СТОХАСТИЧЕСКАЯ КРИПТОГРАФИЯ: МИНИМАЛИСТКИЙ И ЛЕГКОВЕСНЫЙ ПОДХОД

Кулаков Игорь Анатольевич
http://random-art.ru/

Статьей представляются достижения в области стохастических технологий и стохастической криптографии, базирующиеся на динамических системах дискретного времени и развитии нелинейной динамики. Существенным моментом решений является введение предарифметики и нелинейных, конъюнктивно-дизъюнктивных управляемых операций. Это позволило заложить новые методы и подходы реализации высококачественных криптографических примитивов, допускающих предельно эффективную, существенно выраженную нелинейную, параллельную и высокоэкономичную избирательную двоичную обработку по каждому из отдельно взятых разрядов, со скоростью срабатывания транзисторов типовых микросхем. Стохастическая криптография охватывает все разделы симметричной криптографии и благодаря предпринятому развитию алгебры, имеет явное, подавляющее превосходство по техническим показателям перед аналогами, а с этим, по сути, является минималистской и легковесной по исполнению и затратам.

Ключевые слова: арифметика, нелинейная динамика, стохастические системы, технологии, рекуррентный, конгруэнтный, полиномиальный, метод, способ, минималистская, легковесная, симметричная криптография, псевдо, случайные, числа, последовательности, дихотомические, поточный, блочный, шифр, генератор, PRNG, TRNG, LFSR, NFSR, LCG, идентификация, аутентификация, авторизация, шифрование, дешифрование, RFID, NFC, ERP, IoT, IoE.

С развитием и глобализацией информационного пространства, а с ним и нарождающегося киберпространства – криптография и представляемые ею технологии обеспечения безопасности приобретают все более и более важную роль [1]. С идущим стремительным развитием и наполнением физического уровня и переходом на наноуровень обработки, с внедрением новых технологий обработки сигналов (**UWB**), сетевых интегральных (ERP,IoT,IoE) и Облачных технологий, бесконтактных (**RFID**, **NFC**) и сенсорных технологий и технологий интеграции элементов систем (Wi-Fi,Bluetooth,ZigBee) – недооценка роли обеспечения безопасности может вести к крайне тяжелым последствиям и катастрофе [2].

Вместе с тем, несмотря на имеющиеся достижения в области симметричной криптографии [3], консолидацию [4] и усилия научных сообществ [5,6], наблюдается все большее отставание технологий обеспечения безопасности от требований времени и уровня развития техники, а это в свою очередь весьма существенно и негативно сказывается на объемах, времени, стоимости и безопасности обработки информационных потоков.

В связи с этим возникают проблемы, как в условиях экспоненциального роста объемов информационных потоков, с одной стороны, а с другой, в условиях не менее быстрого роста элементов систем с крайним дефицитом ресурса, например радиочастотных меток и смарт-карт, обеспечить рентабельную и эффективную обработку информации, отвечающую необходимым техническим требованиям и требованиям безопасности. Не секрет, что в погоне за выгодой, обеспечение необходимого уровня безопасности на поверку часто оказывается либо банальной профанацией проистекающей из коммерческих или внутриведомственных интересов, либо оказывается принципиально невозможной, либо неприемлемой по программным и аппаратным затратам, и в связи с этим откладывается на неопределенное будущее в расчете выхода вычислительных средств на качественно новый уровень.

По данным компании **Cisco** [7], наиболее продвинутые на сегодня технические разработки позволяют достичь скорости шифрования по нескольким параллельным каналам, от 2 до 10 Гбит/сек (для блочного шифра AES – это порядка 0.5÷0.9 Гбит/сек, при реально достижимой на сегодня пропускной способности каналов связи в 100 Гбит/сек). Кроме этого, из исследований, выполненных в рамках программы **BRIDGE** [6], следует, что для сред с крайним дефицитом ресурса использующих процедуры аутентификации, перед всеми известными легковесными разработками, как не странно, оказывается наиболее перспективным блочный шифр **AES-128**. Согласно лучшим аппаратным решениям, для реализации этого блочного шифра требуется порядка 3200 GE (при рентабельном уровне – в 200 GE) и не менее 10-ти последовательных раундов обработки, с уязвимыми к атакам по мощности и относительно высоко затратными по времени элементарными раундовыми операциями.

Для разрешения указанных проблем и преодоления все увеличивающегося отставания криптографии от уровня развития техники, требуются новые решения и подходы.

Цель статьи – опираясь за десятилетия накопленные материалы, подвести исследователей к новому направлению развития алгебры, стохастических технологий и представляемой ими стохастической криптографии, посредством решения следующих задач:

1. Привлечение внимания теоретиков к противоречиям и проблемам, выявленным в теории чисел, в алгебре и арифметике и указание пути их решения.
2. Ознакомление прикладников с рандомизационным способом и представляемым им новым направлением развития симметричной, стохастической криптографии.
3. Проведение оценки технического и инновационного потенциала развития стохастической криптографии и представляемых ею базовых примитивов.

Как видится по результатам многолетних исследований, приведенных в этой обзорной статье и в полном объеме отраженных на тематическом сайте: http://random-art.ru, решение этих вопросов кроится в развитии алгебры, динамических систем дискретного времени и нелинейной динамики и в развитии представляемых ими стохастических технологий. Существенным моментом решений и развития стохастических технологий является введение предарифметики и нелинейных, конъюнктивно-дизъюнктивных управляемых операций, а также создание рандомизационного способа, охватывающего указанные научно-технические результаты. На этой основе удалось отказаться от малоперспективной и трудоемкой в использовании арифметической операции сложения, а с нею и ее производных, в пользу высокоэффективных элементарных двоичных операций (преобразований и функций). Указанные операции допускают существенно выраженную нелинейную, параллельную и высокоэкономичную избирательную двоичную обработку по каждому из отдельно взятых разрядов, со скоростью срабатывания транзисторов типовых микросхем. Без этого, как показывает аналитика, достичь инновационного прорыва в криптографии, а с нею рентабельно и эффективно решить насущные проблемы обеспечения безопасности – задача нереалистичная.

Как показывают проведенные исследования и расчеты, представляемые ими криптографические примитивы (генераторы случайных чисел, идентификаторов и паролей, поточные и блочные шифры, протоколы аутентификации и др.) прозрачны для анализа, обладают высокими статистическими и криптографическими показателями, легко адаптируются под имеющиеся и перспективные приложения, имеют явное, подавляющее превосходство по техническим показателям перед известными аналогами. Последнее утверждение подтверждается примерами, указывающим на возможность достижения предельно высокой производительности криптографических примитивов (от сотен до тысячи Гбит/сек, за счет полного параллелизма, неограниченного наращивания длины платформ и скорости обработки, сравнимой со скоростью срабатывания транзисторов типовых микросхем), отличающихся от аналогов существенно меньшими энергетическими и аппаратными затратами (от 120-150 GE) и на порядки меньшей себестоимостью схем реализаций.

Стохастические технологии охватывают все разделы симметричной криптографии, являются минималистскими и легковесными по исполнению и по существу, рассчитаны на бессрочную перспективу и носят опережающий характер над уровнем развития техники. Представляемые ими системы и компоненты обеспечения безопасности фактически не оказывают влияния на ключевые технические показатели информационно-коммуникационных, сетевых, бесконтактных (RFID,NFC), сенсорных и им подобных систем. Освещение этих вопросов, как и детальное изложение ценных с точки зрения практической реализации криптографических примитивов, далеко выходит за рамки данной статьи. Для получения развернутой и более детальной информации по эти вопросам, включая обращения к результатам их публичного обсуждения, следует обратиться по адресу: www.gosbook.ru/node/51114.

Обозначения элементарных двоичных операций:

$\wedge, \vee, \neg$ – логические операции AND, OR и NOT;

$\&, |, \oplus, \overline{\oplus}, \bar{}$ – побитовые операции **AND**, **OR**, **XOR**, **XNOR** и инверсии **NOT**, соответственно, над n-разрядами ($n \geq 1$) двоичными величинами;

$\lhd_m, \rhd_m$ – смещение на m разрядов ($m \geq 0$) в сторону старших и младших бит;

rotL_m, **rot**R_m – циклический сдвиг на m разрядов в сторону старших и младших бит;

z **mod** 2^n – остаток от деления на 2^n или тоже, что ограничение изменения разрядов переменной $z \,\&\, (2^n - 1)$ числом n значащих бит.

1. Регистры сдвига с обратной связью

Для начала обратимся к истории. Поистине, знаменательным событием, придавшим колоссальный импульс развитию криптографии, явилось открытие конечных полей $\mathbb{F}_q$ или GF(q), где q – число элементов поля (É. Galois,1830), ***создание линейного рекуррентного метода*** [8] ***на основе регистров сдвига с линейной обратной связью*** (**LFSR**, E. Selmer, 1965).

Позже [8], ***благодаря введению алгебраических 2-адических систем***, регистры сдвига получили развитие, путем замены операция XOR в цепи обратной связи на сложение, с чем получили название – ***регистры сдвига с обратной связью по переносу*** (**FSCR**, A. Klapper, M. Goresky, 1993). Между тем, данный подход не обеспечивает должного периода, нередко сопровождается вырождением, при котором последовательность представляется константой или колеблется в крайне малых пределах, с периодом меньшим критического для большого числа приложений, чем разрядность регистра. Кроме того, реальная криптографическая стойкость FSCR, при несущественно выраженной нелинейности связи по переносу, вызывает большое сомнение. Все это, а также введение операции сложения, использование которой значительно (многократно) сказывается на производительности FSCR, переводит данный подход больше в академическую плоскость исследований, чем в прикладную.

Последовательности n-разрядных двоичных чисел, формируемые на основе LFSR, именуются линейными рекуррентными последовательностями (LRS) и обладают следующими свойствами:

1. Элементы LRS изменяются в интервале $[1, 2^n - 1]$.
2. Период LRS максимален и равен $2^n - 1$.
3. В пределах периода LRS бесповторны, иными словами, не имеют одинаковых элементов.

В отношении реализации:

1. Регистры сдвига в конфигурации Галуа допускают параллельную обработку в один такт по каждому из своих двоичных разрядов, со скоростью сравнимой со скоростью срабатывания транзисторов типовых микросхем.
2. Число логических элементов, требуемых для аппаратной реализации – минимально, и без учета триггеров для организации итераций (порядка $4 \cdot n$ GE), составляет, как правило, 1÷3 GE.

В отношении статистических свойств:

1. Элементы LRS носят по каждому из разрядов равночастотный характер и имеют максимальный период, равный $2^n - 1$.
2. По мнению многих авторов (Solomon W.Golomb), статистические свойства LRS идеальны, хотя статистические тесты на основе пакета **DIEHARD** [9], не подтверждают данного утверждения.

Для определения конфигурации LFSR и его начального состояния, достаточна выборка с его выхода, из $2 \cdot n$ бит [10], а при известном образующем многочлене обратной связи (общепринятое положение) – n бит. Другими словами, не имеет смысла говорить о криптографической стойкости генераторов случайных чисел, построенных на базе LFSR.

Регистры сдвига хорошо изучены и находят широкое применение в криптографии, кодировании и контроля целостности информации. Особо следует выделить приложения, в которых LFSR используются для поддержания периода и предотвращения вырождения криптографических примитивов, организации стеков обратной связи и выработки CLC [10], а также приложения, предназначенные для генерации истинно случайных чисел.

Последние, совместно с решениями инженеров компании **Intel**, закладывающих основы конструирования высокоэффективных источников энтропии, позволяют создавать самые быстрые, от 2÷15 Гбит/сек, и выше, мало затратные генераторы истинно случайных чисел [11]. Такие генераторы, кроме использования в процессорах Intel, могут найти широкое применение для генерации широкополосного, в том числе и псевдослучайного шума в системах UWB, в протоколах разрешения коллизий и аутентификации меток RFID.

Линейный рекуррентный метод допускает развитие, модификацию и усиление, с введением постоянного параметра Hg в одну из модификаций его уравнения [10]:

$$z = Hg \oplus \mathbf{rot}_1(x_{i-1}); \quad \textit{if}\ (\ z \wedge \mathrm{LFSR\_OUT}\ )\ z = z \oplus \mathrm{LFSR_n}; \quad x_i = z, \tag{1}$$

$$z = Hg \oplus x_{i-1};\quad \textbf{\textit{if}}\ (z \wedge \mathrm{LFSR\_OUT})\ z = z \oplus \mathrm{LFSR_n};\quad x_i = \mathbf{rot}_1(z), \qquad (2)$$

где $\mathbf{rot}_1 = \{\mathbf{rot}L_1, \mathbf{rot}R_1\}$ – левый или правый циклический сдвиг на разряд, при

$\mathrm{LFSR\_OUT} \in \{2^{n-1}, 1\}$, для лево и право-направленных LFSR, соответственно,

$\mathrm{LFSR_n}$ – константа обратной связи.

Константа $\mathrm{LFSR_n}$ обратной связи формируется исходя из используемого образующего многочлена [8]. Состояние LFSR, отвечающее условию $x_i \oplus x_{i-1} = x_0 \oplus x_1 = 0$, является запрещенным, т. к. ведет к вырождению уравнений (1), (2) и требует исключения. Исключение запрещенного состояния осуществляется специальным образом перед самым началом функционирования LFSR, исходя из минимальных аппаратных затрат. Такое исключение может быть осуществлено путем инвертирования, на выбор, одного из битов начального условия x_0, либо путем инвертирования одного из битов параметра Hg.

Для информации, на эпюрах Рис.1 – Рис.4, в Приложении, представлены фрагменты LRS, генерируемые на основе непараметрических ($Hg = 0$) и параметрических ($Hg \neq 0$) право-направленных 32-х разрядных LFSR, с 5-ти членными образующими многочленами:

$$x^{32}+x^{16}+x^7+x^2+1, \qquad x^{32}+x^{30}+x^{25}+x^{16}+1,$$

и поставленным им в однозначное соответствие шестнадцатеричными константами обратной связи $\mathrm{LFSR_{32}}$ = 0x00010084 и 0x42010000 [8], для уравнения (1) с предусловной ротацией, при условиях $\{x_0 = 1, Hg = 0\}$ и $\{x_0 = 0, Hg = 1\}$, соответственно.

Для сравнения, на эпюрах Рис.5 – Рис.8, в Приложении, при тех же условиях, представлены фрагменты LRS, генерируемые на основе LFSR с постусловной ротацией, представляемые уравнением (2).

Статистический анализ [9] одноразрядных последовательностей снимаемых с выхода LFSR, для всех представленных вариантов дает почти одинаковые результаты. С результатами прохождения тестов DIEHARD по варианту, представленному на Рис.1, можно ознакомиться в тестовом файле, по ссылке http://t.random-art.ru/?download=Test_1.txt.

Необходимо отметить, что статистические свойства LFSR существенно зависят от используемого образующего многочлена. Так, использование многочлена $x^{32}+x^7+x^6+x^2+1$, например, на который ссылается B. Schneier [8], приводит к вырождению статистических тестов (см. http://t.random-art.ru/?download=Test_BS.txt).

Как следует из приведенных выше примеров, введение параметра Hg существенно сказывается на выходных результатах и при всем этом позволяет почти в 2^n раз увеличить разнообразие генерируемых LRS, что может дать весьма заметное, а в ряде случаев решающее усиление показателей стойкости используемых их криптографических примитивов. Ко всему этому необходимо добавить, что введение в схемотехнические решения параметра Hg может быть осуществлено без дополнительных аппаратных затрат (режим **RO** только на чтение) или это требует очень малых аппаратных затрат, за счет выбора прямого или инвертированного выхода триггеров в цепи итерации (1), (2) и соответствующей разводки проводников.

Из данного раздела следует сделать очень важный для дальнейшего вывод. Именно, линейный рекуррентный метод и его реализация на основе регистров сдвига с линейной обратной связью в конфигурации Галуа, в силу полного параллелизма, малого числа и высокой скорости исполнения используемых логических операций, устанавливают именно те предельно достижимые ориентиры для минималисткой и легковесной криптографии, к которым надо стремиться.

2. Конгруэнтный метод и его нелинейные расширения

Сравнительно ранее линейного рекуррентного метода, появился один из практикуемых и сегодня методов генерации последовательностей случайных чисел (D.H.Lehmer,1949), широко известный под названием линейный смешанный конгруэнтный метод [12].

Линейный смешанный конгруэнтный метод задается рекурсивным уравнением:

$$x_i = a \cdot x_{i-1} + b \mod m. \qquad (3)$$

Нас будет интересовать наиболее простой случай с двоичным модулем $m = 2^n$, а именно:

$$x_i = a \cdot x_{i-1} + b \mod 2^n, \qquad (4)$$

с n-битовой двоичной x переменной, и постоянными коэффициентами – множителем $a \equiv$

$1(\mathrm{mod}\ 4)$ и нечетным приращении b.

Формируемые согласно с уравнением (4) двоичные последовательности, именуют линейными конгруэнтными последовательностями, а средства их реализации – линейными конгруэнтными генераторами (**LCG**) [13]. Последовательности данного типа имеют максимальный период $T_n = T_{\max} = 2^n$, и в пределах его бесповторны. Также известно [14], что такие последовательности, даже усеченные до одного старшего бита, не являются криптографически стойкими.

Линейный конгруэнтный метод (4), в связи с ограничением, накладываемым на второй бит множителя a, носит неполный характер, и допускает неизвестное ранее, если следовать открытым источникам, простое развитие [15], ***именуемое нелинейным расширением***, вида:

$$x'_i = a' \cdot (x'_{i-1} \oplus b') \bmod 2^n, \tag{5}$$

при $a' \equiv 3(\mathrm{mod}\ 4)$ и нечетном приращении b' (собственно, $b' = b$).

Для сравнительного анализа статистических свойств самых старших разрядов конгруэнтных последовательностей (4) и (5), положим $b' = b = 1$,

$$a = m_0 \oplus 2, \quad a' = m_0 \oplus 4, \quad \text{при} \quad m_0 = (2^n - 1)/2^{n/2}. \tag{6}$$

Статистический анализ [9] формируемых на основе уравнений (4) и (5) конгруэнтных последовательностей, при значениях коэффициентов устанавливаемых исходя из соотношений (6), показывает статистическую надежность выборки полученной по самому старшему биту, начиная с платформ, разрядностью $n = 40$ и $n = 36$ бит, соответственно.

Согласно проведенным исследованиям [16], линейный конгруэнтный метод с постоянными коэффициентами (4) и его нелинейное расширение (5), допускают феноменологическое обобщение на случаи, когда коэффициенты $\{a,b\}$, входящие в состав указанных уравнений, являются переменными.

Линейный конгруэнтный метод с переменными коэффициентами задается уравнением:

$$x_i = A_{i-1} \cdot x_{i-1} + B_{i-1} \bmod 2^n, \tag{7}$$

с n-битовой двоичной x переменной, при $A_{i-1} \equiv 1(\mathrm{mod}\ 4)$, для всех i, а его нелинейное расширение, аналогичным уравнением с множителем $A'_{i-1} \equiv 3(\mathrm{mod}\ 4)$, вида:

$$x'_i = A'_{i-1} \cdot (x'_{i-1} \oplus B_{i-1}) \bmod 2^n, \tag{8}$$

с приращением:

$$B_{i-1} = (B^*_{i-1} \mid 3) \oplus b_0, \quad \text{при} \quad b_0 = const = \{0,2\}. \tag{9}$$

Двоичные конгруэнтные последовательности (5) и (6) имеют максимальный период $T_n = T_{\max} = 2^n$, если образующая последовательность B^*, есть смещенная двоичная конгруэнтная последовательность не менее чем на один бит в сторону старших разрядов, а последовательности $\{A,A'\}$ формируются исходя из условий:

$$A_{i-1} = A^*_{i-1} \mid a_0, \qquad A'_{i-1} = A^*_{i-1} \mid a'_0, \tag{10}$$

при константах $a_0 = 1$ и $a'_0 = 3$, с образующей последовательностью A^*, являющейся смещенной двоичной конгруэнтной последовательностью, не менее чем на два бит.

Представленные в работе [16] типовые двоичных LCG с переменными коэффициентами, построенные в соответствии с уравнениями (7), (8) и их статанализ [9], показывает статистическую надежность выборки, полученной по самому старшему биту, начиная с платформ, разрядностью от $n = 33 \div 37$ и $n = 26$ бит, соответственно. В Приложении на Рис.9 и Рис.10 приведены эпюры прохождения тестов, полученные исходя из представленных там же алгоритмов реализации упомянутых типовых LCG.

Линейный конгруэнтный метод с переменными коэффициентами и его нелинейные расширения допускает развитие и обобщение. На их основе создан ***полиномиальный конгруэнтный метод с переменными коэффициентами*** [16].

Между тем, линейный и полиномиальные конгруэнтные методы с переменными коэффициентами и их разновидности не так просто и эффективно устроены, как это кажется. В первую очередь это связано с использованием высоко затратной операции умножения и даже, относительно затратной операции сложения, на которые приходится большая доля вычислительных, аппаратных и энергетических затрат.

Более того, при оценке эффективности, сложности реализации LCG и требуемых аппа-

ратных затрат следует четко понимать, что обычные арифметические операции не допускают распараллеливание вычислений по каждому из отдельно взятых разрядов, что крайне негативно сказывается на конечной производительности генераторов (4),(5) и (7),(8), и в силу чего, выводят их не в практическую, а в академическую плоскость исследований.

Из данного раздела следует очень важный для последующего вывод. Установленный и проверенный факт работоспособности линейного и полиномиального конгруэнтного метода с переменными коэффициентами, а также их нелинейных расширений, предполагающих использование смешанных операций – сложения по модулю 2^n и по модулю 2, прямо свидетельствует о наших наивных представлениях в алгебре, о кольцах вычетов, конечных полях и присущих им свойств.

3. Дихотомические последовательности

Для начала [17] обратимся к двоичному представлению первых чисел натурального ряда, начиная с нуля:

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

Таб.1.. Двоичная последовательность, порождаемая числами натурального ряда

Из образованной таким образом из двоичной последовательности $C = \{c_i: i = \overline{1,m}\}$, составленной из элементов $c_i \in C$, разрядностью $n = 4$ бит, видно, что период повторения T_k каждого очередного k-го бита, равен $T_k = 2^k$ $(k = \overline{1,n})$, для произвольного n. Кроме этого, для каждого k-го бита, элементы i и $(i+T_k/2)$, принадлежащие соседним полупериодам этой последовательности C, комплементарны

$$c_{ki} = \bar{c}_{k(i+Tk/2)}, \tag{11}$$

т.е. связаны между собой операцией комплементации $\bar{}$ NOT.

Двоичная последовательность C, представленная в Таб.1, задается единичным счетчиком инкрементного типа – $c_i = c_{i-1} + 1 \bmod 2^4$, а обратная, рекуррентная к ней последовательность C^*, задается единичным счетчиком декрементного типа – $c^*_i = c^*_{i-1} - 1 \bmod 2^4$, соответственно.

К этому, аналогичной структурой и свойствами наделены все двоичные последовательности формируемые на основе линейного смешанного (4),(5) и (7),(8), а с ним и полиномиального конгруэнтного метода [16].

Кардинальное число $card\ X$ множества всех различных двоичных последовательностей с максимальным периодом $T_n = 2^n$, формируемых на основе уравнений (4) и (5), при различных значениях коэффициентов $\{a,b\}$ и начальных условиях x_0, равно $2^{3(n-1)}$.

Данные результаты допускают нижеследующее естественное обобщение.

Двоичная последовательность $D = \{d_i: i = \overline{1,T_n}\}$ ***называется дихотомической*** или *Dh*-последовательностью, если частотные изменения значений каждого его k-го двоичного разряда носят регулярный характер, при котором любая из подпоследовательностей, образованная из элементов исходной последовательности путем исключения $D \bmod T_k$ их $n-k \in [0,n-1]$ старших разрядов, имеет период повторения $T_k = 2^k$ и в пределах его не содержит одинаковых элементов.

Другими словами, распределение значений последовательности D, составленной ровно из T_n элементов $d_j \in D$, обладает иерархической структурой типа двоичного дерева, состоящей из n уровней $k \in [1,n]$ и $m_k = T_n / T_k$ взаимно непересекающихся на этих k уровнях, идентичных дихотомических классов $D_k \equiv D \pmod{T_k}$, при этом любая однаразрядная двоичная пара $\{d_{ki}, d_{ki+T_k/2}\}$, i и $i+T_k/2$ элементов последовательности D $(i = \overline{1,T_n - T_k/2})$, разделенных полупериодом $T_k/2$, комплементарна, т. е. $\bar{d}_{ki} = \bar{d}_{ki+T_k/2}$.

Перебирая поразрядно полупериоды всех дихотомических классов, порождаемых арифметическим счетчиком $D_i = D_{i-1} + E \bmod 2^n$ по всем ограниченным полупериодом начальным условиям и возможным приращениям E, можно определить кардинальное число $card\ D$

множества всевозможных различных *Dh*-последовательностей:

$$card\ D\ =\ 2^{2^{1-1}-1}\cdot 2^{2^{2-1}-1}\cdot 2^{2^{3-1}-1}\ \ldots\ \cdot 2^{2^{n-1}-1}\cdot 2^{n-1}\cdot 2^{1}\ =\ 2^{2^{n}-1}. \qquad (12)$$

Ко всему, как показывают исследования [17], уравнение формирования различных *Dh*-последовательностей, может быть задано следующим рекуррентным выражением:

$$X_i\ =(a_0 \oplus b_0)\ +\sum_{k=1}^{n} A_k(x_k, x_{k-1},\ldots,x_1)_{i-1}\,2^{k-1} \bmod 2^n \quad (x_{k\,(i-1)}\in 0,1), \qquad (13)$$

при нечетном *n*-разрядном приращении a_0 и коэффициенте a_1, синхропараметре b_0, равным 0 или 1, и суперпозиции [18] одночленов (мономов):

$$A_k(x_k, x_{k-1},\ldots,x_1) = x_k + \sum_{(i_1,\ldots,i_{k-1})} a_{i_1,\ldots,i_{k-1}} x_1^{i_1}\cdot\ldots\ x_{k-1}^{i_{k-1}} \qquad (k>1,\ i_{k-1}\in 0,1) \qquad (14)$$

и мономе $A_1 = (a_1 + 2\cdot b_0)\cdot(x_1 \oplus b_0)$, $a_1 \equiv 1 (\bmod 4)$, где $\sum_{(i_1,\ldots,i_{k-1})} a_{i_1,\ldots,i_{k-1}} x_1^{i_1}\cdot\ldots\ x_{k-1}^{i_{k-1}}$ означает суммирование по всем различным сочетаниям одноразрядных двоичных переменных $\{x_k\}\in X$, числом $2^{2^{k-1}}$.

Суммирование по всем мономам, начальным условиям и приращениям дает кардинальное число $card\ X = 2^{2^n-1}$ множества всех таких различных *Dh*-последовательностей.

Совпадение кардинальных чисел $card\ X = card\ D = 2^{2^n-1}$, означает по Кантору, что любая из возможных *Dh*-последовательностей может быть единственным образом выражена через коэффициенты уравнения (13).

Как видим, число всевозможных *Dh*-последовательностей, даже при небольших *n*, необычайно огромно и охватывает гармоничные, упорядоченные процессы и существенно неупорядоченные, хаотичные процессы. В последнем случае закон распределения изменений в старших разрядах быстро стремится к идеальному равномерному [9].

Следуя здравому смыслу, исходящего из прикладного характера проводимых работ, необходимо отметить, что описание, а тем более формирование *Dh*-последовательностей, представляемых уравнением (13), является непомерно громоздким, вычислительно сложным и слабо предсказуемым по принятым криптографическим меркам и статистическим показателям, что делает данный подход непригодным для практики.

В академическом, нежели чем в практическом плане, малое и при этом не столь эффективное исключение, в силу использования относительно высоко затратной операции сложения, а с ней и операции умножения, составляют ряды, свойственные конгруэнтному методу [12,13,14] и его нелинейному расширению [16].

В целом, разрешить указанные выше проблемы и довести формирование *Dh*-последовательностей до математической прозрачности, должного прикладного и эффективного практического результата оказалось возможным благодаря работе [15] и разработке рандомизационного способа.

4. Рандомизационный способ

В отличие от тривиальных подходов, представляемых рассмотренными выше, рекуррентными и конгруэнтными методами, рандомизационный способ (Random Method) всецело опирается на ***динамические системы с дискретным временем*** с недетерминированным (хаотическим, стохастическим) поведением, характерным для случайных процессов и явлений.

Рандомизационный способ имеет давнюю историю [15], по сути, на фоне ошибочно отвергнутых достижений исследователей и ученых [14], D. Knuth и его приверженцы редкое исключение [12], начатую с “чистого листа” и закладывает основу для построения стохастических систем и стохастических технологий [19], а с ними и стохастической криптографии. Ключевые положения рандомизационного способа запатентованы [20,21].

Решающим моментом развития и становления рандомизационного способа явилось открытие предарифметики (2006 г.), впервые озвученное на конференции **РусКрипто 2006** [22], а позже и ее разновидностей (2010 г.).

Предарифметика предшествует обычной арифметике и ограничена глубиной переноса на один разряд [23].

Сложение (вычитание) в предарифметике подчиняется ряду, формируемому согласно с уравнениями:

$$P_i = ((\mathbf{Imp}(G_{i-1}) \,\&\, P_{i-1}) \lessdot_1) \mid \mathbf{1}, \qquad G_i = G_{i-1} \oplus P_{i-1} \mod 2^n, \tag{15}$$

с функцией импликации $\mathbf{Imp}(c) = c$ для сложения и $\mathbf{Imp}(c) = \bar{c}$ для вычитания, включающим две двоичные переменные $\{G,P\}$ – n-разрядную базу операции G и ее $(n+1)$-разрядное нелинейное дополнение P, путем прибавления (вычитания) единицы 1, фиксируемой в младшем разряде дополнения P, начиная с начальных значений $\{G_O,P_O\}$.

На Рис.11 и Рис.12, в Приложении, приведены ряды, полученные при нулевых начальных условиях $P_O = 0$ и $G_O = 0$, составленные из упорядоченных пар (G_i,P_i), представляющих собой бинарные отношения, задающие операцию сложения и вычитания в предарифметике, и результаты операций сложения g с единицей и ее вычитания d в 4-х разрядной двоичной арифметике.

По отношению к предарифметике, может быть введена и двойственная по отношению к ней – комплементарная предарифметика.

Сложение (вычитание) в комплементарной предарифметике подчиняется ряду, следующему из соотношений (15) и комплементарного свойства $a \mid b = \overline{\bar{a} \,\&\, \bar{b}}$, формируемому при $P' = \bar{P}$ и $G' = \bar{G}$, согласно с уравнениями:

$$P'_i = (\mathbf{Imp}(G'_{i-1}) \mid P'_{i-1}) \lessdot_1, \qquad G'_i = \overline{G'_{i-1} \oplus P'_{i-1}} \mod 2^n, \tag{16}$$

начиная с начальных значений $\{P'_O,G'_O\}$.

На Рис.13 и Рис.14, в Приложении, приведены ряды, полученные при нулевых начальных условиях $P'_O = 0$ и $G'_O = 0$, составленные из упорядоченных пар (G'_i,P'_i), задающих операцию сложения и вычитания в комплементарной предарифметике, и результаты операций сложения g' с единицей и ее вычитания d' в 4-х разрядной комплементарной арифметике.

В предарифметиках, задаваемых уравнениями (15) и (16), в отличие от арифметики, возможно наличие зависящего от начальных условий переходного нелинейного участка длиной $L_T \le n$, после прохождения которого базовая переменная G, благодаря феноменальной саморегуляции ее и ее нелинейного дополнения P, достигает максимального периода 2^n и далее всюду, в границах каждого из последующих периодов ведет себя стационарно и бесповторно, что демонстрируется на Рис.11 – Рис.14.

Наличие такого нестационарного переходного участка, самоисчезающего по мере формирования последующих элементов последовательностей, задаваемых уравнениями (15) и (16), существенно отличается от подобных участков (предпериодов), наблюдаемых при генерации периодических последовательностей на основе рекуррентных подходов [18], а также поведением на этих участках, как правило, ведущим к трудно предсказуемому, нестабильному поведению генераторов, а в особых случаях и к их полному вырождению.

Обращаясь к Рис.11 – Рис.14, видим, что после прохождения переходного участка, последовательности, формируемые на основе уравнений (15) и (16), есть *Dh*-последовательности, во многом подобные *Dh*-последовательностям формируемым на основе единичных арифметических счетчиков.

С введением предарифметик, можно сделать следующие очень важные выводы.

Dh-последовательности, формируемые на основе уравнений (15) и (16), в техническом исполнении на основе так называемых *Dh*-счетчиков, обладают следующими свойствами:

1. Элементы *Dh*-последовательностей изменяются в интервале $[0, 2^n - 1]$.
2. Период *Dh*-последовательностей максимален и равен 2^n.
3. В пределах периода *Dh*-последовательности бесповторны, иными словами, не имеют одинаковых элементов.

В отношении реализации:

1. *Dh*-счетчики допускают параллельную обработку в один такт по каждому из своих двоичных разрядов, со скоростью сравнимой со скоростью срабатывания транзисторов типовых микросхем.
2. Число логических элементов, требуемых для аппаратной реализации, составляет около $2 \cdot n$ GE на сам алгоритм и порядка $8 \cdot n$ GE ($2 \cdot n$ триггеров) для организации итераций.

В отношении статистических свойств:

1. Элементы *Dh*-последовательностей по каждому из *k*-разрядов *Dh*-счетчиков носят неравночастотный характер, с периодом. $T_k = 2^k$ $(k = \overline{1,n})$.

2. О статистических свойствах, также как и для арифметических счетчиков, говорить не приходится.

Первые выводы наводят на мысль об отказе от операции сложения, как таковой и вывода использующих ее криптографических примитивов, любым образом, включая адресацию векторов и таблиц (***S***-блоков любого объема), из разряда минималистских и легковесных.

Кроме этого, введение предарифметики явно указывает [23], что ***операция сложения есть не единовременный акт, а наполнена глубоким динамическим содержанием*** **!**

Рандомизационный способ делится на регулярный и нерегулярный. В регулярном способе, распространение влияния младших битов цифровых блоков на старшие, носит строго однонаправленный, ламинарный характер. В нерегулярном способе разряды цифровых блоков, ко всему, охвачены обратными связями.

Регулярный рандомизационный способ [20] предназначен для формирования упомянутых выше *Dh*-последовательностей, на основе *Dh*-генераторов [24]. В свою очередь, дихотомические генераторы могут быть взаимосвязаны между собой и способны образовывать сети и композиции любой структурной и функциональной сложности [15], и служат основой для построения высококачественных генераторов случайных чисел, поточных шифров и стохастических систем дискретного времени различного назначения.

Нерегулярный рандомизационный способ [21] более широк, наследует основные (структурные и функциональные) свойства регулярного способа [20,24], закладывает основы для построения блочных шифров и по своим характеристикам и статистическим показателям вплотную примыкает к идеальному Хаосу и истинно случайным процессам.

4.1 Регулярный рандомизационный способ

Регулярный рандомизационный способ строится на основе предарифметики и распространении влияния младших битов на старшие. Распространение влияния битов осуществляется таким образом, что последовательности, полученные в результате таких преобразований, сохраняют свойства присущие *Dh*-последовательностям, а старшие значащие биты приобретают статистические свойства, присущие истинно случайным величинам.

Существенным моментом решений является введение нелинейных, *конъюнктивно-дизъюнктивных управляемых двоичных операций*.

Нелинейная управляемая двоичная операция **AND/OR** – $A \,\&^C B$ над парой *n*-разрядных двоичных величин $\{A, B\}$, связанных нелинейной управляемой двоичной операцией - $\&^C$ по закону *C*, задается в зависимости от значений, принимаемых соответствующим *j* разрядом (битом) $c_j \in C$ $(j = \overline{1,n})$ двоичной величины *C*, при этом, если $c_j = 0$, имеет место конъюнкция $a_j \wedge b_j$, иначе, при $c_j = 1$, имеет место дизъюнкция $a_j \vee b_j$ битов $a_j \in A$ и $b_j \in B$. Из определения следует аналитическое соотношение:

$$A \,\&^C B = ((A \,\&\, B) \,\&\, \overline{C}) \mid ((A \mid B) \,\&\, C) = (A \,\&\, B) \oplus (C \,\&\, (A \oplus B)). \qquad (17)$$

В свою очередь, для нелинейной управляемой двоичной операции **OR/AND** - $A \mid^D B$ при $d_j = 0$, имеет место дизъюнкция, а при $d_j = 1$ – конъюнкция, отсюда:

$$A \mid^D B = ((A \mid B) \,\&\, \overline{D}) \mid ((A \,\&\, B) \,\&\, D) = (A \mid B) \oplus (D \,\&\, (A \oplus B)). \qquad (18)$$

Согласно соотношениям (17) и (18) законы управления *C* и *D* в нелинейных двоичных операциях $A \,\&^C B$ и $A \mid^D B$ связаны между собой отрицанием $D = \overline{C}$.

Аналогичным образом могут быть введены нелинейные управляемые двоичные операции **NAND/NOR** - $A \,\overline{\&}^C B$ и **NOR/NAND** - $A \,\overline{|}^D B$:

$$A \,\overline{\&}^C B = \overline{A \,\&^C B} = (\overline{(A \,\&\, B)} \,\&\, \overline{C}) \mid (\overline{(A \mid B)} \,\&\, C) = (A \,\&\, B) \;\overline{\oplus}\; (C \,\&\, (A \oplus B)), \qquad (19)$$

$$A \,\overline{|}^D B = \overline{A \mid^D B} = (\overline{(A \mid B)} \,\&\, \overline{D}) \mid (\overline{(A \,\&\, B)} \,\&\, D) = (A \mid B) \;\overline{\oplus}\; (D \,\&\, (A \oplus B)). \qquad (20)$$

На базе CMOS технологий наиболее экономично и эффективно реализуются ***управляемые логические элементы*** **NAND/NOR**:

$$A \,\overline{\&}^C B = \overline{(A \,\&\, B) \oplus (C \,\&\, (A \oplus B))}, \qquad (21)$$

причем, на это требуется 2.5 GE [20].

Из результатов работы [20] и на основании проведенных исследований, для генерации *Dh*-последовательностей рекомендуется использовать следующие, ***оптимальные с точки зрения программной и аппаратной реализации примитивы***:

$$P_i = (H_P \oplus (G_{i-1} \&^{C_H} P_{i-1})) \lhd_1, \quad G_i = H_G \oplus G_{i-1} \oplus P_{i-1} \oplus Đ(P_{i-1} \lhd_1, G_{i-1}) \mod 2^n, \tag{22}$$

$$P^* = P'_i \lhd_1, \quad G_i = H_G \oplus G_{i-1} \oplus P^* \oplus Đ(P^* \lhd_1, G_{i-1}) \mod 2^n, \quad P'_i = H_P \oplus (G_{i-1} \&^{C_H} P^*), \tag{23}$$

с постоянными коэффициентами – модификаторами $\{H_P, H_G, H_C\}$, нелинейной управляемой операцией $\&^{C_H}$ – **AND**/**OR** (17) или $\overline{\&}^{C_H}$ – **NAND**/**NOR** (19), устанавливаемой посредством выбора H_P, с *n*-разрядными двоичными переменными – базовой переменной *G* и ее нелинейным дополнением *P* и управляющей переменной:

$$C_H = H_C \oplus ((G_{i-1} \lhd_1) \,\&\, \bar{3}), \tag{24}$$

для двух – линейной (легковесной) и нелинейной (минималисткой) функций *Đ* распространения влияния бит:

$$Đ(P,G) = G \lhd_3, \tag{25}$$

$$Đ(P,G) = (P \& (G \lhd_3)) \mid (\bar{P} \& (G \lhd_4)), \tag{26}$$

при начальных условиях $\{P_O, G_O\}$ из интервала $[0, 2^n - 1]$. При нечетных, предписываемых правилами синхронизации коэффициентах $\{H_G, H_C\}$, последовательности, формируемые на основе уравнений (22) и (23), есть *Dh*-последовательности с максимальным периодом, равным 2^n. Здесь не лишним будет напомнить, что введение постоянных коэффициентов при использовании памяти типа RO не ведет к увеличению аппаратных затрат, за счет фиксированного выбора с выхода триггеров отвода с прямым или инвертированным сигналом.

Как показывают исследования, представленный уравнениями (22) и (23) рекурсивный процесс имеет короткий переходной нелинейный участок L_m, не превышающий *n* ($L_m \le n$), быстро исчезающий в результате феноменальной самосинхронизации, после которого формируемые на их основе последовательности $\{G_i\}$, причем, независимо от начальных условий $\{P_O, G_O\}$ и значений коэффициентов *H*, переходят в дихотомические с максимальным периодом $T_{max} = 2^n$ и с неповторяющимися в пределах периода составляющими ее элементами.

Ко всему этому, следует иметь в виду, что число разнообразных *Dh*-последовательностей, формируемых на основе указанных уравнений с прохождением переходного участка, равно $2^{4(n-1)}$, а не $2^{4(n-1)+n}$, как это кажется. Данный факт обусловлен процессом самосинхронизации и вызываемым им последовательным переходом в стационарное состояние, завершающимся с преодолением переходного участка L_m, при этом переход в стационарное состояние ведет к строгой биективной функциональной зависимости нелинейного дополнения *P* от базовой *G* переменной.

В программной и аппаратной реализации, с учетом представления нелинейных управляемых операций, задаваемых формулами (17) и (19), из уравнений (22) и (23) следуют два равнозначных по показателям алгоритма формирования *Dh*-последовательностей (Таб.2).

Таблица 2. ***Dh*-ГЕНЕРАТОРЫ. БАЗОВЫЕ ПРИМИТИВЫ**

Исходные данные: n – длина платформы генерации, бит.
Константы: MOD_N = $2^n - 1$ = (Cn – 1) | Cn при Cn = 1<< (n-1);
C_3 = MOD_N >> 2.
Начальные условия – {Po,Go} из интервала [0, MOD_N].
{Hp,Hg,Hc} - случайные числа в качестве коэффициентов.
Синхронизация коэффициентов:
Hg |= Cn, Hc |= Cn.
Исследуемые двоичные переменные:
G – базовая переменная;
P – нелинейное дополнение.
Управляющая переменная:
C = Hc ^ ((g>>1) & C_3).
Функция распространения влияния бит:
D(p,g) = g >> 3 – линейная функция;
D(p,g) = (p & (g >> 3)) | ((p ^ MOD_N) & (g >> 4)) – нелинейная функция.

1. Генерация псевдослучайных последовательностей	2. Генерация бесповторных ключей (идентификаторов и паролей)
g = G; p = P >>= 1; G ^= p; P = Hp ^ (g & p) ^ (C & G); p >>= 1; G ^= Hg ^ D(p,g); При использовании линейной функции D(p,g), алгоритм допускает существенное упрощение: g = G; P >>= 1; G ^= P; P = Hp ^ (g & P) ^ (C & G); G ^= Hg ^ (g >> 3); **Тестовые примеры генерации**, для двух крайних случаев, при использовании управляемой операции **AND**/**OR** – Hp = 0 и операции **NAND**/N**OR** – Hp = MOD_N, при n = 20 и нулевых начальных условиях Po = Go = 0, приведены на эпюрах Рис.15 и Рис.16 – для линейной функции распространения влияния бит, и Рис.17 и Рис.18 - для нелинейной функции, соответственно.	g = G; p = P; G ^= p; P = (Hp ^ (g & p) ^ (C & G)) >>1; p >>= 1; G ^= Hg ^ D(p,g); При использовании линейной функции D(p,g): g = G; G ^= P; P = (Hp ^ (g & P) ^ (C & G)) >>1; G ^= Hg ^ (g >> 3); **Тестовые примеры генерации** – не приводятся, т.к. всего лишь отличаются отображением нелинейного дополнения со смещением вправо на 1.

Примечание.
Представленные алгоритмы допускают параллельную обработку по каждому значащему биту входящих в их состав переменных, со скоростью, соизмеримой с исполнением одной элементарной двоичной операции, типа XOR.

Для аппаратной реализации *Dh*-генераторов с линейной функцией распространения влияния бит (легковесных), без учета триггеров организации итерации, требуется - $5.5 \cdot n$ GE, а с нелинейной функцией (минималистских) - $7.5 \cdot n$ GE.

Длина ключа, при исключении зависимости выхода от изменений на переходном участке, составляет $4 \cdot (n-1)$, а в случае введения зависимости выхода - $5 \cdot (n-1)$.

Для получения *Dh*-последовательностей, отображаемых базовой переменной – *G*, требуется *n* холостых итераций, позволяющих гарантированно исключить наблюдаемые на эпюрах переходные участки. Формируемые таким образом *Dh*-последовательности будут иметь максимальный период $Tmax = 2^n$, с неповторяющимися в пределах периода элементами.
Ко всему, как показывает статистический анализ [9], старшие значащие разряды базовой – *G*, начиная с 26-го, независимо от начальных условий и модификаторов {Hp,Hg,Hc}, имеют статистические свойства, мало отличающиеся от свойств, присущих истинно случайным величинам.

Первый из алгоритмов, представляемый формулами (23), в первую очередь ориентирован на реализацию *Dh*-генераторов [20], выступающих в качестве исходных для формирования истинно случайных и псевдослучайных последовательностей, шифрирующих гамм и реализации протоколов односторонней и взаимной аутентификации

Второй из алгоритмов реализации *Dh*-генераторов (22), ориентирован на формирование последовательностей бесповторных *n*-разрядных ключей (идентификаторов и паролей).

Dh-генераторы и формируемые на их основе последовательности, как уже отмечалось, носят однонаправленный, ламинарный характер, при котором несущественные изменения в младших разрядах, приводят к существенным, экспоненциально наращиваемым изменениям в старших разрядах. Такая зависимость представляет особый смысл и особую ценность для реализации криптографических примитивов поточного типа, строящихся посредством усечения младших значащих бит. Ко всему, если обратить внимание на зависимости (22) и (23), следует констатировать факт, что даже самая несущественная перестановка одного неусекаемого бита, способна привести к существенным изменениям выхода.

По данным исследований, имеется целый класс преобразований не сказывающийся на технических показателях, позволяющих получить результирующие последовательности, с обращением высокой функциональной сложности, сравнимой с полным перебором ключей.

Указанные преобразования требуют несущественных программных и крайне малых дополнительных аппаратных затрат, составляющих в разных случаях, например, для поточных шифров от 8 до 16 GE. По данным расчетов, производительность поточных шифров на имеющейся базе, может составлять, около 10 Гбит/сек.

Если распространять регулярный рандомизационный способ на примитивы блочного типа, следует признать, что очевидным недостатком регулярного рандомизационного способа является неравночастотный характер изменения бит, с периодом. $T_k = 2^k$ ($k = \overline{1,n}$).

Для примера, одним из способов устранить указанный недостаток, позволяет следующая функция выхода сюръективного типа, с представляемой ею результирующей R переменной:

$$R_i = \mathbf{rot}L_C(R_{i-1}) \oplus G_{i-1} \oplus P_{i-1}, \qquad (27)$$

с циклическим сдвигом – c, равным ближайшему взаимно простому к $n/2$.

Результаты генерации 20-ти разрядных равночастотных последовательностей, для линейной и нелинейной функции распространения влияния бит и нелинейной управляемой операции NAND/NOR, представлены на эпюрах, Рис.19 и Рис.20, в Приложении.

Анализ [9] показывает статистическую надежность по каждому из разрядов, начиная с 21 разрядных платформ. К этому, для реализации функции выхода требуется $3 \cdot n$ GE. Длина ключа увеличивается на n бит за счет выбора начального условия R_O.

Для генерации бесповторных ключей, функция выхода должна иметь биективный характер. В связи с этим, построение стойких в криптографическом отношении генераторов бесповторных ключей – задача не тривиальная.

Между тем, задача решена в расчете на производительность от одного, до нескольких десятков миллиардов ключей в секунду, вне зависимости от их разрядности, при длине секретного ключа около $8 \cdot n$ и общих аппаратных затратах, порядка $16.5 \cdot n$ GE. В такой постановке, при использовании соответствующей микросхемы, можно отказаться от хранения ключей и с ее помощью успешно противостоять массированным атакам на отказ от обслуживания.

Существенным моментом решений на основе *Dh*-генераторов является разработка минималистских и легковесных протоколов односторонней и взаимной аутентификации поточного типа, рассчитанных на среды с крайним дефицитом ресурса, такие как метки RFID, как кремниевые, так и органические.

Расчеты показывают, что для реализации таких протоколов, минимальная длина платформы составляет 10 бит, а для реализации требуется около $3 \cdot n$ триггеров и порядка $5.5 \cdot n$ GE. Собственно, при таких аппаратных затратах, для введения протоколов аутентификации оказывается достаточным имеющийся резерв на кристалле, что в свою очередь не ведет к увеличению стоимости промышленного производства радиочастотных меток. Более того, использование потокового протокола, не только не ведет к уменьшению радиуса действия меток, но и наоборот, позволяет его увеличить, за счет более эффективной реализации радиочастотного интерфейса и способов обработки сигналов.

Регулярный рандомизационный способ допускает ***мультипликативное комплексирование с* LFSR**, при этом обратное не верно. При существенном улучшении статистических показателей, период повторения таких последовательностей составляет $2^n \cdot (2^n - 1)$.

В этом плане необходимо отметить, что такое комплексирование в полном объеме и на высоком качественном уровне устраняет недостатки присущие реализации нелинейных регистров с обратной связью - **NFSR** [8], а с ним и реализации *Dh*-генераторов в целом.

4.2 Нерегулярный рандомизационный способ

Как уже отмечалось, в силу дихотомических свойств [17], присущих *Dh*-генераторам, изменения битов формируемых на их основе последовательностей носят неравночастотный характер, с периодом 2^k ($k = \overline{1,n}$), что делает младшие биты фактически непригодными для прямых практических приложений. Более того, если говорить в целом, такой неравночастотный характер изменения бит, делает *Dh*-генераторы непригодными для построения криптографических примитивов блочного типа.

Устранить указанный недостаток позволяют генераторы с обратной связью по выходу и по нелинейному дополнению, далее именуемые как ***рандомизационные R-генераторы***. Не вдаваясь в детали, организация обратных связей дело тонкое, т.к. может вести к образованию последовательностей с коротким периодом или к их вырождению. Оставим рассмотрение этой темы на будущее. Здесь же, для общей информации, приведем два примера.

Для организации обратной связи по выходу, выберем два младших бита $W_{12} = R_{i-1} \,\&\, 3$, входящих в выражение (27) и введем их в уравнения (23):

$$P^* = P'_i \lessdot_1, \quad G_i = H_G \oplus G_{i-1} \oplus P^* \oplus (G_{i-1} \lessdot_3) \oplus W_{12} \mod 2^n, \quad P'_i = H_P \oplus (G_{i-1} \&^{C_H} P^*). \quad (28)$$

Во втором случае используется второй бит $W_2 = R_{i-1} \,\&\, 2$ выхода и обратная связь по биту переполнения нелинейного дополнения P:

$$P^* = \mathbf{rot}L_1(P'_i), \quad G_i = H_G \oplus G_{i-1} \oplus P^* \oplus (G_{i-1} \lessdot_3) \oplus W_2 \mod 2^n, \quad (29)$$
$$P'_i = H_P \oplus ((G_{i-1} \oplus W_2) \&^{C_H} P^*).$$

Результаты работы 20-ти разрядных R-генераторов, построенных на основе уравнений (28) и (29), приведены на эпюрах, Рис.21 и Рис.22, в Приложении. Анализ [9] показывает равночастотный характер изменения выходных бит R-генераторов, начиная с 18 разрядных платформ.

В отличие от поточных, ***производительность блочных шифров растет линейно с увеличением длины платформы генерации*** и для платформ длиной свыше $n = 64$ бит, может достигать сотни и тысячи Гбит/сек.

Заключение

Все результаты, подтверждаются на детально выверенных моделях разработанных автором, а также независимыми исследованиями [15,20,21] и предварительной экспертизой [20,22], которые могут быть легко воспроизведены, не только владеющими основами программирования начинающими учеными и специалистами среднего профиля, но и творческой молодежью.

Приведенные примеры указывают на возможность достижения предельно высокой производительности криптографических примитивов (от сотен до тысячи Гбит/сек, за счет полного параллелизма, неограниченного наращивания длины платформ и скорости обработки, сравнимой со скоростью срабатывания транзисторов типовых микросхем), отличающихся от аналогов существенно меньшими энергетическими и аппаратными затратами (от 120–150 GE) и на порядки меньшей себестоимостью схем реализаций.

Хотя данное направление еще молодо, но в прикладной части уже хорошо развито и доведено до схемотехнических решений [20,21] необходимых для изготовления минималистских и легковесных высокорентабельных промышленных образцов, по статистическим, функциональным и техническим показателям, недостижимо далеко опережающим известные на сегодня аналоги.

К недостаткам данной работы можно отнести явное отставание теории от практики (как видится по имеющимся заделам, это дело времени), а также следующие обстоятельства.

Элементарный анализ *Dh*-генераторов, представляемых уравнениями (22) и (23), показывает, что такие генераторы не являются криптографически стойкими и просто вскрываются, при движении от младших разрядов к старшим разрядам. Ко всему, *Dh*-генераторы представленные уравнениями (22) уязвимы к дифференциальному криптографическому анализу. К слову, прямое аналитическое вскрытие и уязвимость к дифференциальному анализу можно устранить за счет использования двухмерных односторонних функций [15,20,24], правда, на это понадобится в два раза больше аппаратных затрат.

Предварительно проведенный анализ указывает на ***возможность достижения высокой криптографической стойкости на основе усеченных Dh-генераторов***. Ведутся работы [20] по строгому доказательству этого ключевого положения.

Источники информации

1. Микросенсорные (RFID, SMART) технологии и Кибер-сети. Обеспечение безопасности.
   http://www.gosbook.ru/node/58365,
   Госбук - экспертная сеть по вопросам государственного управления. Рабочая группа:
   http://www.gosbook.ru/gosblock_page/group-activities/tab/group-activities_all/51114
2. Предарифметика, Стохастический метод и Стохастические технологии.
   http://t.random-art.ru/recommendation/. Тематический сайт: http://random-art.ru/
3. Advanced Encryption Standard. http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
4. International Association for Cryptologic Research. http://www.iacr.org/
5. Network of Excellence in Cryptology. http://www.ecrypt.eu.org/ecrypt1/
   European Network of Excellence in Cryptology II ECRYPT II. http://www.ecrypt.eu.org/
6. Building Radio Frequency IDentification for the Global Environment (BRIDGE).
   http://www.bridge-project.eu/
7. Решения Cisco с шифрованием на втором уровне.
   http://www.cisco.com/web/RU/news/releases/txt/2012/103012a.html
8. B. Schneier, Applied cryptography.
   2nd Edition, John Wiley & Sons (1996).
9. Marsaglia G. DIEHARD Tests, 1997, http://en.wikipedia.org/wiki/diehard_tests/
   A Statistical Test Suite for the Validation of Pseudorandom Number Generators.
   NIST Special Publication 800-22, (FIPS PUB 140-1,2). NIST, 2001.
10. Иванов М.А. Криптографические методы защиты информации в компьютерных
    системах и сетях. КУДИЦ-ОБРАЗ, Москва, 2001.
11. Самые быстрые генераторы случайных чисел. Решения от Intel и прогнозы развития.
    http://www.gosbook.ru/node/56317
    Intel® Security Driver: http://www.intel.com/design/software/drivers/platform/security.htm
    Random Number Generators (Entropy Sources): http://random-art.ru/ra_gn/
12. Donald E. Knuth, The Art of Computer Programming,
    vol.2, 3rd Edition, Addison-Wesley, 1997.
13. Greenberger M. Notes on a New Pseudo-Random Number Generator.
    Massachusetts Institute of Technology, Cambridge, Mass., 1960.
14. Brickell et al. A Surkey of Recent Results.
    Proc. of the IEEE, Vol. 76, no. 5, May 1988.
15. Способ придания реальным объектам рандомизационных свойств и рандомизационная
    система.
    International Patent Application PCT/RU03/00141 dated 7 April 2003,
    Eurasian Patent Application No. 200500946 dated 11 July 2005.
16. Кулаков И.А. Полиномиальный конгруэнтный метод с переменными коэффициентами и
    его нелинейные расширения.
    Рукопись статьи, Москва, 2012, http://random-art.ru/?download=LCM_ru.pdf
17. Кулаков И.А. Стохастическая криптография. Дихотомические последовательности и их
    свойства.
    Рукопись статьи, Москва, 2012, http://random-art.ru/?download=Dh_Sqn_New.pdf
18. Глухов М. М., Елизаров В. П., Нечаев А. А. АЛГЕБРА.
    М.: Гелиос АРВ, 2003.
19. Кулаков И.А. Рандомизационный метод.
    Москва, 2011, http://random-art.ru/random_method/
20. Регулярный рандомизационный способ. Анализ и аналитика.
    Москва, 10 декабря 2012. http://t.random-art.ru/?download=PPC%20Patent.pdf
    International Patent Application «A Method for Forming Regular Binary Sequences»
    № PCT/RU2011/000648 dated 26 August 2011.
    Publication No. WO 2013/028095 dated 28 February 2013.
    Российский патент № 2469382, Бюллетень № 34 от 10 сентября 2012.
21. Нерегулярный рандомизационный способ. Анализ и аналитика.
    Москва, 10 декабря 2012. http://t.random-art.ru/?download=HPC%20Patent.pdf
    International Patent Application «A Method for Forming Non-Regular Binary Sequences»
    № PCT/RU2011/000647 dated 26 August 2011.
    Publication No. WO 2013/028094 dated 28 February 2013.
    Российский патент № 2467378, Бюллетень № 32 от 20 ноября 2012.
22. Стохастические системы и криптография.
    Материалы конференции РусКрипто 2006, Москва, 3-5 февраля, 2006.
    http://random-art.ru/?download=RusCrypto.pdf
23. Предарифметика. Теория чисел.
    Рукопись статьи, май 2011, http://random-art.ru/?download=predarifmetics.pdf
24. Кулаков И.А. Линейные конгруэнтные и рандомизационные генераторы.
    Рукопись статьи, Москва, 2012, http://random-art.ru/?download=LCG_RNG_ru.pdf

Приложение

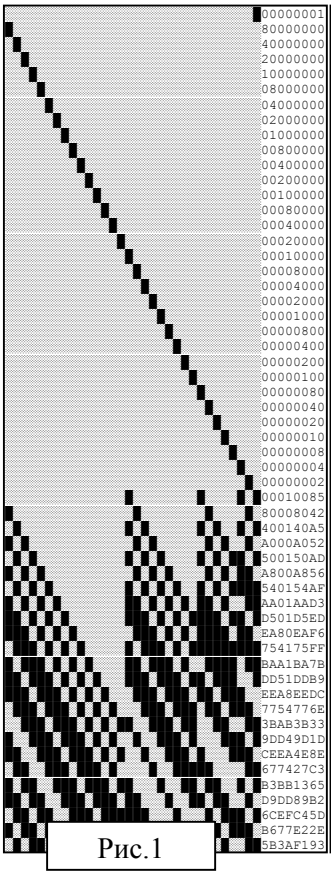

Рис.1

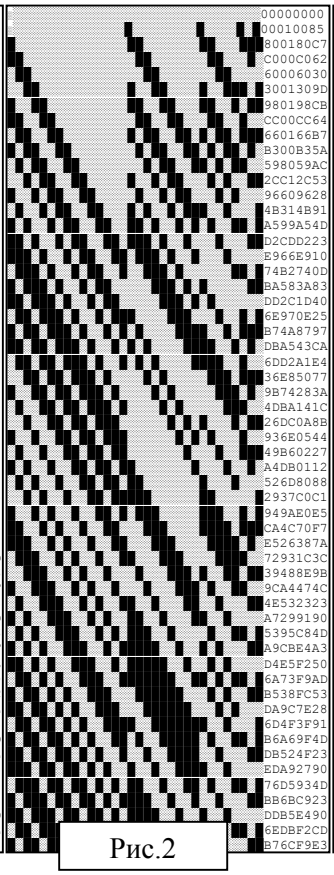

Рис.2

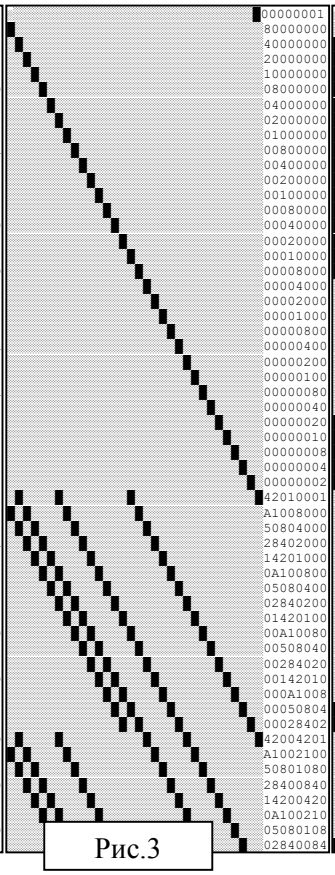

Рис.3

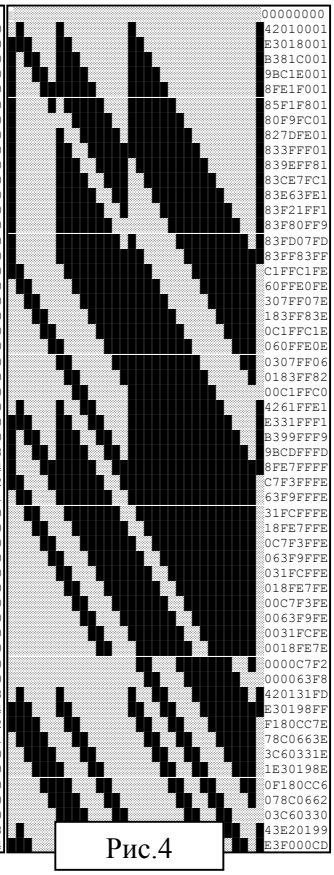

Рис.4

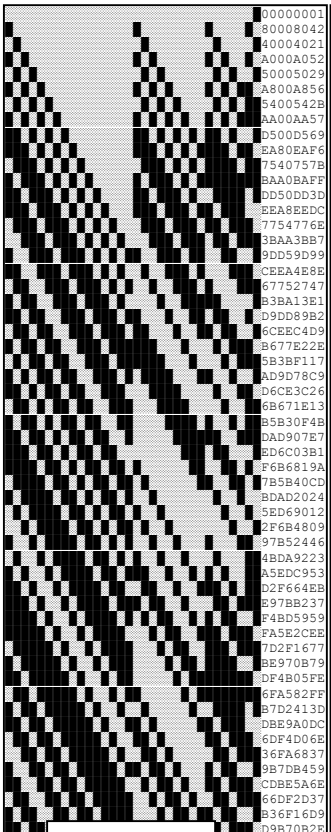

Рис.5

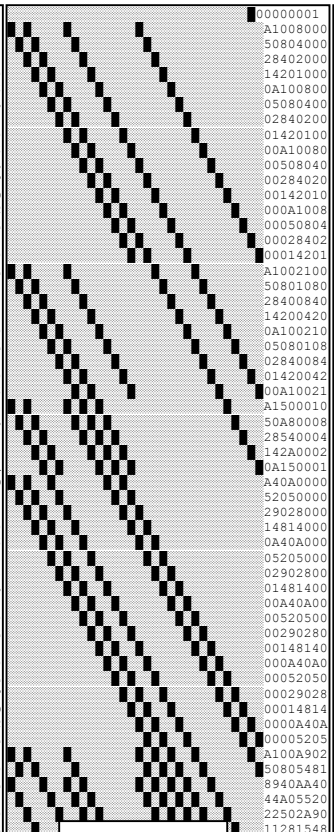

Рис.6

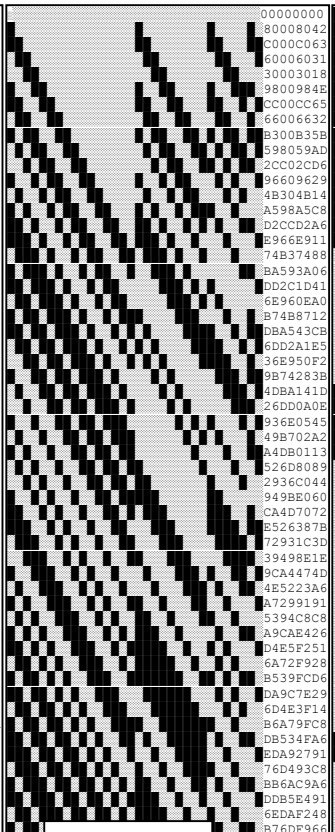

Рис.7

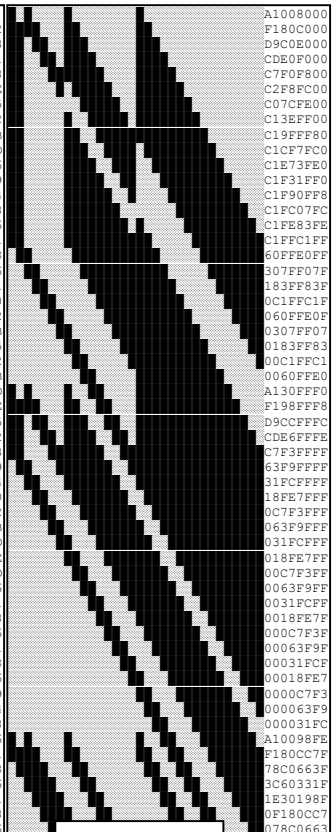

Рис.8

Линейный конгруэнтный метод (LCM) с переменными коэффициентами

Исходные данные:

n – длина платформы генерации, бит.

Rx, Ra, Rb – задающие параметры генератора, общей длиной = n + (2·n – 3) бит.

RHa, RHb – компоненты ключа генерации, общей длиной = 2·n – (5÷6) бит.

Синхронизация параметров генератора:

x = Rx; a = Ra | 3; b = Rb | 1;

Ha = (RHa | 7) ^ 3; Hb = (RHb | 7) ^ 3;

x – результирующая переменная конгруэнтного генератора.

Ha, Hb – приращения коэффициентов генерации.

Полная длина ключа генерации:

k = n + (2·n – 3) + (2·n – (5÷6)) = 5·n – (8÷9) бит.

Каждый из ключей генерации специфицирует уникальную двоичную конгруэнтную последовательность, с периодом 2^n. В пределах периода, элементы последовательности бесповторны.

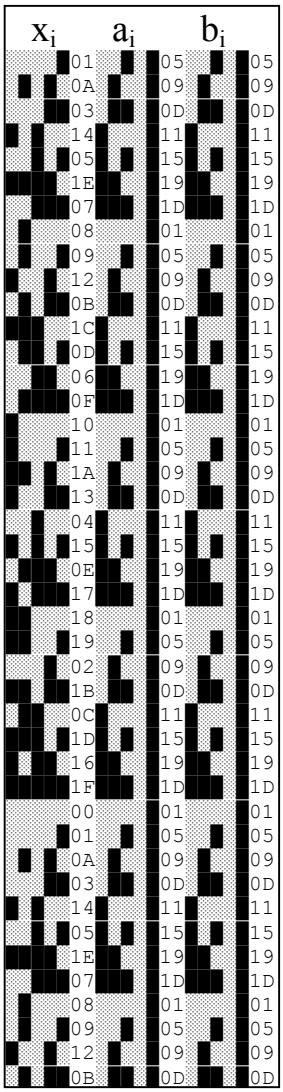

Рис. 9

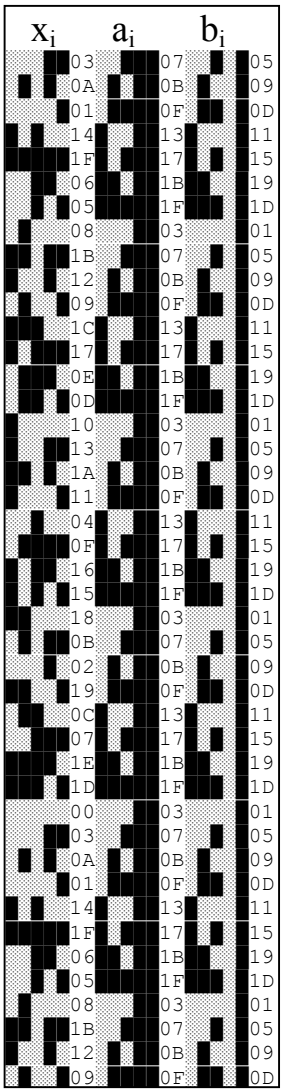

Рис. 10

Типовой пример реализации LCM

Предварительная синхронизация множителя: a ^= 2;

Формирование очередного элемента конгруэнтной последовательности:

x = (a*x + b) & MOD_N; (MOD_N = 2^n – 1)

a += Ha; b += Hb;

Тестовый пример генерации (см. эпюру на Рис.9), при *n* = 5.

Начальные условия: x = 0; a = 1; b = 1; Ha = 4; Hb = 4;

Типовой пример реализации нелинейного расширения LCM

Формирование очередного элемента конгруэнтной последовательности:

x = (a*(x ^ b)) & MOD_N; (MOD_N = 2^n – 1)

a += Ha; b += Hb;

Тестовый пример генерации (см. эпюру на Рис.10), при *n* = 5.

Начальные условия: x = 0; a = 3; b = 1; Ha = 4; Hb = 4;

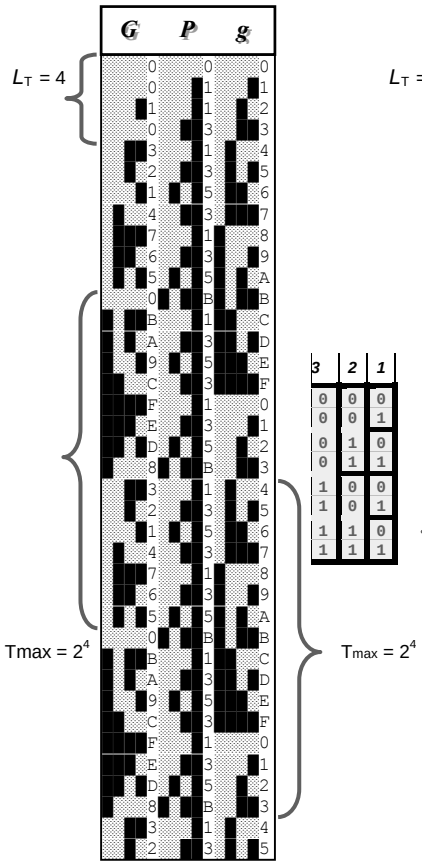

Рис. 11

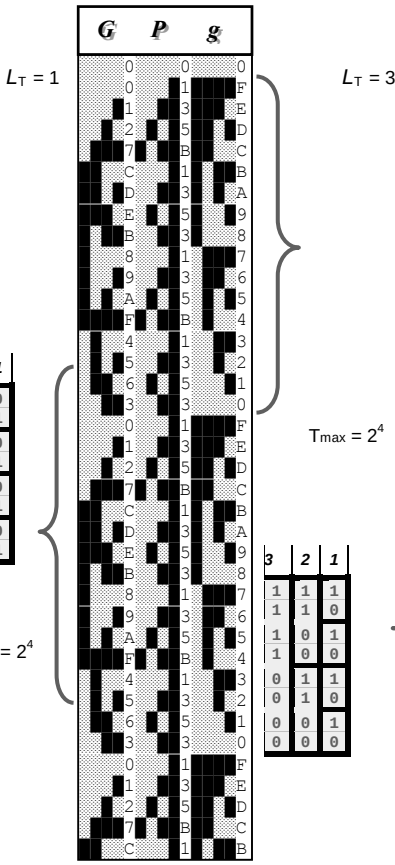

Рис. 12

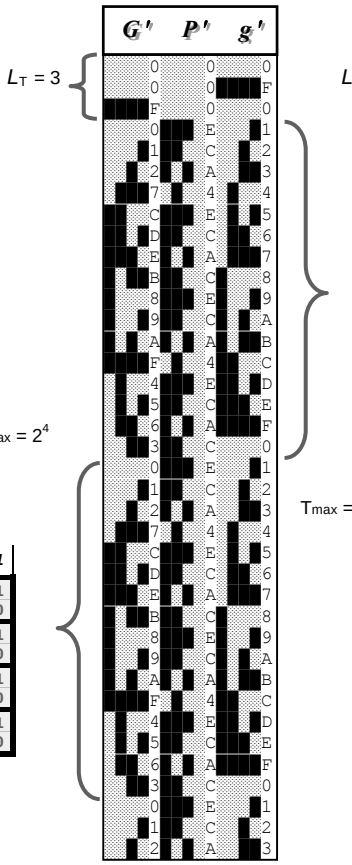

Рис. 13

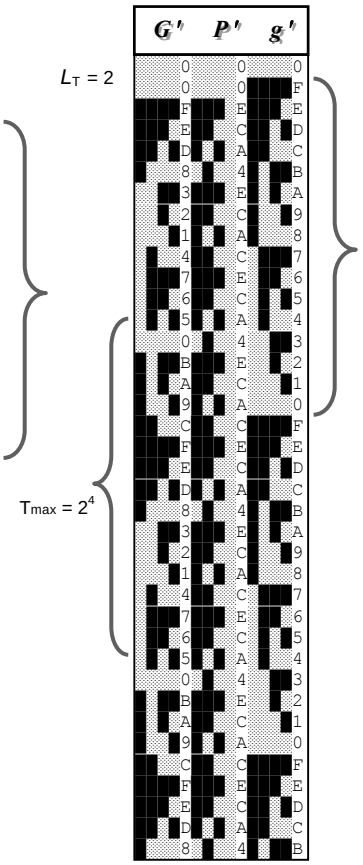

Рис. 14

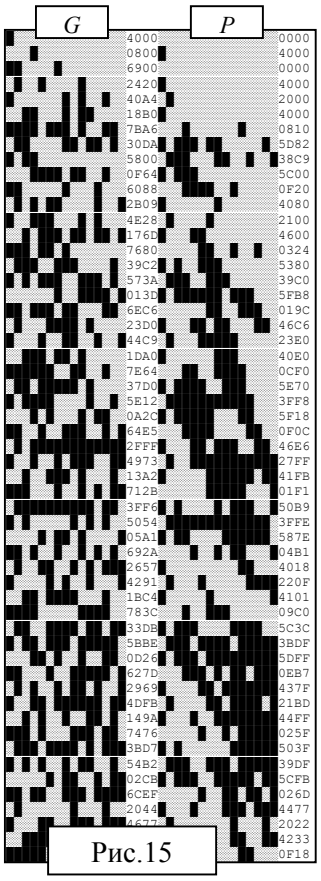

Рис.15

Рис.16

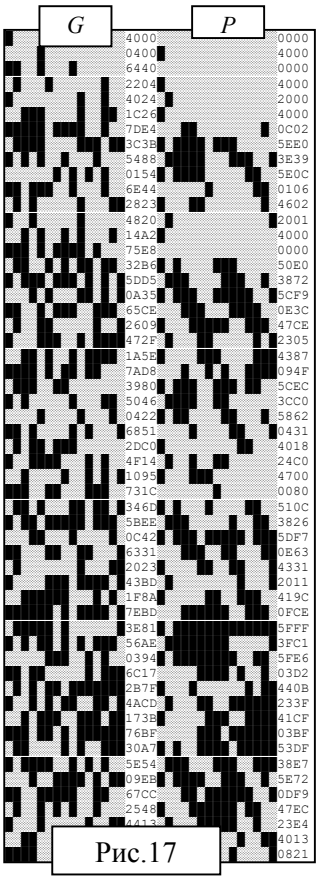

Рис.17

Рис.18

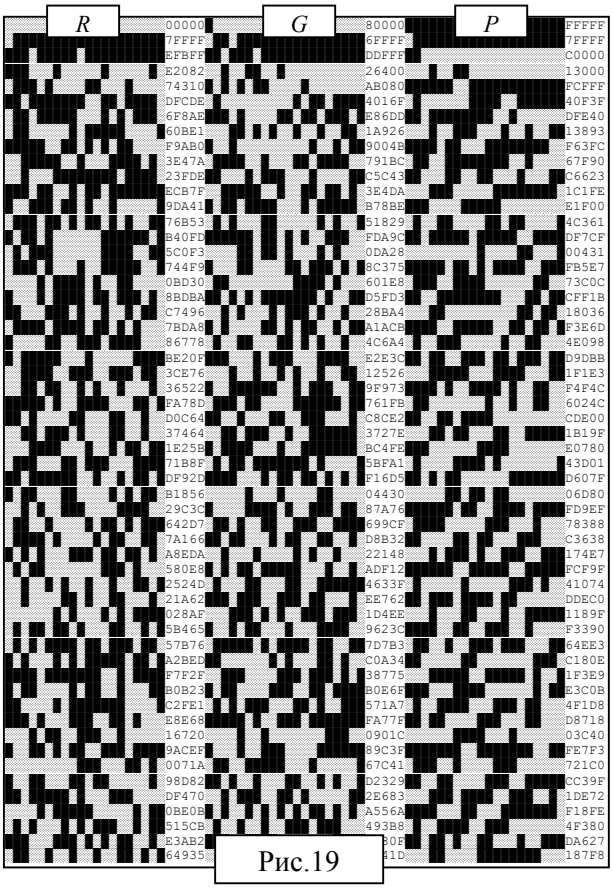

Рис.19

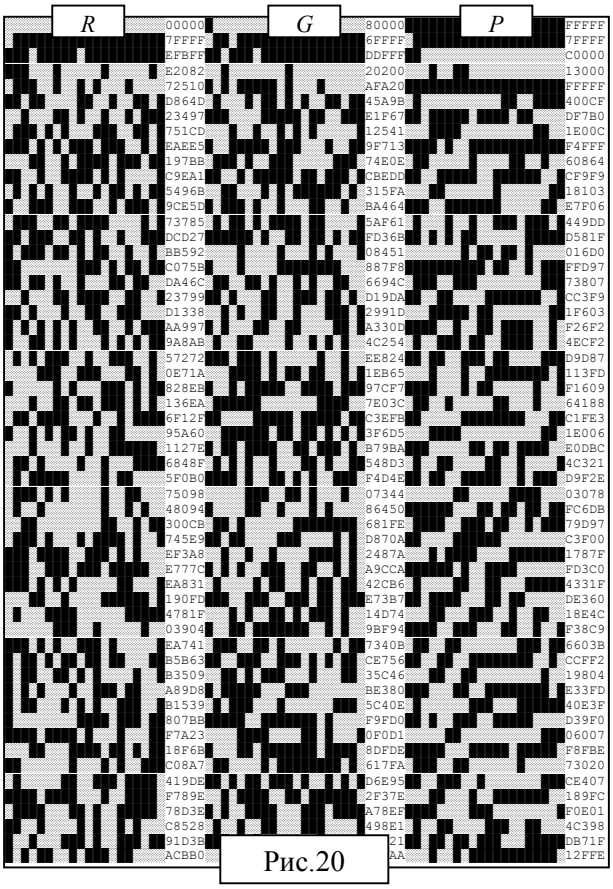

Рис.20

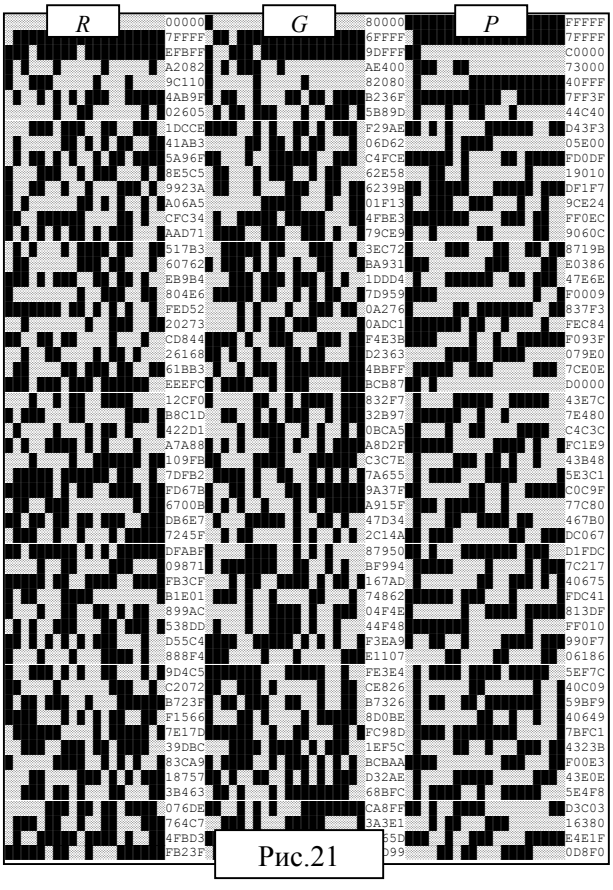

Рис.21

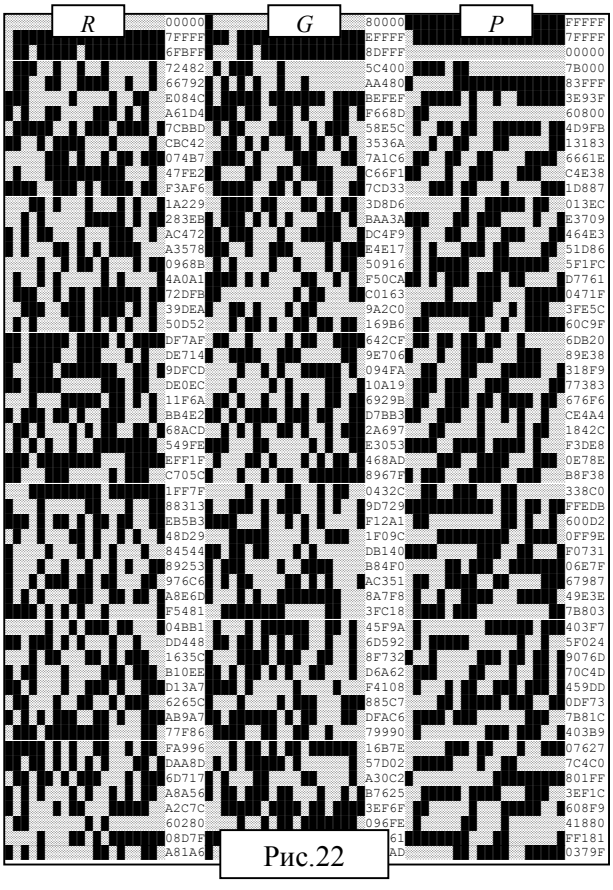

Рис.22