторам, рандомизаторы ***RK***-генераторов должны удовлетворять следующему ряду требований:

1. Порядок катенации битов элементов преобразуемых последовательностей от раунда к раунду (от итерации к итерации), устанавливаемый рандомизатором, должен обеспечивать равномерное выравнивание частот изменения битов исходных для них *D*-последовательностей. В этом случае, за счет надежных в статистическом отношении старших срезов этих после-

довательностей, могут быть достигнуты высокие статистические показатели младших срезов и статистическая надежность ***RK***-генераторов в целом

2. Порядок преобразования должен обеспечивать наиболее высокую, экспоненциально нарастающую от раунда к раунду (от итерации к итерации), лавинную скорость распространения влияния старших значащих битов *D*-последовательностей, на младшие. В этом случае число раундов, необходимое для получения сильных в криптографическом отношении последовательностей, будет минимально.

3. Порядок преобразования должен задавать существенно выраженное, нарастающее от раунда к раунду (от итерации к итерации) нелинейное преобразование битов, зависящее от раундовых ключей или модификаторов, используемых на каждой итерации рандомизатора.

Анализ широкого класса рандомизаторов позволил выделить нелинейно-управляемые операторы, удовлетворяющие представленным выше требованиям, со скоростью функционирования в раунде, соизмеримой со скоростью исполнения двух логических операций XOR, независимо от длины платформы генератора. При этом для получения надежных в статистическом отношении последовательностей обычно требуется не более двух раундов.

Число раундов *g* необходимых для построения сильных в криптографическом отношении ***RK***-генераторов, не велико и приблизительно равно

$$g = 2 \cdot \log_2 (n/2 - \Delta n + 1) + 1 \qquad (0 \le \Delta n \le n/2), \qquad (20)$$

где Δn – число младших вскрываемых бит ***RK***-генератора.

7.7. Нерегулярные дихотомические генераторы

Как было представлено ранее в параграфах 7.2 и 7.3, за счет выбора закона вариации коэффициентов и управления вводимой в состав *D*-оператора нелинейной операции, закон изменения входящих в его состав переменных может носить регулярный и нерегулярный характер.

При внутреннем управлении, а также при управлении от внешних ординарных дихотомических и ламинарных генераторов, *D*-операторы и построенные на их основе *Dh*-генераторы сохраняют присущие им регулярные, дихотомические свойства.

При управлении от внешних дихотомических и ламинарных генераторов контрординарного типа, *LFSR* и других периодических генераторов, закон изменения переменных входящих в состав *D*-оператора приобретает нерегулярный характер. ***Нерегулярные дихотомические генераторы***, иначе ***Gh***-генераторы, построенные на основе нерегулярных *D*-операторов, утрачивают бесповторные и приобретают ***равноповторные свойства***. ***Гарантированный период*** таких генераторов, не меньше наибольшего из периодов всех внешних управляющих генераторов. В общем случае, в зависимости от начального состояния генератора, период формируемой им рандомизационной последовательности может быть и значительно больше.

<u>*Gh*-генераторы имеют следующие преимущества</u>:

1. За счет внешнего управления, гарантированный период *Gh*-генераторов, может существенно превышать период повторения $T_n = 2^n$, соответствующих им *Dh*-генераторов.

2. Удается частично ликвидировать стабилизацию параметров *D*-оператора относительно базовой переменной и существенно увеличить пространство его внутренних состояний с T_n, многократно на величину, равную произведению периодов внешних управляющих периодических генераторов.

3. Достижение функциональной необратимости по существу уравнений *D*-оператора, за счет существенно выраженного взаимно неоднозначного (сюръективного) характера осуществляемых преобразований.

4. Общее улучшение статистических свойств *Gh*-генераторов при вариации коэффициентов образующих их *D*-операторов, за счет придания его переменным статистических свойств внешних управляющих периодических генераторов. Повышение устойчивости к линейным атакам, за счет формального, существенно выраженного нелинейного вложения пространства большего числа измерений, в меньшее.

5. Улучшение статистических свойств *Gh*-генераторов при введении в состав образующих их *D*-операторов нелинейных управляемых операций, за счет сокращение длины и числа протяженных немонотонных участков. Повышение устойчивости к дифференциальным атакам, за счет использования на каждой итерации генератора различных, существенно выраженных нелинейных преобразований.

Gh-генераторы имеют следующие недостатки:

1. Использование непериодических генераторов или периодических генераторов вариации коэффициентов очень малого периода $T << T_n$, особенно в случаях ламинарных и других генераторов, когда период пропорционален длине платформы генерации n, не гарантирует, что при некоторых из начальных условий, пусть и с ничтожно малой вероятностью при больших n, не произойдет вырождения *Gh*-генератора.

2. Наличие протяженного начального переходного участка, неоднородность распределения частот, обусловленная однонаправленным характером рассеяния битов и как следствие, не столь высокое качество генерируемых рандомизационных последовательностей.

3. Неравнозначный вклад битов ключа и битов управляющего входного потока, обусловленный однонаправленным характером распространения влияния битов входящих в состав *D*-операторов.

В качестве примера, на эпюре 5, представлены результаты работы 64-х разрядного *Gh*-генератора с подполем Галуа *GF(2)*, полученного путем последовательных итераций его образующего *D*-оператора (10) с прямым выходом B, при начальных условиях B = P = D = Q = H = 0 и g = 3.

Генератор Галуа устанавливает закон вариации коэффициента $\boldsymbol{H}$, используемого в качестве входа *Gh*-генератора и задается оператором

$$\boldsymbol{H}_i = (\boldsymbol{H}_{i-1} \gg 1) \oplus (\boldsymbol{H}_{i-1} \wedge 1 \;?\; \boldsymbol{H_C} : \boldsymbol{H_N}). \qquad (21)$$

Для исключения вырождения генератора Галуа, постоянные $\{\boldsymbol{H_C},\boldsymbol{H_N}\}$ входящие в состав указанного уравнения вычисляются в зависимости от начального значения $\boldsymbol{H}_0$ коэффициента $\boldsymbol{H}$:

$$\boldsymbol{H_C} = C_G, \qquad \boldsymbol{H_N} = 2^{n-1} \quad \text{при четном } \boldsymbol{H}_0;$$
$$\boldsymbol{H_C} = C_G \vee 2^{n-1}, \qquad \boldsymbol{H_N} = 0 \quad \text{при нечетном } \boldsymbol{H}_0,$$

с константой C_G, задаваемой исходя из образующего примитивного многочлена

$$\Phi(x) = x^{64} + x^4 + x^3 + x^1 + 1,$$

в нашем случае для 64-х битовой платформы генерации, равной $\boldsymbol{C_G} = 0\mathbf{x}D$.

На эпюре заметен характерный переходной вырожденный участок, длиной $(n + Np)$, где Np – число параметров в контуре уравнений генерации.

Побитовый статистический анализ указанного генератора показывает, наличие существенной корреляции между битами 1-го среза, быстро убывающая от среза к срезу. Начиная с 6 среза и выше, заметной корреляции между битами срезов не выявлено.

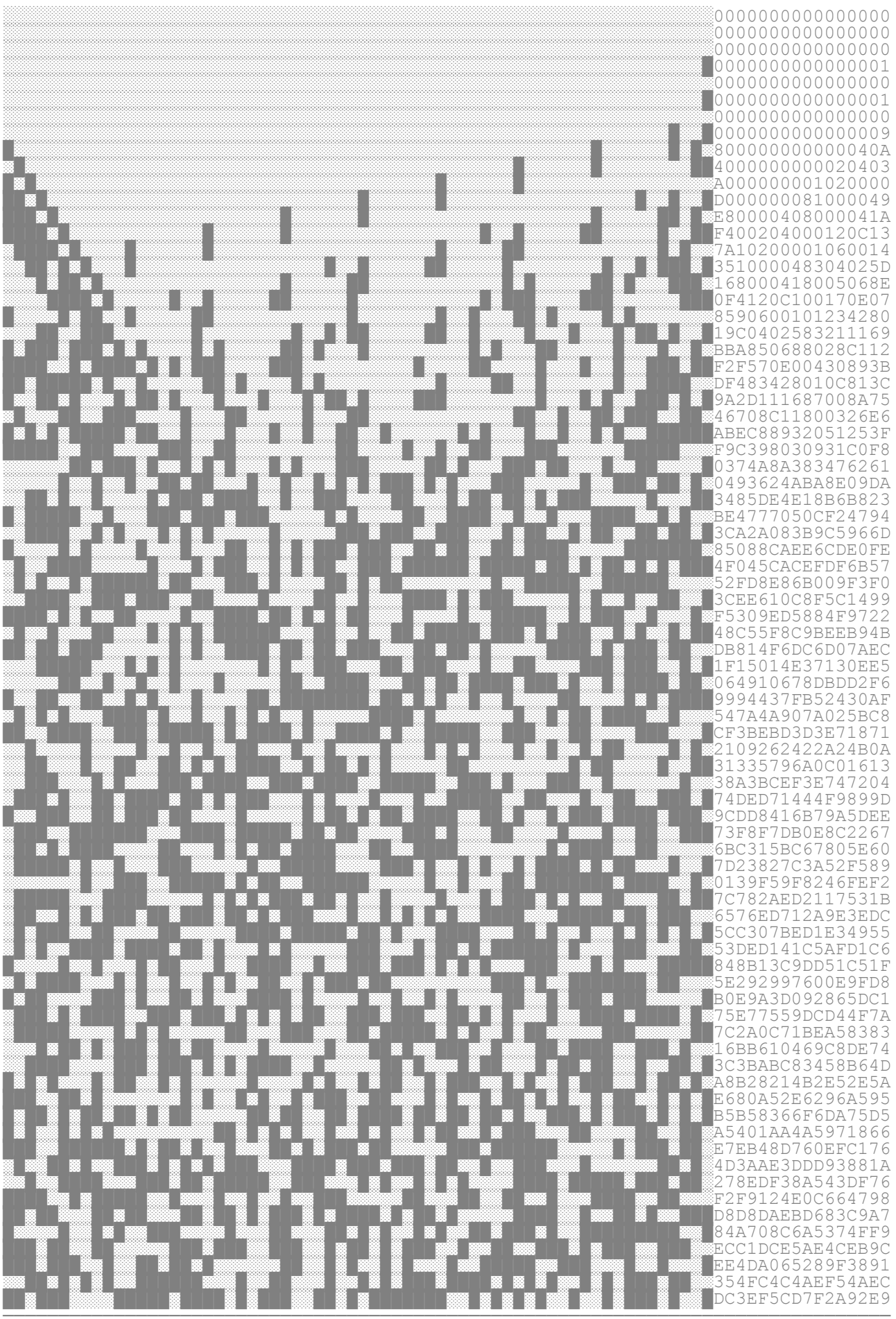
Поэлементный анализ также показывает наличие заметной корреляции между элементами формируемой таким образом рандомизационной последовательности.

Устранение указанного недостатка осуществляется на основе рандомизаторов и односторонних операторов.

7.8. Односторонние операторы и генераторы гаммы

Для придания дихотомическим и другим рандомизационным последовательностям, формируемым на основе регулярных и нерегулярных *D*-операторов, статистических свойств присущих наиболее качественным криптографическим примитивам ***(RC4***, ***AES***, ***ГОСТ)***, равно *идеальному* равномерному закону распределения, используются ***рандомизаторы сюръективного типа*** $\boldsymbol{R}^{\bullet}$.

Эпюра 5. 64-х битовый *Gh*-генератор с подполем Галуа



К $\boldsymbol{R}^{\bullet}$-рандомизаторам предъявляются следующие требования, формулируемые по отношению к преобразованиям исходных для них *D*-последовательностей:

1. Исходя из общих требований предъявляемых к ***RA***-технологиям, скорость функционирования рандомизаторов должна быть сопоставима со скоростью исполнения одной логической операции XOR.

2. Последовательности, формируемые на основе рандомизаторов, должны носить равноповторный характер с периодом T, не менее 2^n, сопоставимым по величине с $e^n \approx 2^{1.443\,n}$, где e – число Эрмита, равное 2.71828… .

3. Для получения высоких статистических показателей, порядок катенации битов элементов преобразуемых последовательностей от раунда к раунду (от итерации к итерации), устанавливаемый рандомизатором, должен обеспечивать равномерное выравнивание частот изменения битов исходных для них *D*-последовательностей.

4. Порядок преобразования должен обеспечивать наиболее высокую, экспоненциально нарастающую от раунда к раунду (от итерации к итерации), лавинную скорость распространения влияния старших значащих битов *D*-последовательностей, на младшие.

5. Порядок преобразования должен задавать однозначно необратимое и существенно выраженное, нарастающее от раунда к раунду (от итерации к итерации) нелинейное преобразование битов.

Рассмотрим один из наиболее простых рандомизационных операторов данного класса, предназначенный для придания дихотомическим последовательностям и связанным с ними дихотомическим величинам указанных свойств.

Закон преобразования дихотомической переменной $\boldsymbol{D}$, может быть задан линейным рекуррентным уравнением:

$$\boldsymbol{G}_i = \boldsymbol{rot}(\boldsymbol{D}_{i-1}, \boldsymbol{S}_C) \oplus \boldsymbol{rot}(\boldsymbol{G}_{i-1}, \boldsymbol{S}_G), \qquad (22)$$

при начальном условии $\boldsymbol{G}_0$ рандомизационной переменной $\boldsymbol{G}$, с операциями циклического сдвига $\boldsymbol{rot} = \{\boldsymbol{rotL}, \boldsymbol{rotR}\}$, влево или вправо, на $\boldsymbol{S}_C$ и $\boldsymbol{S}_G$ значащих бит, соответственно.

Формируемые на основе данного оператора результирующие последовательности $\{\boldsymbol{G}_i\}$ удовлетворяют представленным выше требованиям и носят равноповторный характер, при смещении $\boldsymbol{S}_G = \boldsymbol{\hbar}_n$ равным характеристическому $\boldsymbol{\hbar}_n$ – ближайшему простому к n/e, не кратному n. Последовательность не смещена, при $\boldsymbol{S}_C = \boldsymbol{\eta}_n$ равным характеристическому $\boldsymbol{\eta}_n$ – максимальному, меньшему $n/2$, взаимно простому с n. При равенстве смещений, характеристическое смещение $\boldsymbol{\eta}_n$ понижается до ближайшего, взаимно простого с n.

Выполняя обращение уравнения (22), имеем:

$$\boldsymbol{D}_{i-1} = \boldsymbol{rot}(\boldsymbol{G}_i \oplus \boldsymbol{rot}(\boldsymbol{G}_{i-1}, \boldsymbol{S}_G), n - \boldsymbol{S}_C). \qquad (23)$$

Формально из обращения следует сюръективный характер преобразования (22), при неизвестном предшествующем значении $\boldsymbol{G}_{i-1}$ переменной $\boldsymbol{G}$. На самом деле, этот вывод несостоятелен, т. к. фактически $\boldsymbol{G}_{i-1}$ всегда нам известно, или может быть определено.

Для придания рандомизатору действительно однозначно необратимых и существенно выраженных нелинейных свойств, в уравнение (22) можно ввести нелинейную управляемую операцию, следующим образом:

$$\boldsymbol{G}_i = \boldsymbol{G}^{\circ}_{i-1} \oplus \boldsymbol{G}^{\bullet}_{i-1}, \quad \boldsymbol{G}^{\circ}_{i} = \boldsymbol{rot}(\boldsymbol{D}_{i-1}, \boldsymbol{S}_C) \oplus \boldsymbol{rot}(\boldsymbol{G}^{\circ}_{i-1}, \boldsymbol{S}_G), \qquad (24)$$

$$\boldsymbol{G}^{\bullet}_{i} = (A_{i-1} \curlywedge \boldsymbol{G}^{\bullet}_{i-1}) \oplus (\boldsymbol{B}_{i-1} \curlywedge (A_{i-1} \oplus \boldsymbol{G}^{\bullet}_{i-1})) \; - \text{ внутреннее управление } \; \boldsymbol{G}^{\bullet} = A \curlywedge^{B} \boldsymbol{G}^{\bullet},$$

либо

$$\boldsymbol{G}^{\bullet}_{i} = (A_{i-1} \curlywedge \boldsymbol{G}^{\bullet}_{i-1}) \oplus (\boldsymbol{E}_{i-1} \curlywedge (A_{i-1} \oplus \boldsymbol{G}^{\bullet}_{i-1})) \; - \text{ внешнее управление } \; \boldsymbol{G}^{\bullet} = A \curlywedge^{E} \boldsymbol{G}^{\bullet},$$

где $\boldsymbol{E}$ – генератор Галуа или другой n-разрядный периодический генератор.

Композиция *D*-оператора и рандомизатора, образуют ***однонаправленный рандомизационный оператор*** – *W*. В зависимости от типа используемого *D*-оператора, однонаправленный рандомизационный *W*-оператор может быть ***регулярным*** и ***нерегулярным***.

В результате последовательных итераций *W*-оператора, проводимых на основе соответствующего оператора, порождается равноповторная последовательность, именуемая ***гаммой***, а сам оператор именуется ***генератором гаммы***.

В целях гарантированного придания генератору необратимых свойств, например как это диктуется в случае (22)-(23), и как следствие, большей устойчивости к функциональным, аналитическим и корреляционным атакам, направленных на вскрытие его внутреннего состояния, используется не прямой $\boldsymbol{G}_{i-1}$, а ***косвенный*** $\boldsymbol{R}_i$ ***выход генератора***:

$$\boldsymbol{R}_i = \boldsymbol{G}_{i-1} \oplus \boldsymbol{V}_{i-1}, \qquad (25)$$

где $\boldsymbol{V}$ – одна из рандомизационных переменных, входящих в состав *D*-оператора.

На эпюре 6, представлены результаты работы регулярного 64-х разрядного генератора гаммы с прямым выходом B, при начальных условиях $G = B = P = D = Q = H = 0$ и $g = 3$, с рандомизатором (22). Даже не вооруженным глазом видны отличия *Gh*-генератора (Эпюра 5) и генератора гаммы, особенно сильные со стороны младших значащих бит.

Побитовый статистический анализ регулярных генераторов гаммы данного типа, показывает, наличие существенной корреляции между битами срезов, при длине платформы генерации до 24 бит, включительно. Начиная с длины платформы 25 бит и выше, заметной корреляции между битами срезов не выявлено.

Поэлементный анализ прямого выхода G, показывает наличие заметной корреляции до длины платформы генерации в 23 бит. При использовании косвенного выхода $R = G \oplus Q$, критическая длина платформы генерации составляет 18 бит. Для более длинных платформ, заметной корреляции между элементами формируемой таким образом рандомизационной последовательности, не выявлено.

Объединим результаты примеров параграфов 7.7 и 7.8, 64-х разрядным нерегулярным – конвертируемым см. Рис.3, так называемым генератором гаммы с подполем Галуа.

На представленной ниже эпюре 7, приведены результаты работы такого генератора гаммы, при начальных условиях $G = B = P = D = Q = H = 0$ и $g = 3$, с рассмотренным в параграфе 7.8 генератором Галуа и рандомизатором (22).

Побитовый статистический анализ указанного генератора показывает, наличие существенной корреляции между битами срезов, при длине платформы генерации до 12 бит, включительно.

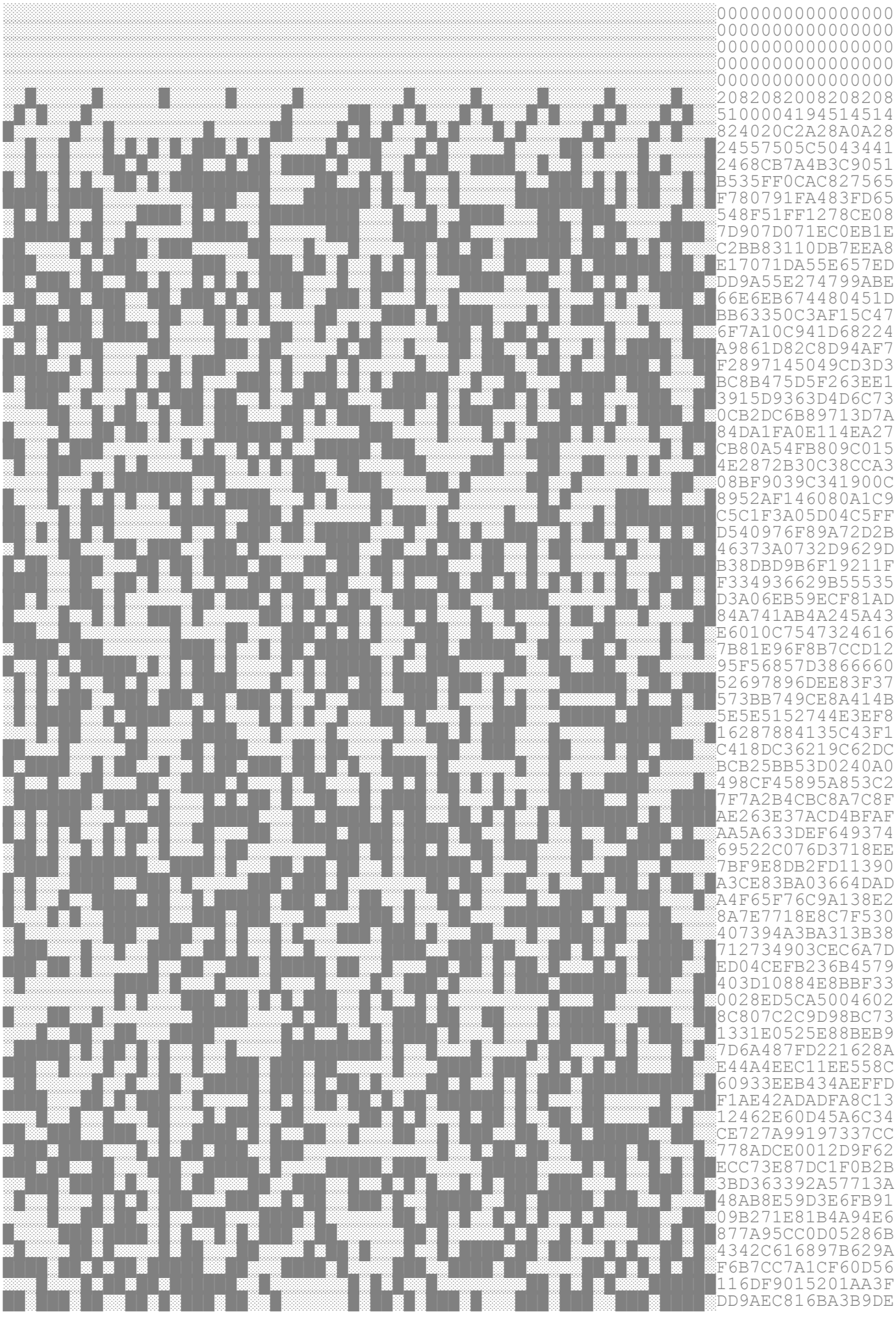
Поэлементный анализ, показывает наличие существенной корреляции до длины платформы генерации в 11 бит. Для более длинных платформ, заметной корреляции между битами срезов и элементами формируемой таким образом рандомизационной последовательности, не выявлено.

В силу последнего, далее будем придерживаться нерегулярных генераторов гаммы с образующим *D*-оператором типа (17), законом вариации (конвертации) входящего в их состав коэффициента $\boldsymbol{H}$, имеющим период не менее $2^n - 1$ и рандомизатором типа (22).

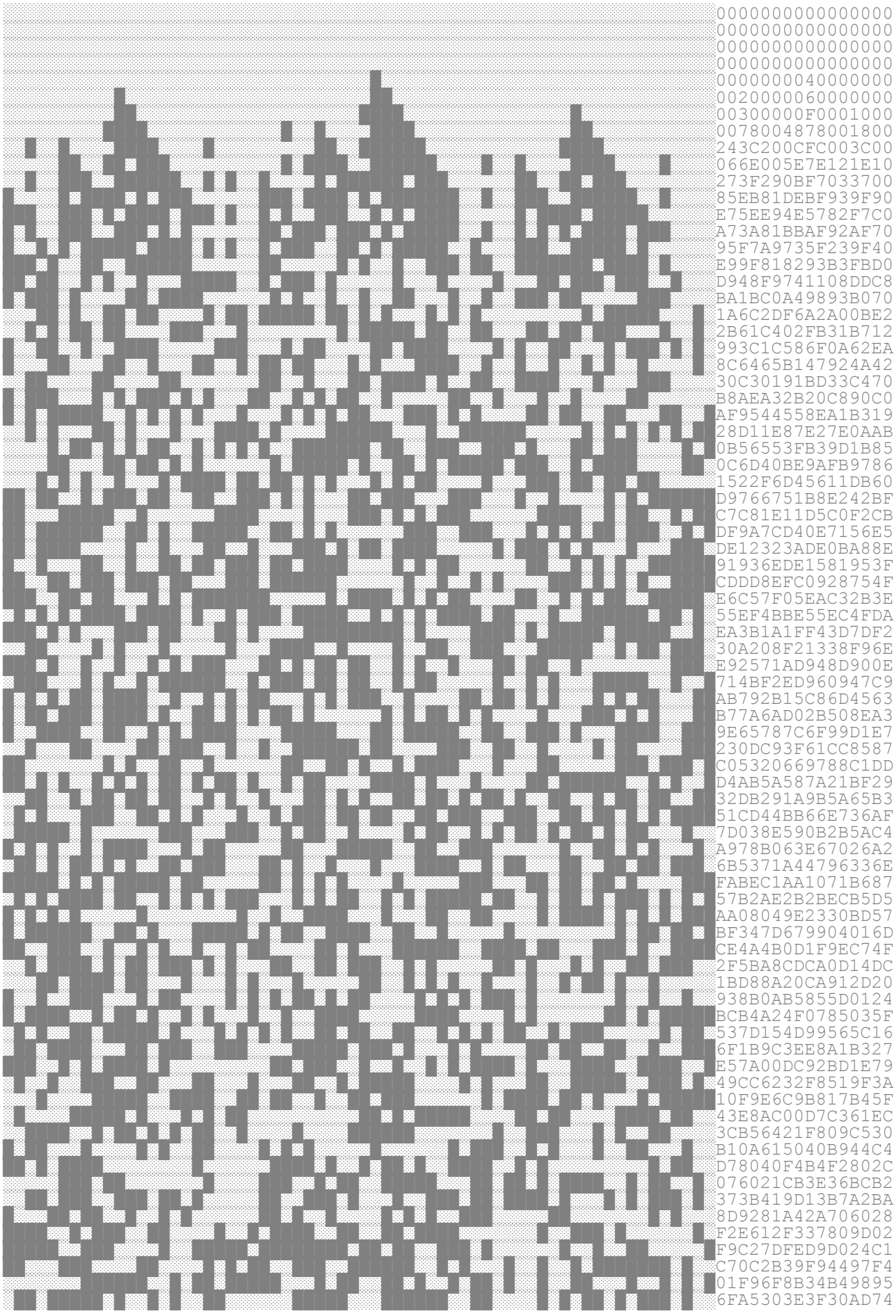
По структуре построения (Рис.3), представленный генератор гаммы допускает многократное использование секретных ключей $\boldsymbol{K}$, за счет возможности перестройки работы входящего в его состав *D*-оператора по открытому ключу $\boldsymbol{K}_0$ (синхропосылки).

Исходя из общих криптографических требований, для того чтобы это было возможно, необходима существенная зависимость выходного потока от изменения одного из битов начального значения коэффициента $\boldsymbol{H}_0$, устанавливаемого по открытому ключу $\boldsymbol{K}_0$.

Эпюра 6. 64-х битовый регулярный генератор гаммы



Эпюра 7. 64-х битовый нерегулярный генератор гаммы с подполем Галуа



Генераторы гаммы имеют следующие достоинства:

1. За счет внешнего управления, гарантированный период генераторов гаммы, может существенно превышать период повторения $T_n = 2^n$, соответствующих им *Dh*-генераторов.

2. Возможность многократного использования секретных ключей. Многократное увеличение пространства внутренних состояний с T_n, на величину, равную произведению периодов внешних управляющих периодических генераторов.

3. Высокая статистическая надежность рандомизационных последовательностей формируемых генераторами, особенно при использовании особо эффективных механизмов выравнивания частот.

4. Достижение функциональной необратимости по существу уравнений генератора. Высокая устойчивость к корреляционным и линейным атакам.

5. Устойчивость к дифференциальным атакам, особенно в условиях введения управляемых нелинейных операций.

Генераторы гаммы имеют следующие особенности:

1. Использование непериодических генераторов и периодических генераторов вариации коэффициентов очень малого периода, может приводить к эпизодическому, пусть и крайне редкому, но все же вырождению генератора.

2. Усложнение процедуры инициализации генератора, необходимое для обеспечения равнозначности вклада всех битов ключа.

7.9. Однонаправленные операторы и рандомизационные агрегаты

Мультипликативная композиция $W \circ W \circ \ldots W$ из q одинаковых односторонних операторов W, образует мультипликативно степенной, ***однонаправленный оператор*** W^q, степени q. Проще говоря, однонаправленный *(рандомизационный)* оператор выполняет не одно, а конечное q число последовательных преобразований, часто называемых ***раундами***.

В зависимости от типа используемого *D*-оператора, порождаемый им рандомизационный однонаправленный W^q-оператор может быть ***регулярным*** и ***нерегулярным***. W^q-оператор в композиции с оператором выхода, собственно следуя системным принципам как и сам оператор, именуются ***рандомизационным*** или ***W^q-агрегатом***.

В целях гарантированного придания оператору данного типа необратимых свойств, как это было оговорено ранее в (19), используется не прямой $\boldsymbol{G}_q$, а ***косвенный $\boldsymbol{Z}_q$ выход агрегата***:

$$\boldsymbol{Z}_q = \boldsymbol{G}_q \oplus \boldsymbol{V}_q, \qquad (26)$$

где $\boldsymbol{V}_q$ – результирующее значение одной из рандомизационных переменных входящих в состав образующего *D*-оператора агрегата, после завершения его q итераций.

По определению, однонаправленные операторы и агрегаты, в соответствии с образующим его односторонним оператором W, могут иметь один или несколько двоичных конвертируемых или неконвертируемых входов $\boldsymbol{H_0}$.

Функциональная схема построения $\boldsymbol{W}^q$-агрегатов показана на Рис. 4.

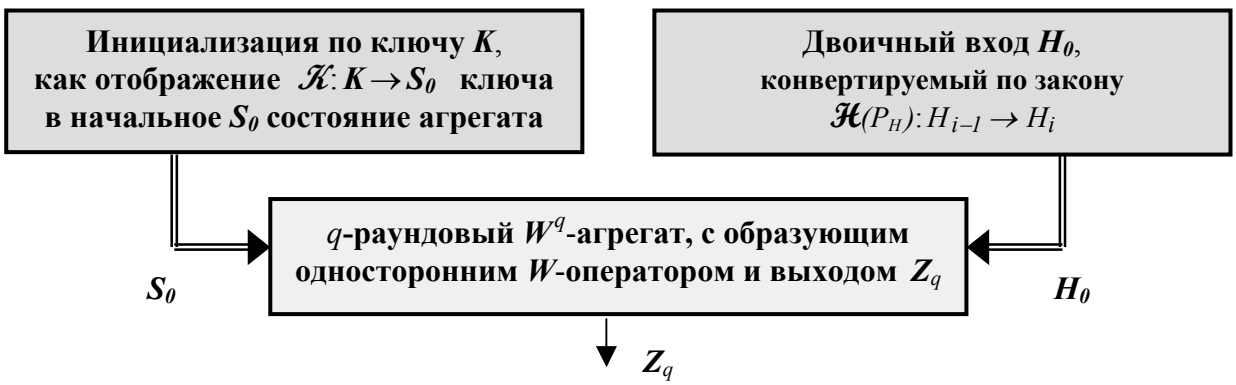


Рис. 4. Функциональная схема построения $\boldsymbol{W}^q$-агрегатов

W^q-агрегаты, определенные на множестве $\boldsymbol{m}$ двоичных входов – модификаторов $\boldsymbol{H}$ и множестве $\boldsymbol{n}$ выходов $\boldsymbol{Z}$, порождают семейство однонаправленных псевдослучайных ***PR-операторов*** $\boldsymbol{\mathcal{F}_m = \{f_K(H)\}_{K \in \Omega_K}}$ (Рис.6), а при одном выходе ***PR-функций*** $\boldsymbol{\mathcal{F} = \{f_K(H)\}_{K \in \Omega_K}}$ (Рис.5), определенных на множестве состояний $\boldsymbol{\Upsilon = \Upsilon_H \times \Upsilon_K}$.

Здесь, $\boldsymbol{\Omega_K = \{K\}}$ и $\boldsymbol{\Omega_H = \{H\}}$ – множества всех допустимых ключей $\boldsymbol{K}$ и модификаторов $\boldsymbol{H}$, а $\boldsymbol{\Upsilon_H}$ и $\boldsymbol{\Upsilon_K}$ пространства модификации и состояний, соответственно, формируемые $\boldsymbol{\Upsilon_H = \mathcal{H}(\Omega_H)}$ и $\boldsymbol{\Upsilon_K = \mathcal{K}(\Omega_K)}$ по пространство модификаторов $\boldsymbol{\Omega_H}$, и ключевому пространству $\boldsymbol{\Omega_K}$.

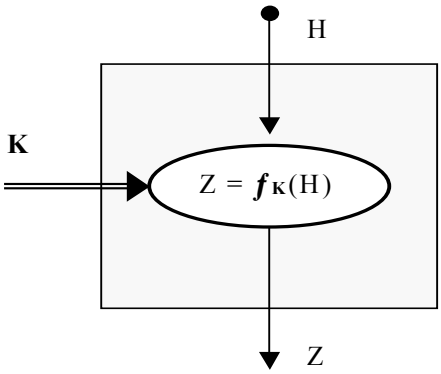


Рис. 5. Одномерная ***PR***-функция

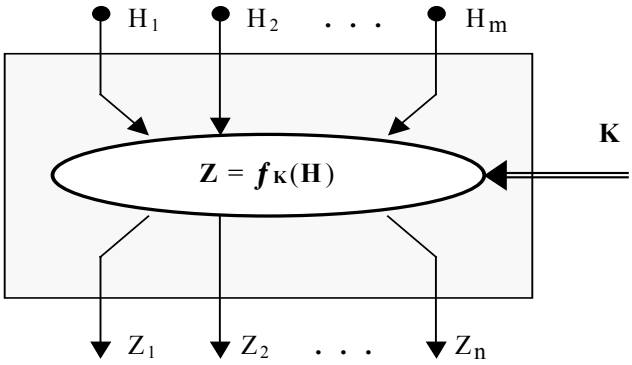


Рис. 6. Многомерный ***PR***-оператор

На основе W^q-агрегатов, при открытом ключе $\boldsymbol{K}$ могут быть построены, соответственно, одномерные и многомерные ***хеш-функции и операторы***, при секретном ключе – ***MAC-функции и операторы*** выработки показателей контроля целостности информации.

По открытым ключам – модификаторам (синхропосылки) $\boldsymbol{H_0}$, устанавливаемых прямо или по открытому ключу $\boldsymbol{K_0}$, можно перестраивать работу W^q-агрегатов (Рис.4).

Исходя из общих криптографических требований, в этом случае необходимо, чтобы несущественные линейные изменения $\boldsymbol{H_0}$ на входе W^q-агрегатов, приводили к существенным нелинейным изменениям на их выходе.

Проверка нелинейности выхода W^q-агрегата может быть проведена на основе имитационно-статистической модели, путем линейной итерации входа $\boldsymbol{H_i = \{C_{Li}, C_{Ri}\}}$, задаваемой лево $\boldsymbol{C_L}$ (ординарным) или право $\boldsymbol{C_R}$ направленными единичными счетчиками, при суммировании, начиная с $\boldsymbol{C_0 = 0}$, в направлении от младших битов к старшим и от старших битов к младшим битам входа оператора (Рис.8). При этом начальное состояние агрегата S_0 варьируется $\boldsymbol{\mathcal{K}: K \rightarrow S_0}$ в ключевом пространстве $\boldsymbol{\Omega_K}$ и восстанавливается каждый раз по фиксированному ключу $\boldsymbol{K}$, перед началом формирования каждого его очередного i-элемента.

Принимается – изменения выхода агрегата носят существенно нелинейный характер, если формируемые на его основе имитационной модели двоичные последовательности $\boldsymbol{Z}$ и составляющие их срезы статистически надежны и, соответственно, равномерно распределены и при этом $q < n$. Здесь n – длина платформы агрегата.

Результаты поэлементного статистического анализа нелинейности W^q-агрегата, построенного на основе рассмотренного в предыдущем параграфе одностороннего W-оператора с подполем Галуа, с прямым выходом и 32-х битовой платформой генерации, показывают наличие заметной при 16 раундах для лево $\boldsymbol{C_L}$ и 28 раундов для и право $\boldsymbol{C_R}$ направленных вариантов реализации счетчиков.

При тех же условиях и качественных результатах, побитовый анализ дает 18 раундов и 26 раундов, для $\boldsymbol{C_L}$ и $\boldsymbol{C_R}$ счетчиков, соответственно.

Такая заметная поляризация результатов, как упоминалось неоднократно, обусловлена неравнозначным вкладом битов входного потока, вносимым D-оператором.

Устранить указанный недостаток оказалось возможным на основе новой конфигурации генераторов в GF(2).

Построенные на основе этой конфигурации генераторы, отличаются от генераторов в конфигурации Галуа – близкой к лавинной скорости распространения влияния битов.

Указанные генераторы задаются уравнением:

$$\boldsymbol{H}_i = (\boldsymbol{H}_{i-1} \vee \boldsymbol{P}_H) \oplus \boldsymbol{rot}(\boldsymbol{H}_{i-1}, \boldsymbol{S}_H) \oplus \{\boldsymbol{P}_1 : \boldsymbol{p}_i = 1, \boldsymbol{P}_0 : \boldsymbol{p}_i = 0\}, \qquad (27)$$

при $\boldsymbol{p}_i = \boldsymbol{P}_S \wedge \boldsymbol{H}_{i-1}$ и начальных условиях $\boldsymbol{H}_0$, с операцией циклического сдвига $\boldsymbol{rot} = \{\boldsymbol{rotL}, \boldsymbol{rotR}\}$ влево или вправо на фиксированное число $\boldsymbol{S}_H$ значащих бит и константами $\boldsymbol{P} = \{\boldsymbol{P}_H, \boldsymbol{P}_S, \boldsymbol{P}_1, \boldsymbol{P}_0\}$. Смещение $\boldsymbol{S}_H$, должно быть взаимно простым с n и для достижения наибольшей скорости распространения влияния битов и принимается равным характеристическому $\hbar_n$ или η_n, введенным в (22). Константы $\boldsymbol{P}$ подбираются на основе специально разработанной методики, исходя из условия, что последовательность, формируемая генератором, есть M-последовательность в GF(2) с периодом $2^n - 1$.

В силу особенностей построения, генераторы данного типа именуются ***турбулентными*** или ***Tb-генераторами***. В зависимости от направления циклического сдвига, ***Tb***-генераторы могут быть лево или право направленными. При аппаратной реализации, скорость функционирования ***Tb***-генераторов, также как и генераторов Галуа, соизмерима со скоростью исполнения одной логической операцией XOR.

Для примера, на эпюре 8, в первой колонке представлены результаты работы 32-х разрядного генератора Галуа (21), а во второй, право направленного ***Tb***-генератора (27), при $S_H = 11$, $P_H = 0x8800$, $P_S = 0x1$, $P_1 = 0x8800$, $P_0 = 0x800$ и нулевых начальных условиях $H_0 = 0$.

Представленный в примере ***Tb***-генератор характеризуется 17-ти членным примитивным образующим многочленом (32,31,29,26,24,23,21,18,16,14,12,10,8,6,4,2,0) высокой плотности, отличающийся от *LFSR* более сильно выраженным недетерминированным характером поведения и высокой скоростью распространения влияния битов.

Результаты поэлементного имитационно-статистического анализа нелинейности представленного выше 32-х разрядного агрегата, с ***Tb***-генератором в составе ***H***-конвертера (Рис.8), вместо генератора Галуа, показывают наличие заметной корреляции при 17 раундах как для лево $\boldsymbol{C}_L$, так для право $\boldsymbol{C}_R$ направленных вариантов реализации счетчиков.

При тех же условиях и качественных результатах, побитовый анализ дает 18 раундов, для обоих типов счетчиков. Как видно, поляризация результатов исчезла, в результате выравнивания вкладов битов входного потока.

Полученные оценки имитационно-статистического анализа нелинейности распространяются и на генераторы гаммы и равноповторные генераторы ключевого потока, при определении число холостых итераций необходимых для преодоления переходного участка и выхода генераторов в безопасный рабочий режим.

Рандомизационные агрегаты с косвенным выходом (26) – $\boldsymbol{Z}_q = \boldsymbol{G}_q \oplus \boldsymbol{V}_q$, после завершения q раундов, гарантирующих установленный уровень криптографической безопасности и модификации выходной переменной $\boldsymbol{G}_q = \boldsymbol{G}_q \oplus \boldsymbol{W}_q$, где $\boldsymbol{W}_q$ – рандомизационная переменная D-оператора $(\boldsymbol{W}_q \neq \boldsymbol{V}_q)$, допускают перевод в режим поточного шифрования n-битовых блоков данных $\boldsymbol{I}_i$

$$\boldsymbol{O}_i = \boldsymbol{G}_{q+i} \oplus \boldsymbol{I}_i \qquad (i = \overline{1, m}) \qquad (28)$$

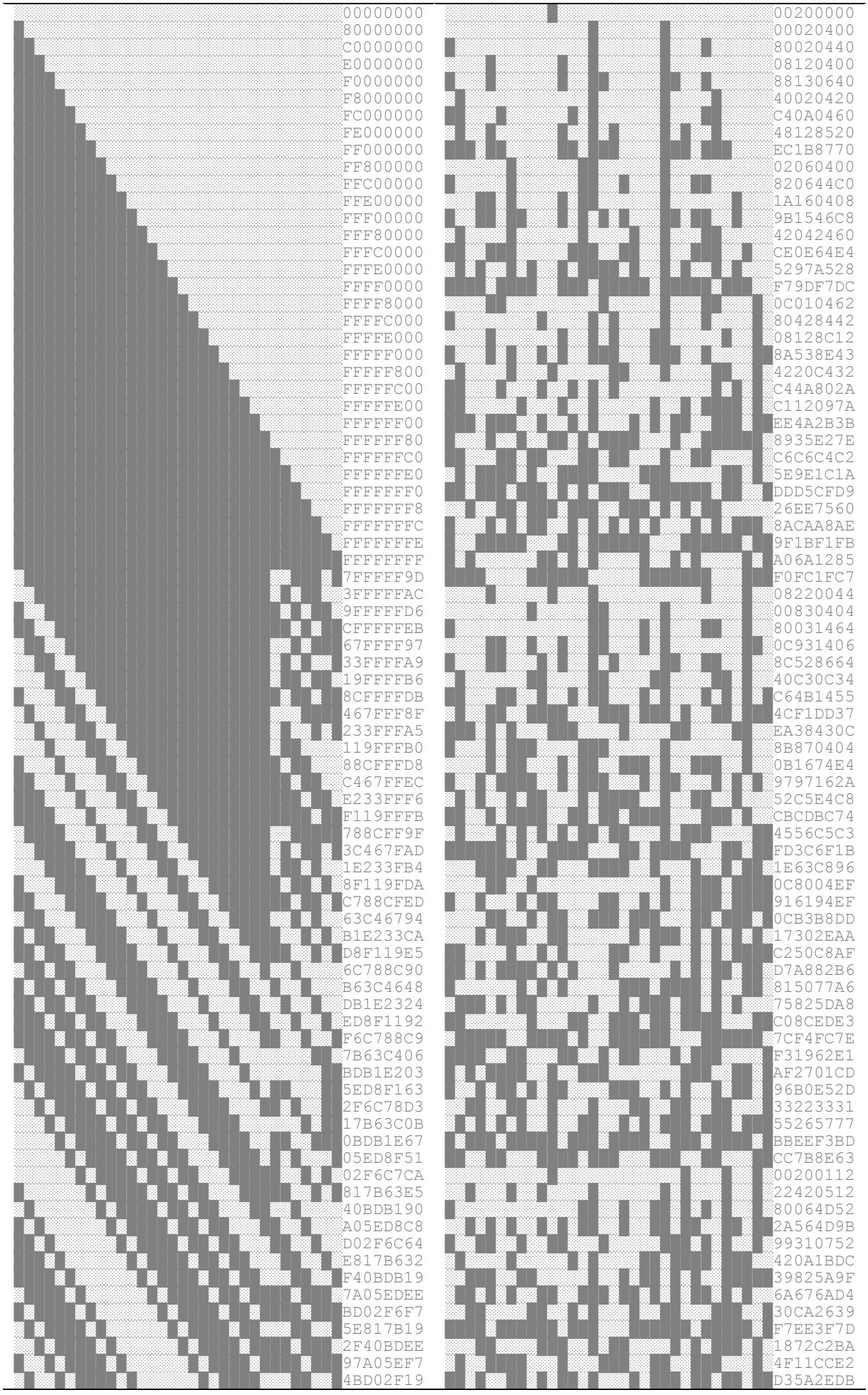
или режим расшифрования поступающей информации $\boldsymbol{O}_i$

$$\boldsymbol{I}_i = \boldsymbol{G}_{q+i} \oplus \boldsymbol{O}_i,$$

но при этом, число шифрируемых блоков m не должно сказываться на общей криптографической стойкости агрегата.

Представленный здесь типичный вариант реализации агрегатов с ***Tb***-генератором, D-оператором (17) и рандомизатором (22), вынесен на ***открытое обсуждение*** и детальную криптографическую экспертизу.

Эпюра 8. 32-х битовый генератор Галуа и турбулентный генератор



8. Типичный пример реализации агрегата и его анализ

Типичный, открытый для обсуждения вариант реализации рандомизационного агрегата в составе Протокола односторонней аутентификации, задается *D*-оператором (17)

$$B_i = B_{i-1} \oplus P_{i-1}, \quad A_i = (2^{\boldsymbol{q}} \cdot A_{i-1}) \oplus Q_{i-1}, \quad P_i = (2^{\boldsymbol{g}} \cdot A_{i-1} \vee \boldsymbol{H}^{\bullet}) \oplus D_{i-1},$$
$$Q_i = B_{i-1} \oplus \boldsymbol{H}^{\circ}, \quad D_i = (2 \cdot (A_{i-1} \wedge P_{i-1})) \vee 1 \quad (\boldsymbol{g} \geq 2, \boldsymbol{q} = 2 \cdot \boldsymbol{g} + 1),$$

при

$$\boldsymbol{H}^{\bullet} = \boldsymbol{H} \bmod 2^{\boldsymbol{g}}, \quad \boldsymbol{H}^{\circ} = \boldsymbol{H}^{\bullet} \oplus \boldsymbol{H},$$

с переменным коэффициентом $\boldsymbol{H}$,

$$\boldsymbol{H}_i = (\boldsymbol{H}_{i-1} \vee \boldsymbol{P}_H) \oplus \boldsymbol{rot}(\boldsymbol{H}_{i-1}, \boldsymbol{S}_H) \oplus \{\boldsymbol{P}_1 : \boldsymbol{p}_i = 1, \boldsymbol{P}_0 : \boldsymbol{p}_i = 0\},$$

задаваемым ***Tb***-генератором (27) и включает в себя рандомизатор (22)

$$\boldsymbol{G}_i = \boldsymbol{rot}(\boldsymbol{D}_{i-1}, \boldsymbol{\eta}_n) \oplus \boldsymbol{rot}(\boldsymbol{G}_{i-1}, \boldsymbol{\hbar}_n),$$

с операциями циклического сдвига $\boldsymbol{rot} = \{\boldsymbol{rotL}, \boldsymbol{rotR}\}$, влево или вправо, на $\boldsymbol{\eta}_n$ и $\boldsymbol{\hbar}_n$ значащих бит, равных максимальному, меньшему $n/2$, взаимно простому с n и ближайшему простому к n/e, не кратному n, соответственно. При равенстве смещений, характеристическое смещение $\boldsymbol{\eta}_n$ понижается до ближайшего, взаимно простого с n.

В качестве выхода $\boldsymbol{Z}_r = \boldsymbol{G}_r$ агрегата после завершения $\boldsymbol{r}$ раундов, используется так называемый прямой выход $\boldsymbol{G}_r$ рандомизатора $\boldsymbol{R}^{\bullet}$. Алгоритм допускает существенное усиление за счет использования не прямого $\boldsymbol{G}_r$, а косвенного $\boldsymbol{Z}_r = \boldsymbol{G}_r \oplus \boldsymbol{V}_r$ выхода агрегата. Здесь $\boldsymbol{V}_r$ – результирующее значение одной из рандомизационных переменных входящих в состав образующего *D*-оператора агрегата, после завершения его $\boldsymbol{r}$ итераций.

8.1. Алгоритм односторонней аутентификации

Представленный вариант реализации рандомизационного агрегата, способен порождать семейство односторонних псевдослучайных функций, упомянутых в разделе 7.9, как наиболее сильных для использования в Протоколах аутентификации.

Алгоритм аутентификации построенный на его основе, имеет следующий вид.

Входные данные: $\boldsymbol{K}$ – секретный ключ аутентификации;
$\boldsymbol{R}$ – открытый маркер, n-битный случайный вектор, выдаваемый верификатором.

Алгоритм:

1 шаг:

- Инициировать ключом $\boldsymbol{K}$, n-битные регистры A,B,D,P,Q,G
  (можно считать ключ составляет эти 6 регистров, т.е. имеет длину $\boldsymbol{6 \cdot n}$ бит);
- Инициализировать значением $\boldsymbol{R}$ регистр H.

2 шаг:

Выполнить $\boldsymbol{r}$ раз следующую последовательность преобразований (в командах языка СИ):

```
G = RotR(A, η_n) ^ RotR(G, ħ_n);                    // R•-рандомизатор
Z = A & P;
D = D ^ ((A << 3) | (H & 0x7));
A = Q ^ (A << 7 );
Q = B ^ (H & 0xFFFFFFF8);                           // D-оператор
B = B ^ P;
P = D;
D = (Z << 1) | 0x1;
H = ( H | 0x8800) ^ RotR(H,11) ^ ( H & 0x1 ? 0x8800 : 0x800);   // Tb-генератор
```

или равнозначным безусловным оператором

H = (H | 0x8800) ^ **RotR**(H,11) ^ ((H & 0x1) << 15) ^ 0x800;

где Z – вспомогательный *n*-битный регистр,
RotR(B,s) – циклический сдвиг вправо двоичного вектора B на ***s*** бит.

Выход: итоговое значение регистра G, которое верификатор будет сравнивать со своим вычисленным значением.

Задача. Оценить сложность и восстановить начальные состояния регистров A,B,D,P,Q и G, по различным *откликам* ***G*** на открытые маркеры – *запросы* ***R*** выбираемые нападающим.

При использовании косвенного выхода ***G*** ^ ***D***, требуется несущественная модернизация *D*-оператора:

```
Z = A & P;
D = ((D << 1) | 0x1) ^ ((A << 3) | (H & 0x7));      вместо   D = D ^ ((A << 3) | (H & 0x7));
A = Q ^ (A << 7 ); Q = B ^ (H & 0xFFFFFFF8);
B = B ^ P; P = D;
D = Z;                                               вместо   D = (Z << 1) | 0x1.
```

8.2. Криптографический анализ алгоритма

Разработка схемы атаки и анализ криптографических показателей представленного примитива, рассчитанного на 32-х разрядные платформы аутентификации радиочастотных (**RF**) меток, используемых в системах ***радиочастотной сертификации***, при циклических сдвигах $\eta_n = 15$ и $\hbar_n = 11$, не специфицированных выше, проведена кандидатом физико-математических наук, ведущим специалистом фирмы **ЛАН Крипто**, Ивановым Александром Геннадьевичем.

Для построения метода имитации и клонирования электронной метки рассматривается, как меняется отклик метки при изменении запроса верификатора.

Возьмем два запроса верификатора h и h', отличающихся на величину h_0, т.е.

$$h' = h + h_0.$$

Будем обозначать состояния регистра X ($X = H, A, B, D, P, Q, G$) после i ($i = 0,1,2,\ldots16$) шагов вычисления на запросе h через x_i, а на запросе h' – через x'_i. Определим X_i как разность значений x_i и x'_i, т.е. $X_i = x_i + x'_i$ для X = H, A, B, D, P, Q, G.

Таким образом, перед началом вычислений имеем:

$$H_0 = h_0,\ D_0 = P_0 = B_0 = Q_0 = A_0 = G_0 = 0. \qquad (29)$$

В соответствии со схемой вычисления значения D_i, P_i, B_i, Q_i, A_i и G_i выражаются через предшествующие значения и состояния регистров a_{i-1} и p_{i-1} по формулам:

$$\begin{aligned}
D_i &= \left(a_{i-1} \,\&\, P_{i-1} + A_{i-1} \,\&\, p_{i-1} + A_{i-1}P_{i-1}\right) << 1 = \overline{1}\,a^1_{i-1}P^1_{i-1} + \overline{1}\,A^1_{i-1}p^1_{i-1} + \overline{1}\,A^1_{i-1}P^1_{i-1} \\
P_i &= D_{i-1} + 7H_{i-1} + \left(A_{i-1} << 3\right) = D_{i-1} + 7H_{i-1} + \overline{7}\,A^3_{i-1} \\
B_i &= B_{i-1} + P_{i-1} \\
Q_i &= B_{i-1} + \overline{7}H_{i-1} \\
A_i &= Q_{i-1} + \left(A_{i-1} << 7\right) = Q_{i-1} + \overline{0x7F}\,A^7_{i-1} \\
G_i &= \left(G_{i-1} \lhd 21\right) + \left(A_{i-1} \lhd 17\right) = G^{21}_{i-1} + A^{17}_{i-1}
\end{aligned} \qquad (30)$$

Здесь верхний индекс указывает величину циклического сдвига вектора влево $\lhd$, а черта сверху шестнадцатеричной константы – инвертирование разрядов константы.

Приведенные формулы показывают, что все состояния регистров выражаются через значения a_1, a_2, … ; p_2, p_3, … и H_0, H_1, … . Применительно к итоговому состоянию регистра G мы получаем соотношение, в левой части которого стоит многочлен от параметров a_1, a_2, … ; p_2, p_3, … и H_0, H_1, ..., а в правой - разность откликов метки на запросах *h* и *h'*.

Отклик метки на запросе *h* считаем известным. Для программной имитации метки достаточно реализовать процедуру вычисления значение полученного многочлена для любого значения *h'*. В этом многочлене параметры H_0,H_1,..., линейным образом выражаются через начальное значение $H_0 = h+h'$. Поэтому для вычисления значения многочлена достаточно найти значения его коэффициентов, в качестве которых выступают многочлены от параметров a_1, a_2, … и p_2, p_3, …, фигурирующих в соотношении. Для определения этих параметров составим и решим систему уравнений.

Для получения очередного уравнения возьмем новый запрос верификатора к метке и снова сравним отклик с начальным откликом. Изменение запроса означает смену значения H_0 в исходных данных (29) и последующие изменение значений параметров H_1, … в соотношениях (30) вплоть до итогового уравнения с G.

В полученном уравнении каждый моном от параметров a_1, a_2, … и p_2, p_3, … рассматриваем как независимое неизвестное. В результате мы получаем линейную систему уравнений. Набрав число независимых уравнений в количестве неизвестных, мы решаем систему и находим значения неизвестных мономов. После этого мы можем вычислять значение многочлена на любом входе. (Если число возможных уравнений меньше числа неизвестных, то это означает, что неизвестные зависимы и нам необходимо меньше уравнений, чтобы их решить.)

В таблице 2 приведены данные о степени нелинейности относительно параметров a_1, a_2, … и p_2, p_3, …. В скобках приведена степень нелинейности относительно параметров H_0, H_1, ..., если она отличается от степени нелинейности относительно параметров a_1, a_2, … и p_2, p_3, … .

Таблица 2 . Оценка сверху степени нелинейности состояний регистров

число раундов	D=A&P	P	B	Q	A	G	G⊕D
5	**2**	**2**	**1**	**1**	**0(1)**	**0(1)**	**2**
6	**3**	**2**	**2**	**1**	**1**	**0(1)**	**3**
7	**3**	**3**	**2**	**2**	**1**	**1**	**3**
8	**4**	**3**	**3**	**2**	**2**	**1**	**4**
9	**5**	**4**	**3**	**3**	**2**	**2**	**5**
10	**6**	**5**	**4**	**3**	**3**	**2**	**6**
11	**8**	**6**	**5**	**4**	**3**	**3**	**8**
12	***9***	**8**	**6**	**5**	**4**	**3**	***9***
13	*12*	***9***	**8**	**6**	**5**	**4**	***12***
14	*14*	*12*	***9***	**8**	**6**	**5**	***14***
15	*18*	*14*	*12*	***9***	**8**	**6**	***18***
16	*22*	*18*	*14*	*12*	***9***	**8**	***22***
17	***27***	*22*	*18*	*14*	*12*	***9***	*27*
18	*>32*	***27***	*22*	*18*	*14*	*12*	***>32***
19	*>32*	*>32*	***27***	*22*	*18*	*14*	*>32*
20	*>32*	*>32*	*>32*	***27***	*22*	*18*	*>32*
21	*>32*	*>32*	>32	*>32*	***27***	*22*	*>32*
22	*>32*	*>32*	>32	*>32*	*>32*	***27***	*>32*
23	*>32*	*>32*	*>32*	*>32*	*>32*	*>32*	***>32***

Таблица 3 содержит оценку сверху числа мономов от параметров a_1, a_2, … и p_2, p_3, …

Таблица 3. Оценка сверху числа мономов в выражениях

число раундов	D	P	B	Q	A	G
5	7	5	4	2	1	1
6	11	7	8	4	2	1
7	23	11	14	8	5	2
8	71	23	24	14	12	6
9	311	71	46	24	25	17
10	1871	311	116	46	48	41
11	15288	1871	426	116	93	88
12	-	15288	2296	426	208	180
13	-	-	17583	2296	633	387
14	-	-	-	17583	2928	1019
15	-	-	-	-	20510	3946
16	-	-	-	-	-	24455

Таблицы 2 и 3 дают оценку **сверху** на число запросов к метке. Рассматриваемый метод имитации имеет сложность меньше 2^n операций тогда и только тогда, когда степень нелинейности отклика метки меньше размерности вычислительной платформы. Поэтому при размере вычислительной платформы $n = 32$, требуется не менее **23 раундов**. При усилении алгоритма, за счет использования косвенного выхода $\boldsymbol{G} \oplus \boldsymbol{D}$, число раундов заметно меньше и равно **18**. Приведенные значения являются необходимыми, но не достаточными для обоснования максимальной криптографической стойкости: даже имея большую степень нелинейности, преобразование может содержать малое число мономов, что ведет к падению стойкости.

Последнее нашло отражение в развитии метода атаки, направленной на непосредственное клонирование метки. Предварительные расчеты показали, что при 16 раундах, для клонирования метки требуется около 16000 запросов.

В целом, представленные материалы показывают, что имеющиеся в распоряжении ресурсы вполне достаточны для реализации рентабельной и надежной защиты радиочастотных меток. При этом если не накладывать ограничений на число транзакций к метке, обусловленное исчерпыванием электронного слоя составляющих ее элементов, предполагаемый 16-ти раундовый вариант алгоритма верификации радиочастотных меток нуждается в усилении, по меньшей мере, по числу раундов.

Из результатов открытого для анализа типичного, линейного варианта реализации алгоритма аутентификации и заключения криптографической экспертизы, следует, что даже в этом очень далеком от действительно эффективных, не разглашаемых по коммерческим соображениям решений, имеющиеся в распоряжении ресурсы вполне достаточны для реализации надежной защиты радиочастотных меток, без заметного увеличения их стоимости. Так, для варианта аутентификации с косвенным выходом, для обеспечения полнофункциональной защиты требуется 18 раундов. С учетом ограничений по числу технически осуществимых запросов к RF-метке, достаточно 13 раундов.

Особенно эффективна, предназначенная для промышленной реализации, замена линейных криптографических примитивов их нелинейными аналогами, позволяющая устранить присущие линейным системам серьезные недостатки. В этом случае, при меньших аппаратных затратах число раундов аутентификации может быть уменьшено с 18 до 12 и с 13 до 9.

Не останавливаясь на достигнутом, для снятия рисков компрометации криптографической стойкости инструментальных средств ***RA***-технологий, на основе совершенствования методик имитационно-статистического моделирования и развития методик детальных криптографических атак, ведутся работы по созданию **программного комплекса**, предназначенного для все-

стороннего обоснования представляемых криптографических примитивов и протоколов защиты.

Не малая роль в этом процессе отводится на организацию противодействия массированным сторонним атакам на аутентификаторы считывающих устройств и RF-метки, подробно рассмотренную в работе [9]. Представленные в ней механизмы, основанные на сигнализации попытки несанкционированного доступа и реалистичном физическом ограничении числа запросов на аутентификацию, к примеру до 250-500, позволяют упростить конструкцию алгоритма аутентификации, повысить его стойкость к тотальным атакам и, в конечном счете, уменьшить число раундов аутентификации.

Собственно, с учетом ограничений накладываемых на число обращений к меткам и достигаемым высоким уровнем криптографической стойкости, на первый план выходят задачи достижения адекватной криптозащите, физической и производственно-технологической защиты памяти RF-меток и аутентификаторов считывающих устройств от стороннего проникновения.

9. Заключение

В итоге, на основе развития теории стохастических систем, к настоящему времени завершена разработка технологии построения эффективных симметричных криптографических примитивов стохастической криптографии, рассчитанных, на любые практически значимые платформы от 8 до 4096 и более бит, включающие в себя следующие функционально законченные компоненты:

- нелинейные счетчики, для управления циклами и организации недетерминированного доступа к памяти,
- бесповторные и равноповторные генераторы ключевого потока, необходимые для построения эффективных систем управления ключами и защиты от несанкционированного доступа,
- генераторы гаммы, для обеспечения высокопроизводительного синхронного и самосинхронизирующегося поточного шифрования,
- односторонние и взаимные верификаторы и аутентификаторы, используемые для проверки и подтверждения подлинности материальных объектов, включая условия крайнего дефицита ресурсов,
- хеш-функции и операторы, предназначенные для сжатия и необратимого преобразования данных,
- MAC-функции и операторы, по выработке показателей контроля целостности информации,

Особое внимание уделено развитию ***минималисткой криптографии***, рассчитанной на среды с крайним дефицитом ресурсов, например, какими являются дешевые радиочастотные метки.

Особенно если учесть не вынесенные на обсуждение потенциальные возможности разработанной технологии. Так, например, представленный в предыдущем разделе типичный вариант реализации рандомизационного агрегата, способного порождать семейство односторонних псевдослучайных функций, пригодных для использования в Протоколах аутентификации, допускает следующие усиления, не учтенные в проведенной функциональной атаке:

1. Использование косвенного выхода в составе *D*-оператора, в целях придания агрегату большей устойчивости к функциональным, аналитическим и корреляционным атакам, направленным на вскрытие значений входящих в его состав постоянных параметров и переменных.
2. Включение в состав рандомизатора нелинейной управляемой операции, для придания внутреннему состоянию агрегата существенно выраженных нелинейных свойств.
3. Включение в состав рандомизатора нелинейной управляемой операции, для придания конечному выходу агрегата существенно выраженных нелинейных свойств.
4. Использование для вариации коэффициентов и управляемой операции модифицированных генераторов в поле GF(2), с неизвестным параметром.

5. Введение в состав рандомизатора агрегата дополнительных контекстно-зависимых механизмов выравнивания частот, для достижения им более качественных статистических и более высоких криптографических показателей.
6. Усечение младших значащих битов в косвенном (прямом) выходе *D*-оператора, как наиболее сильно влияющих на его конечные статистические и криптографические показатели. При условии, если такое усечение оправдано, не смотря на снижение общей производительности и возможное увеличение стоимости производимых на его основе устройств.
7. Замена линейного по архитектуре дихотомического *D*-оператора, составляющего ядро рандомизационного агрегата, его нелинейным аналогом – полихотомическим оператором, с возможными, перечисленными выше усилениями 1-6.

Последнее положение, связанное с заменой линейного по архитектуре дихотомического *D*-оператора, его нелинейным аналогом – полихотомическим оператором, разработано в полном объеме и является основой для разработки криптографических устройств нового поколения и налаживания их промышленного производства.

Литература

1. Математическая энциклопедия. Изд. Советская энциклопедия.
   «Вероятностное пространство», т.1, Москва, 1977.
   «Динамические системы», т.2, Москва, 1979.
   «Эргодическая теория», т.5, Москва, 1985 и др.
2. Г. Шустер, «Детерминированный хаос. Введение». Мир, Москва, 1988.
   H. G. Schuster, Deterministic chaos: an introduction, VCH, Weinheim, 1988.
3. Н. В. Карлов, Н. А. Кириченко, «Колебания, Волны, Структуры».
   ФизМатЛит, Москва, 2003.
4. И. Кулаков, «Способ придания реальному объекту рандомизационных свойств и рандомизационная система». Заявка PCT/RU03/00141 от 7 апреля 2003.
5. Н. Птицын, «Приложение теории детерминированного хаоса в криптографии».
   МГТУ им. Н. Э. Баумана, Москва, 2002, np@beep.ru
6. Б. Шнайер. «Прикладная криптография». Изд. ТРИУМФ, Москва, 2002.
   B. Schneier, «Applied cryptography», 2nd Edition, John Wiley & Sons (1996).
7. Д. Кнут, «Искусство программирования. Получисленные алгоритмы»,
   т.2, Москва, 2003.
   Donald E. Knuth, «The Art of Computer Programming»,
   vol.2, 3rd Edition, Addison-Wesley.
8. C. W. Weller, «A High-Speed Carry Ckt. For Binary Adders».
   IEEE Trans. On Computers vol. C-18, No.8, Aug. 1969, pp. 728-732.
   S. A. Schwartz, «Single Line Propagation Adder and Method for Binary Addition».
   US Patent, 4,152,775, May 1, 1979.
9. И. А. Кулаков. «Развитие технологий RFID»
   Random Art Labs, Москва, май 2006.

Оглавление. Стохастические системы и криптография

Москва 2006