РАНДОМИЗАЦИОННЫЕ ГЕНЕРАТОРЫ

Кулаков Игорь Анатольевич.

Random Art Labs Limited
chief@random-art.com

Рассматриваются новые способы формирования последовательностей (псевдо) случайных чисел, с любым наперед заданным периодом повторения. Приводятся алгоритмы реализации высокоскоростных, одно- и многоразрядных, допускающих эффективную параллельную обработку бесповторных и равноповторных генераторов случайных чисел. Даются условия достижения их высокой криптографической стойкости. Дается анализ их функциональной и статистической надежности.

В статье приводятся новые результаты, полученные в области построения стохастических систем и криптографии [1]. Основное внимание уделяется практическим аспектам реализации высоко скоростных, простых в программном и аппаратном исполнении, статистически надежных и криптографически стойких генераторов случайных чисел, как одним из наиболее важных составляющих элементов симметричной криптографии и стохастических систем.

Основу представленных здесь генераторов случайных чисел составляют дихотомические или *Dh*-генераторы [3]. Последние из них предназначены для формирования последовательностей специального вида, так называемых *дихотомических последовательностей* [2].

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

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

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

Из образованной таким образом двоичной последовательности видно, что период повторения T_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, i и $(i+T_k/2)$ элементы принадлежащие соседним полупериодам этой последовательности комплементарны

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

т.е. связаны между собой операцией комплементации $\overline{\ }$ *НЕ*.

Указанные свойства именуются *дихотомическим порядком* и *дихотомическим комплементом* элементов данной последовательности, соответственно.

Дихотомические генераторы в пределах своего периода повторения T_n, равного 2^n, носят бесповторный характер. Либо имеют небольшой переходной участок (аттрактор), после которого они феноменальным образом приходят в стационарное состояние и далее всюду ведут себя как бесповторные, в пределах периода $T_n = 2^n$. *Dh*-генераторы могут быть многомерными и параметрическими, способны образовывать структурные композиции любой сложности и могут иметь любой, сколь угодно большой период повторения. Анализ показывает, что на основе таких генераторов возможно достижение функциональной неразрешимости по существу, со стороны старших битов формируемых на их основе псевдослучайных последовательностей [3].

Дихотомические последовательности, формируемые на основе указанных генераторов, могут быть усечены со стороны младших значащих бит. При таком усечении, указанные последовательности утрачивают бесповторные свойства.

Для оценки общего числа повторений, рассмотрим двоичную последовательность $B = \{b_k: k = \overline{1, L}\}$, длиной L, составленную из элементов $b_k \in \{0,1\}$. Разобьем эту последовательность на равные блоки s_i, длиной n. Положим длина $L = n \cdot T_n$, при этом $T_n = 2^n$. Каждому блоку $s_i = \{b_j: j = (i-1) \cdot n + k, i = \overline{1, T_n}, k = \overline{1, n}\}$, образованной таким образом новой, *n-разрядной двоичной последовательности* $S_n = \{s_i: i = \overline{1, T_n}\}$, соответствует некоторое свое n-разрядное двоичное число $s_i \in [0, T_n - 1]$.

Положим, что эта последовательность, есть одна из реализаций составленной из n значащих бит случайной величины ξ. Будем различать *бесповторные* и *равноповторные* случайные величины.

Случайные величины ξ, все реализации S_ξ которых не содержат в пределах своего периода T_n равных между собой элементов, либо начиная с некоторого очередного элемента с номером $i_\xi \le h$, не превосходящего некоторого порогового значения h, самостоятельно приобретают бесповторные свойства, называются *бесповторными величинами*, а сами реализации *бесповторными последовательностями*.

Случайные величины не являющиеся бесповторными, для реализаций которых число повторений любых из чисел $s_i \in [0, T_n - 1]$ этой последовательности равновероятны, будем называть *равноповторными величинами*, а формируемые на их основе реализации *равноповторными последовательностями*.

Для оценки общего числа повторений в таких последовательностях, вычислим показатель

$$E_n = \left(\frac{T_n}{T_n - 1} \right)^{T_n}.$$

Существует предел $e = \lim_{T_n \to \infty} E_n$, при котором с возрастанием n, показатель E_n быстро стремиться к числу Эрмита $e = 2{,}718\,281\ldots$.

На основе исследований ρ-разрядных D-последовательностей S_ρ, усеченных на ε их младших значащих бит, иначе *усеченных* n-разрядных дихотомических последовательностей $S_n \subset S_\rho$ $(n = \rho - \varepsilon)$, замечено, что общее среднее число повторений r_n двоичных чисел в данной последовательности S_n, при длине статистической выборки 2^n, равно

$$r_n = \frac{2^n}{C_\varepsilon}, \quad C_\varepsilon = \left(\frac{T_\varepsilon}{T_\varepsilon - 1} \right)^{T_\varepsilon}$$

при $T_\varepsilon = 2^\varepsilon$.

Выражая r_n через вероятность общего числа повторений P_n, при равновероятном размещении T_n различных n-разрядных двоичных чисел среди всех T_n элементов последовательности S_n,

$$r_n = 2^n P_n,$$

имеем

$$P_n = \frac{1}{C_\varepsilon}.$$

На основе экспериментальных результатов и их аппроксимации, установлено аналитическое выражение *эмпирического закона* распределения общего числа повторений $r_{(n-k)}$:

$$r_{(n-k)} = 2^{n-k} P_n \prod_{i=0}^{k} 2^{-\frac{Q_i}{Q_i + Q_n}} \qquad (k = \overline{0, n-1}), \tag{1}$$

в статистической выборке $S_{(n-k)} \subseteq S_n$, составленной из 2^{n-k} n-разрядных двоичных чисел $s \in S_{(n-k)}$, с аргументом Q задаваемым рядом $\{Q_i: i = \overline{0, k}\} = (0, 1, 2, 4, 6, \ldots p_k - 1\}$, при $p_0 = 1$, исходя из множе-

ства простых чисел p и постоянной распределения Q_n, равной

$$Q_n = \frac{1 - \frac{2}{T_\varepsilon}}{1 + E_n}.$$

При $r_{(n-k)} \le 1$, можно вычислить вероятность повторения чисел $P_{(n-k)}$, в статистической выборке $S_{(n-k)}$ длиной 2^{n-k}

$$P_{(n-k)} = r_{(n-k)} / 2^{n-k}.$$

При больших $k \ge 8$, вероятность повторения чисел $P_{(n-k)}$, можно оценить по формуле

$$P_{(n-k)} \approx 1/2^{k+1}.$$

В частности, отсюда следует. Вероятность того, что два соседних числа последовательности S_n совпадут, в этом случае $k = n - 1$, равна $1/2^n$.

Оценка величин отклонений общего числа повторений, получаемых на основе эмпирического закона $r_{(n-k)}$ и экспериментальных данных $r^*_{(n-k)}$, при различных длинах 2^{n-k} $(k = \overline{0, n-1})$ статистической выборки $S_{(n-k)}$, осуществляется на основе относительных погрешностей $\delta_{(n-k)}$, вычисляемых по формуле:

$$\delta_{(n-k)} = \frac{r_{(n-k)} - r^*_{(n-k)}}{r_{(n-k)}} \cdot 100\%,$$

Для повышения точности вычислений, вводятся средние относительные погрешности $\Delta_{(n-k)}$, вида:

$$\Delta_{(n-k)} = \frac{r_{(n-k)} - R^*_{(n-k)}}{r_{(n-k)}} \cdot 100\%,$$

рассчитываемые исходя из экспериментальных данных $R^*_{(n-k)}$, полученных по m независимым реализациям $S_{i,(n-k)}$ $(i = \overline{1, m})$, путем усреднения

$$R^*_{(n-k)} = \frac{1}{m} \cdot \sum_{i=1}^{m} r^*_{i,(n-k)},$$

результатов $r^*_{i,(n-k)}$, полученных по каждой из них.

Для проведения сравнительного анализа экспериментальных и эмпирических результатов, использовался дихотомический генератор [3] усеченный на ε младших значащих бит, с 16-ти разрядным выходом $r_i = (B_{i-1} \oplus D_{i-1})/2^\varepsilon \bmod 2^{16}$, задаваемый самосинхронизирующимся параметрическим $\{P,D,Q\}$ рандомизационным оператором $R(P_{i-1},D_{i-1},Q_{i-1})$: $B_{i-1} \to \{B_i,P_i,D_i,Q_i\}$, составленным из операторов:

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

Кроме этого, проведен статистический анализ распределения числа повторений в последовательностях, формируемых на основе генератора псевдослучайных чисел RC4 и блочного шифра ГОСТ 28147-89, функционирующим в режиме обратной связи по выходу, а также представленного ниже рандомизационного генератора гаммы. Для анализа таких генераторов, следует принять

$$C_\varepsilon = E_n.$$

Расчеты по 500 статистическим выборкам, при различном числе усекаемых бит и различных объемах статистических выборок, приведены в таблице 1.

Table 1. Testing of repeation number

Statistical sample		65536	32768	16384	8192	4096	2048	1024	512	256	128
Truncation	**Estimates**										
1 bit	Empiric	**16384**	4096	1024	256	64	16	4	1	0.25	0.06
	Mean	16350	4043	1011	250	62	16	4	1	0.21	
Ratio Error	Δ (%)	0.209	1.288	1.313	2.190	3.069	-0.16	-5.65	-21.8	17.6	
2	Empiric	**20736**	5628	1470	376	95	24	6	2	0.38	0.10
	Mean	20708	5632	1469	375	95	24	6	2	0.35	0.03
	Δ (%)	0.136	-0.073	0.067	0.139	0.302	-1.27	-3.96	-7.69	9.17	
3	Empiric	**22519**	6324	1685	435	111	28	7	2	0.45	0.11
	Mean	22458	6308	1669	430	111	28	7	2	0.35	0.03
	Δ (%)	0.270	0.264	0.932	1.251	0.704	0.24	1.01	-6.14	23.7	
4	Empiric	**23336**	6657	1790	465	119	30	8	2	0.49	0.12
	Mean	23303	6657	1788	463	118	31	8	2	0.40	0.02
	Δ (%)	0.139	0.012	0.115	0.359	1.516	-0.97	-5.49	-2.58	17.4	
6	Empiric	**23920**	6901	1869	487	125	32	8	2	0.52	0.13
	Mean	23923	6909	1866	485	125	31	8	2	0.40	0.04
	Δ (%)	-0.014	-0.118	0.146	0.481	0.483	2.11	2.23	4.92	22.2	
8	Empiric	**24062**	6961	1888	493	127	32	8	2	0.52	0.13
	Mean	24049	6954	1877	489	124	32	8	2	0.45	0.03
	Δ (%)	0.053	0.109	0.574	0.836	1.926	2.30	3.15	0.07	13.7	
10	Empiric	**24098**	6976	1893	494	127	32	8	2	0.53	0.13
	Mean	24099	6977	1886	492	124	32	8	2	0.42	0.04
	Δ (%)	-0.007	-0.006	0.397	0.566	2.342	1.88	1.78	7.61	19.3	
13	Empiric	**24108**	6981	1895	495	127	32	8	2	0.53	0.13
	Mean	24105	6979	1887	492	125	31	8	2	0.45	0.05
	Δ (%)	0.011	0.017	0.389	0.586	1.808	3.17	3.98	3.18	14.0	
16 bits	Empiric	**24109**	6981	1895	495	127	32	8	2	0.53	0.13
	Mean	24110	6984	1888	493	126	32	8	2	0.47	0.04
	Δ (%)	-0.003	-0.036	0.355	0.400	1.435	2.69	4.94	6.94	9.88	
Equirepeated Empiric Distribution Law		**24109**	**6981**	**1895**	**495**	**127**	**32**	**8**	**2**	**0.53**	**0.13**
RC4	Mean	24108	6981	1886	490	126	31	8	2	0.42	0.05
	Δ (%)	0.006	-0.001	0.465	0.901	1.282	4.15	5.65	3.86	20.5	
GOST	Mean	24113	6983	1885	492	125	31	8	2	0.42	0.04
	Δ (%)	-0.017	-0.026	0.522	0.563	1.526	3.15	5.18	2.81	19.8	
Randomization Generator	Mean	24106	6981	1885	490	124	32	8	2	0.46	0.06
	Δ (%)	0.013	-0.006	0.494	1.016	0.962	1.97	0.30	2.71	13.3	

Из представленной таблицы видно, что с увеличением числа усекаемых битов дихотомической последовательности, формируемой на основе уравнений (2), распределение числа повторений быстро сходится к распределению присущему генератору случайных чисел RC4 и блочному шифру ГОСТ. Небольшие отклонения, показывают достаточно высокую точность совпадения экспериментальных данных и эмпирических результатов. Учитывая высокие статистические показатели последовательностей формируемых такими генераторами, а также сюръективный характер используемых ими преобразований, можно говорить о “совершенном” равноповторном характере этих последовательностей. Далее, последовательности с законом распределения числа повторений близким к эмпирическому идеальному (1), будем называть с*овершенными равноповторными последовательностями*.

На основе дихотомических генераторов обладающих функциональной неразрешимостью по существу, можно построить криптографически сильные генераторы случайных чисел и другие стохастические устройства и системы, с заданными статистическими свойствами.

Решение этих задач - это тема раздела стохастической криптографии, включающего в себя задачи построения статистически и функционально надежных генераторов случайных чисел, однонаправленных функций, блочных шифров и других стохастических операторов. Далее рассматриваются способы построения на основе *Dh*-генераторов бесповторных и равноповторных генераторов случайных чисел, иначе *генераторов ключевого потока* и *генераторов гаммы*, объединенных под общим названием - *рандомизационные генераторы* [1]. Структурная схема *N*-канального *m*-разрядного рандомизационного генератора, с длиной платформы генерации $n = m \cdot N$ бит, приведена на Рис.1. Инициализация генератора осуществляется путем установки его начального состояния в соответствии с ключом. В последующем начальное состояние рандомизационного генератора, осуществляющего формирование бесповторного ключевого потока или равноповторной гаммы, иначе *рандомизационной последовательности*, а также начальное состояние используемого для генерации ключей дихотомического генератора может меняться в зависимости от значений используемых им модификаторов.

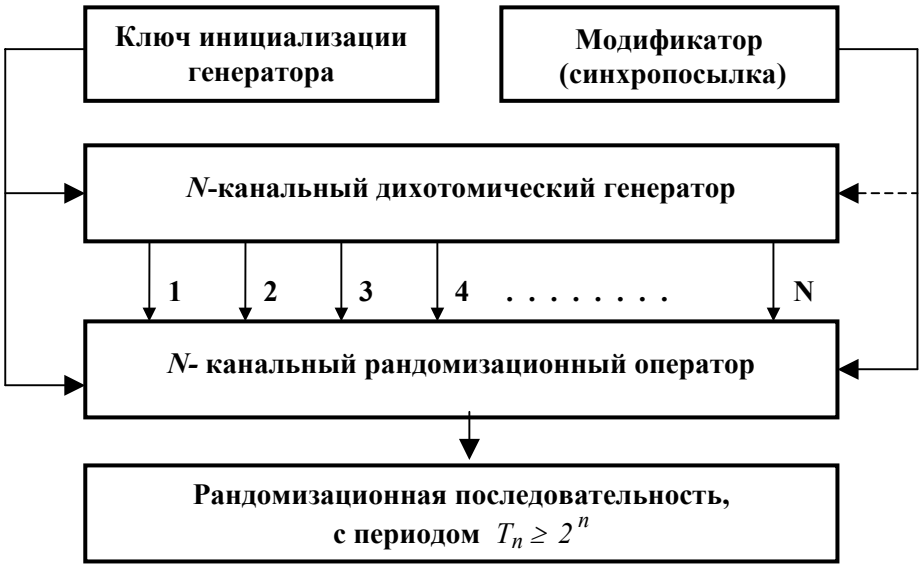

Рис.1

При анализе рандомизационных генераторов следует руководствоваться общими требованиями, предъявляемыми к генераторам (псевдо)случайных чисел. А именно, требованиями обеспечения статистической и функциональной надежности, при предельно возможном периоде формируемых на их основе случайных последовательностей [4].

Первое из требований исходит из проверки соответствия статистических свойств этих последовательностей “идеальному” равномерному закону распределения. С конструктивной точки зрения, будем говорить о *статистической надежности* рандомизационных генераторов, если формируемые ими последовательности удовлетворяют известным статистическим критериям, присущим упомянутому выше закону распределения [5], определенные на всем множестве допустимых начальных состояний генератора.

Второе требование обусловлено обеспечением криптографической стойкости рандомизационных генераторов и достигается за счет аналитической неразрешимости и статистической неопределенности уравнений генерации. Последние условия определяют *функциональную надежность* генератора, а именно, возможность определения или предсказания всех n или части $n_r \leq n$ значений битов r_{kj} $(k = \overline{1,n})$ всех известных предшествующих r_{i-1} и последующих r_{i+1} элементов последовательности, с вероятностями p_{kj} не превосходящими $p_{kj} \leq p_k$ гарантированных заданных p_k, на основе любых из

известных фрагментов последовательности $\{r_0, r_1,\ldots r_i\}$, формируемых генератором.

Последнее, третье требование, касающееся периода, выполняется автоматически, исходя из свойств дихотомических последовательностей, используемых в качестве исходных, для формирования последовательностей случайных чисел с заданным законом распределения.

Получение надежных в статистическом и функциональном отношении случайных последовательностей, может быть осуществлено путем биективных или сюръективных преобразований дихотомических последовательностей, предусматривающих распространение влияния старших битов на младшие, младших битов на старшие, катенации (связывания) и усечения битов, а также за счет эффективных приемов перемешивания преобразуемых таким образом битов. На основе этих преобразований могут быть достигнуты не только высокие статистические показатели формируемых последовательностей, но и может быть обеспечена функциональная неразрешимость по существу, за счет надежного сокрытия дихотомических свойств, присущих исходным для них *D*-последовательностям.

Практический результат оптимален, если задачи формирования *D*-последовательностей и их преобразования криптографически сильны, взаимно обусловлены и супераддитивны, необратимы по существу, почти всюду дополняют друг друга и гармонично сочетаются между собой.

Учитывая все выше сказанное, перейдем к рассмотрению конкретных вариантов реализации рандомизационных, так называемых ***RA-генераторов***, а именно бесповторных генераторов ключевого потока и равноповторных генераторов гаммы.

В зависимости от приложений, в качестве генераторов ключевого потока обычно используются криптографически сильные, функционально неразрешимые по существу со стороны старших значащих бит дихотомические генераторы [3]. Например, к числу таких генераторов относятся *N*-канальные, *m*-разрядные 3-х параметрические $\{P,D,G\}$ дихотомические генераторы, задаваемые рандомизационным оператором $R_\Delta(P_{i-1},D_{i-1},G_{i-1})$: $B_{i-1} \to \{B_i,P_i,D_i,G_i\}$, вида:

$$B_{ki} = B_{k(i-1)} \oplus P_{k(i-1)}, \quad P_{ki} = (4\cdot B_{k(i-1)}) \oplus \bar{D}_{k(i-1)} \bmod 2^m \quad (k=\overline{1,N}), \tag{3}$$
$$D_{ki} = G \oplus G_{k(i-1)}, \quad G_{ki} = (2\cdot(B_{k(i-1)} \wedge P_{k(i-1)})) \vee Q \bmod 2^m,$$
$$G = \mathbf{rot}_L(B_{k(i-1)},S_m), \quad Q = Q_{k(i-1)}, \quad Q_{ki} = (B_{k(i-1)} \wedge P_{k(i-1)})/\, 2^{m-1},$$

с прямым $r_{ki} = B_{k(i-1)}$ или косвенным выходом $r_{ki} = B_{k(i-1)} \oplus D_{k(i-1)}$, при $G|_{k=1} = G_0$ и $Q|_{k=1} = G_0$ *mod 2*. Здесь $\mathbf{rot}_L$, это операция циклического сдвига $\mathbf{rot}_L(B_{k(i-1)},S_m)$ двоичной *m*-битовой переменной B_k влево на S_m бит, где S_m - ближайшее простое к $m/3$, не кратное m.

В силу свойств присущих таким генераторам, в качестве закрытых ключей могут использоваться старшие, а в качестве открытых ключей или идентификаторов, младшие биты дихотомической последовательности. При числе $k_S \geq \rfloor \log_2 S_K \lfloor +1$ используемых таким образом младших значащих бит, где S_K-максимально возможный объем используемых элементов ключевого потока, множество доступных идентификаторов будет иметь бесповторный и некомлементарный характер. В других случаях для получения надежных в статистическом и функциональном отношении последовательностей ключевого потока, необходимо осуществить выравнивание частот и сокрытие частотных свойств битов исходных для них *D*-последовательностей. Эти действия осуществляются на основе рандомизационных операторов формирования ключевого потока Рис.1, в зависимости от множества так называемых *H-модификаторов*. Указанные операторы должны носить биективный или инъективный характер, если необходимо наследование бесповторных свойств преобразуемой ими исходной последовательности. Для этого значения H-модификаторов обычно фиксируются и не меняются по ходу итерации генератора

Для осуществления эффективных, статистически и функционально надежных преобразований дихотомических последовательностей, могут использоваться простые одно или сложные *r*-кратные модификации или тоже, что одно или *r*-раундовые рандомизационные операторы [1].

Как следует из практики [4], данные операторы должны удовлетворять следующим структурным требованиям, если ставятся задачи построения криптографически сильных генераторов:

1. Порядок катенации каналов (элементов блока) генератора устанавливаемый оператором, должен обеспечивать равномерное и наиболее быстрое выравнивание частот изменения битов используемых дихотомических последовательностей.

2. Алгоритм катенации должен обеспечивать эффективное перемешивание битов внутри элементов выходного блока генератора и существенно выраженное нелинейное преобразование битов каналов от раунда к раунду, в соответствии с установленным выше порядком

3. Перемещение элементов выходного блока генератора между раундами должно обеспечивать лавинно (экспоненциально) нарастающую от раунда к раунду скорость распространения влияния старших значащих битов дихотомических последовательностей, на младшие.

Рассмотрим наиболее характерные примеры структурной реализации таких операторов.

В начале рассмотрим основные типы порядков, используемые для катенации каналов рандомизационных генераторов.

С формальной точки зрения, платформа *m*-разрядного *N*-канального генератора общей длиной $n = m \cdot N$ бит, может быть представлена двоичной векторной величиной $X = \{x_k: k = \overline{1, N}\}$, составленной из *N*, *m*-разрядных двоичных x_k векторных компонент. Тогда по определению, порядок катенации каналов генератора, может быть выражен бинарным порядком, задаваемым парами $(i = I_k, j = J_k)$, определенными на частично упорядоченных *ординальных* множествах *{I,J}*. В условиях дихотомии, среди бинарных порядков представляют наибольший интерес *ламинарный (N,N–1)(N–1,N–2)… (2,1)*, *контр-ламинарный (1,2)(2,3)… (N–1,N)*, *торнадный (N,2)(2,N–1)… (⌈(N+1)/2⌉,1)* и *ротационный (N,1) (N–1,2)… (⌈(N+3)/2⌉,⌊N/2⌋)* порядок катенации векторных компонент. Бинарный порядок можно представить ассоциативным вектором $A = \{a_k: k = \overline{1, N}\}$, с элементами $a_k \in [1,N]$, указывающими на номера соответствующих двоичных *X* компонент $(a_1, a_2)(a_2, a_3)\ldots(a_{N-1}, a_N)$.

На основе ротационного и торнадного порядка достаточно просто осуществить экспоненциально нарастающую от раунда к раунду скорость распространения влияния старших значащих битов дихотомических последовательностей, на младшие. В первом случае, перед каждым очередным раундом $r \le k_r$, кроме первого, следует осуществить циклический сдвиг вправо на $2^{r-2} \bmod N$ двоичных векторных компонент блока генератора. Во втором случае осуществляется циклический сдвиг вправо на $2^{r-2} \bmod (N-1)$ всех, кроме одной первой двоичной векторной компоненты блока генератора.

В различных случаях порядок катенации может быть уточнен, если это оправдано с точки зрения функциональной надежности и топологии аппаратной реализации генератора

И последнее, существует большое множество возможных вариантов построения алгоритмов катенации битов блоков генераторов. Составленные по ним операторы должны обеспечивать не только эффективное перемешивание битов и нелинейную катенацию каналов генератора, наращиваемую от раунда к раунду, но также одно- и много разрядную двоичную параллельную обработку.

В условиях функциональной неразрешимости по существу со стороны старших значащих бит *D*-последовательностей, используемых в качестве исходных для получения достаточно сильных в криптографическом отношении последовательностей случайных чисел, следующие три группы опера-

торов позволяют наиболее просто и эффективно решить перечисленные выше задачи:

$$x_j = (z_j \oplus H_{rk}) \oplus ((g_j \lessdot\gtrdot 1) \vee p_i) \bmod 2^m, \quad g_j = z_j \wedge x_i, \quad p_i = g_i \lessdot\gtrdot (m-1) \bmod 2^m, \tag{4.I}$$

$$x_j = (z_j \oplus x_i) \oplus ((g_j \lessdot\gtrdot 1) \vee p_i) \oplus H_{rk} \bmod 2^m, \quad g_j = z_j \wedge x_i, \quad p_i = g_i \lessdot\gtrdot (m-1) \bmod 2^m, \tag{4.II}$$

$$x_j = (z_j \oplus x_i) \oplus ((g_j \lessdot\gtrdot 1) \vee p_i) \oplus \{H^{\bullet}_{rk}: h_i = 1, H^{\circ}_{rk}: h_i = 0\} \bmod 2^m, \tag{4.III}$$

$$h_i = f_h(x_i) \in \{0,1\}, \quad g_j = z_j \wedge x_i, \quad p_i = (g_i \oplus q_i) \lessdot\gtrdot (m-1) \bmod 2^m, \quad q_i = f_q(x_i) \quad (k = \overline{2,N}).$$

Здесь $(i = a_{k-1}, j = a_k)$ - упорядоченная пара катенируемых компонент, $z_j = \mathbf{rot}_L(x_j, S_m)$, при смещении влево на указанное выше простое число S_m бит, $\lessdot\gtrdot$ - операция сдвига влево или вправо, в зависимости от направления катенации битов внутри компонент, $\{h_i, q_i\}$ - предикативные переменные распространения влияния и конкатенации компонент, $\{H_{rk}, H^{\bullet}_{rk}, H^{\circ}_{rk}\}$ - двоичные m-разрядные модификаторы преобразования компонент выходного блока генератора в раундах $r = \overline{1,kr}$. Случаи обработки первой по списку в ассоциативном ряде A, компоненты $j = a_1$, именуемой вершиной, оговариваются особо.

Принимая за основу представленную выше группу операторов (4.I-III), с учетом требований соблюдения биективности преобразований, необходимых для сохранения бесповторных свойств, присущих D-последовательностям, рандомизационным операторам формирования ключевого потока, с вершиной ассоциативного списка в самом старшем канале N, можно придать следующий вид:

$$x_N = (x_N \oplus H_{r1}) \oplus (g_N \gtrdot 1), \quad g_N = x_N \wedge (x_N \gtrdot 1), \tag{5.I}$$

$$x_j = (z_j \oplus H_{rk}) \oplus ((g_j \gtrdot 1) \vee p_i), \quad g_j = z_j \wedge x_i, \quad p_i = g_i \lessdot (m-1) \bmod 2^m,$$

$$x_N = (z_N \oplus x_N) \oplus (g_N \gtrdot 1) \oplus H_{r1}, \quad z_N = x_N \gtrdot 1, \quad g_N = z_N \wedge x_N, \tag{5.II}$$

$$x_j = (z_j \oplus x_i) \oplus ((g_j \gtrdot 1) \vee p_i) \oplus H_{rk}, \quad g_j = z_j \wedge x_i, \quad p_i = g_i \lessdot (m-1) \bmod 2^m,$$

$$x_N = (z_N \oplus x_N) \oplus (g_N \gtrdot 1) \oplus \{H^{\bullet}_{r1}: h_N \neq 0, H^{\circ}_{r1}: h_N = 0\}, \tag{5.III}$$

$$z_N = x_N \gtrdot 1, \quad g_N = z_N \wedge x_N, \quad h_N = x_N \wedge SIGN \quad (SIGN = 2^m - 1),$$

$$x_j = (z_j \oplus x_i) \oplus ((g_j \gtrdot 1) \vee p_i) \oplus \{H^{\bullet}_{rk}: h_i \neq 0, H^{\circ}_{rk}: h_i = 0\}, \quad g_j = z_j \wedge x_i,$$

$$p_i = (g_i \oplus q_i) \lessdot (m-1) \bmod 2^m, \quad q_i = x_i \gtrdot S_m, \quad h_i = x_i \wedge SIGN,$$

при этом для всех раундовых модификаторов $\{H^{\bullet}_{r1}, H^{\circ}_{r1}\}$ связанных с каналом N, должны соблюдаться условия синхронизации $H^{\bullet}_{r1} \wedge SIGN = H^{\circ}_{r1} \wedge SIGN$. Для достижения оптимальных условий распространения влияния и перемешивания битов блока генератора, перед каждым очередным раундом r, кроме первого, следует принять $x_N = \mathbf{rot}_L(x_N, S_m)$. Рассмотрим другие характерные особенности представленных алгоритмов.

Алгоритмы нелинейны, за счет входящей в их состав конъюнктивной компоненты $g_j = z_j \wedge x_i$. Последним двум из них присущи существенно выраженные лавинные свойства, за счет составляющей x_i, входящей в состав аддитивной компоненты $(z_j \oplus x_i)$ уравнений 5.II и 5.III, ответственной за распространение влияния битов между каналами генератора. За счет двоичной алгебраической структуры, при аппаратной реализации скорость функционирования таких операторов в одном раунде, может быть соизмерима со скоростью выполнения трех операций *XOR*, вне зависимости от длины платформы построенных на их основе генераторов. Для рандомизационных операторов типа I, эта скорость измеряется двумя такими операциями.

Как показывает анализ, представленные алгоритмы обладают различной полиномиальной сложностью $O(L^{\alpha})$ возможности предсказания частотных свойств младших значащих бит D-последовательностей, используемых в качестве исходных для получения последовательностей ключевого потока. Здесь $L = n^{k_r}$, а показатель $\alpha = \{1,2,1+N\}$, для соответствующих 5.I-III алгоритмов. Вполне очевидно, что при выполнении условия $L^{\alpha} > 2 \cdot S_K$, где S_K - максимально возможный объем используемых элементов ключевого потока, можно говорить о функциональной неразрешимости уравнений (5).

Анализ будет не полным, без оценки статистических свойств указанных генераторов. Можно говорить о статистической надежности генераторов, если формируемые на их основе последовательности *Z* установленного объема *V* бит, составленные из *(V/n)* двоичных *n*-разрядных чисел z_s $(s = \overline{1,n})$, а также последовательности или *s*-слайки $Z_s = \{z_{si}: i = \overline{1,V}\}$, составленные из всех $z_{si} \in \{0,1\}$ битов исходной для них двоичной последовательности *Z* объемом *(V·n)* бит, все вместе и каждый в отдельности, удовлетворяют критериям статистических тестов [5]. Далее рассматриваются генераторы с сильным в функциональном и статистическом отношении - ротационным и торнадным порядком катенации каналов. Ламинарный порядок, в силу присущих ему слабостей, не рассматривается.

Как показывают результаты тестирования, генераторы I-го типа не отличаются статистической надежностью, без специального предварительного раунда, предусматривающего распространение влияния старших битов, на младшие. В последнем случае, статистическая надежность генераторов первого типа, а во всех других случаях генераторов II и III-го типа достигается уже после первого раунда, начиная с 64-х разрядной платформы.

Двухраундовые 4-х канальные 8-ми разрядные генераторы II и III-го типа, с длиной платформы генерации 32 бит, достаточно надежны в статистическом отношении, в силу присущих им лавинных эффектов. В Таблице 2, представленной в Приложении, представлен вариант реализации на псевдо С, генератора III-го типа. Дан детальный анализ функциональной зависимости битов ключевого потока от битов исходной для него *D*-последовательности после завершения первого раунда и на начало катенации каналов во втором раунде преобразований, для ротационного и торнадного порядка катенации каналов, соответственно. Последний из них предпочтительней с точки зрения функциональной и статистической надежности формируемой последовательности, что косвенно подтверждается результатами статистических тестов. Приведены оценки ω, характеризующие минимальный период 2^{ω} слайков результирующей последовательности.

Для всех рассмотренных выше типов генераторов ключевого потока не выявлено слабых ключей, приводящих к заметному вырождению формируемых на их основе последовательностей.

Перейдем к рассмотрению следующего класса генераторов случайных чисел, известных как генераторы гаммы. В отличие от бесповторных генераторов ключевого потока, формируемые на основе генераторов гаммы последовательности случайных чисел должны носить, свойственный генераторам типа RC4 и блочным шифрам функционирующим в режиме обратной связи по выходу, указанный выше равноповторный характер (1). Как было показано выше, такие последовательности можно получить на основе усеченных *Dh*-генераторов. Кроме этого, равноповторные последовательности могут быть получены путем рассеяния и перемешивания битов исходных для них *D*-последовательностей. Эти действия могут быть осуществлены на основе рандомизационных операторов формирования гаммы Рис.1, иначе рандомизаторов, в зависимости от множества *P-модификаторов*. Для придания исходным для них *D*-последовательностям необходимых равноповторных свойств, выход указанных операторов должны носить сюръективный характер. Значения *P*-модификаторов могут фиксироваться, либо могут меняться по ходу итерации генератора по вполне определенному или недетерминированному закону.

По идеологии построения и структуре, рандомизаторы подобны *Dh*-генераторам и также как последние, могут иметь параметрический и многомерный характер, могут быть рассчитаны на параллельную одно и многоразрядную беспроцессорную обработку [3]. В силу сюръективного, параметрического и многомерного характера таких операторов они могут быть функционально неразрешимы по существу, независимо от функциональных и статистических свойств используемых исходных для них *D*-последовательностей.

Рандомизаторы, также как и рассмотренные выше операторы формирования ключевого потока, относятся к классу однонаправленных операторов. Изложение общих принципов построения таких операторов - это отдельная тема, которая будет освещена в последующих публикациях. Здесь, не вдаваясь в детали реализации, в качестве примера рассмотрим n-разрядный 4-х параметрический $\{P,D,Q,Z\}$ рандомизатор $R_G(P_{i-1},D_{i-1},Q_{i-1},Z_{i-1},G_{i-1}): X_i \to \{G_i,P_i,D_i,Q_i,Z_i\}$, с входом $x \in \{X_i\}$ и прямым $g = G_{i-1}$ или косвенным $g = G_{i-1} \oplus Q_{i-1}$ выходом $g \in \{G_i\}$, составленный из операторов:

$$G_i = Z_{i-1} \oplus Q_{i-1}, \quad Q_i = D_{i-1} \oplus P_{i-1}, \quad D_i = G_{i-1} \oplus (G_{i-1} \lessdot d) \bmod 2^n, \qquad (6)$$
$$Z_i = \mathbf{rot}_L(G_{i-1} \oplus X_i,S_n), \quad P_i = ((Z_{i-1} \wedge D_{i-1}) \lessdot 1) \vee H_D \bmod 2^n,$$

с постоянной S_n, равной ближайшему простому к $n/3$, не кратному n, постоянной d, равной ближайшему целому к $\log_2(n/3)$ и $H_D = \{1: d = 1, 0: d > 1\}$. При использовании рандомизаторов с прямым выходом, уравнения (6) аналитически разрешимы относительно своих аргументов, если используемая им входная последовательность $\{X_i\}$ известна или легко предсказуема относительно составляющих ее бит. При использовании косвенного выхода, рандомизационные переменные $\{G,P,D,Q,Z\}$, характеризующие внутреннее состояние рандомизатора, могут быть выражены через известное его выходное состояние, определяемое рандомизационной переменной g, в следующем виде:

$$G_i = \mathbf{g_i} \oplus G_{i-1} \oplus \mathbf{rot}_L(G_{i-2} \oplus \mathbf{x_{i-1}},S_n), \quad Q_i = \mathbf{g_{i+1}} \oplus G_i, \quad D_i = G_{i-1} \oplus (2^d \cdot G_{i-1}) \bmod 2^n,$$
$$Z_i = \mathbf{rot}_L(G_{i-1} \oplus \mathbf{x_i},S_n), \quad P_i = (2 \cdot (\mathbf{rot}_L(G_{i-2} \oplus \mathbf{x_{i-1}},S_n) \wedge (G_{i-2} \oplus (2^d \cdot G_{i-2})))) \vee H_D \bmod 2^n.$$

Из представленных выражений следует аналитическая неразрешимость уравнений (6), т.к. на любой итерации i, закон изменения переменных характеризующих внутреннее состояние рандомизатора не может быть однозначно выражен даже через все известные его внешние состояния. Иначе, при неизвестных и скрытых от внешнего доступа аргументах (6), по всем известным внешним их состояниям невозможно аналитически вычислить одно из последующих и каждое из предшествующих значений их выходных переменных. Учитывая лавинные свойства и существенно выраженный нелинейный характер представленных рандомизаторов, общий эффект от использования в качестве исходных аналитически неразрешимых D-последовательностей, будет носить супераддитивный характер. В этих случаях, могут использоваться дихотомические или *Dh-счетчики* [3], задаваемые наиболее простым в реализации, двухпараметрическим $\{P,D\}$ рандомизационным оператором $R_C(H,P_{i-1},D_{i-1}): X_{i-1} \to \{X_i,P_i,D_i\}$, при нечетном фиксированном значении модификатора H и прямым выходом X, вида:

$$X_i = X_{i-1} \oplus P_{i-1}, \quad P_i = H \oplus D_{i-1}, \quad D_i = (X_{i-1} \wedge P_{i-1}) \lessdot 1 \bmod 2^n. \qquad (7)$$

Статистический анализ рандомизационных генераторов гаммы [5], построенных на основе композиции операторов 7 и 6, показывает достаточно высокую статистическую надежность формируемых на их основе последовательностей. Так, для всех n, начиная с 12-ти, заметной корреляции битов в целом и в части по слайкам, не выявлено ни при каких начальных условиях. Отмечается увеличение периода, более чем в 2 раза, при этом последовательности носят равноповторный характер, что подтверждается результатами статистических тестов (см. таблицу 1).

Таким образом, учитывая аналитическую неразрешимость уравнений функционирования представленных рандомизаторов и проведенный статистический анализ, можно говорить по существу о возможности достижения функциональной неразрешимости всех значащих битов формируемых на их основе последовательностей случайных чисел. Для получения устойчивой статистики при любых начальных условиях генерации, достаточно $\rfloor \log_2(n) \lfloor$ холостых итераций генератора.

Рассмотренные генераторы гаммы строго ориентированы на одноразрядные вычислительные устройства или на устройства с разрядностью регистров не меньшей длины платформы генератора, что явно недостаточно для подавляющего числа приложений. Указанные ограничения могут быть устранены на основе многоканальных рандомизаторов.

Многоканальные генераторы гаммы строятся на основе одноканальных, путем сцепления каналов признаком результата, образуемого на стыке каналов и распространения влияния битов младших каналов на старшие. В качестве примера рассмотрим N-канальный m-разрядный 5-ти параметрический $\{W,P,D,Q,Z\}$ рандомизатор $R_G(W_{i-1},P_{i-1},D_{i-1},Q_{i-1},Z_{i-1},G_{i-1}): X_i \to \{G_i,W_i,P_i,D_i,Q_i\}$, с входом $x \in \{X_{ik}\}$ и прямым $g = G_{i-1}$ или косвенным $g = W_{i-1} \oplus Q_{i-1}$ выходом $g \in \{G_{ik}\}$, составленный из операторов:

$$G_{ki} = Z_{k(i-1)} \oplus Q_{k(i-1)}, \quad Q_{ki} = D_{k(i-1)} \oplus P_{k(i-1)}, \quad D_{ki} = W_{k(i-1)} \oplus (W_{k(i-1)} \lessdot d) \bmod 2^m, \qquad (8)$$
$$W_{ki} = G_{k(i-1)} \oplus w_k, \quad w_{k+1} = G_{k(i-1)} \oplus X_i, \quad Z_{ki} = \mathbf{rot}_L(W_{k(i-1)} \oplus X_i, S_m),$$
$$p = Z_{k(i-1)} \wedge D_{k(i-1)}, \quad P_{ki} = (p \lessdot 1) \vee q_k \bmod 2^m, \quad q_{k+1} = p \gtrdot (m-1),$$

по каждому из каналов $k = \overline{1, N}$, с оговоренными выше постоянными S_m и d, а также признаком результата q_k, таким, что перед каждой очередной i-ой итерацией генератора $q_1 = \{1: d = 1, 0: d > 1\}$. Рандомизационная переменная w, ответственная за распространение влияния битов младших каналов на старшие, первоначально принимается равной $w_1 = W_0$, а после завершения каждой очередной итерации $w_1 = \mathbf{rot}_L(w_{N+1},S_m)$. Из аналитической неразрешимости уравнений (6), немедленно следует аналитическая неразрешимость уравнений (8).

В качестве опорных генераторов для формирования гамм, могут использоваться N-канальные m-разрядные Dh-счетчики, задаваемые двухпараметрическим $\{P,D\}$ рандомизационным оператором $R_C(H,P_{i-1},D_{i-1}): X_{i-1} \to \{X_i,P_i,D_i\}$, вида:

$$X_{ki} = X_{k(i-1)} \oplus P_{k(i-1)}, \quad P_{ki} = H_k \oplus D_{k(i-1)}, \quad p = X_{k(i-1)} \wedge P_{k(i-1)}, \qquad (9)$$
$$D_{ki} = (p \lessdot 1) \vee q_k \bmod 2^n, \quad q_{k+1} = p \gtrdot (m-1),$$

с произвольными постоянными $H = \{H_k\}$ по каждому из каналов $k = \overline{1, N}$ и признаком результата q_k, таким, что перед каждой очередной i-ой итерацией генератора $q_1 \equiv H_1 \oplus 1 \ (mod\ 2)$.

Статистический анализ построенных на основе N-канальных операторов 8-ми разрядных и выше рандомизационных генераторов гаммы, показывает по всем показателям и при всех начальных условиях достаточно высокую статистическую надежность формируемых на их основе последовательностей, начиная с минимальной 16-ти битовой и до ближайшей обозримой 16384-х битовой длины платформы генерации. Для получения устойчивой статистики при любых начальных условиях генерации, достаточно $N \cdot \rfloor log_2(m) \lfloor$ холостых итераций генератора.

Из всего вышеизложенного, с тем же основанием, как это было сделано выше, можно говорить о возможности достижения функциональной неразрешимости по существу всех значащих битов формируемых на основе многоканальных генераторов гаммы равноповторных последовательностей случайных чисел.

Представленные генераторы гаммы позволяют организовать высокоэффективную параллельную и последовательную обработку. В первом случае, расчет критической длины пути показывает, что скорость функционирования всюду параллельных генераторов гаммы может быть соизмерима со скоростью выполнения одной операции *XOR*, вне зависимости от длины платформы генератора. Во втором случае, за счет последовательной много тактовой обработки, с числом тактов равным числу битов в платформе, число элементов необходимое для реализации основной цепи генератора минимально 5-8, что позволяет предельно снизить потребляемую энергию и себестоимость подобных схем реализаций.

Выводы:

1. Схемы реализации ***RA***-генераторов просты в исполнении, обладают высокой статистической надежностью, допускают параллельную одно и многоразрядную, включая беспроцессорную обработку на любых платформах вычислительных устройств и требуют небольшого объема памяти.

2. Алгоритмы реализации ***RA***-генераторов в программном исполнении многократно превосходят наиболее совершенные образцы. Например, по производительности генераторы гаммы более чем в 4 раза превосходят генератор случайных чисел RC4, а одно и двух раундовые генераторы 128-ми разрядного ключевого потока приблизительно в 5-9 и 3-5 раз блочный шифр RC6, при реализации в DOS на языке программирования C. В аппаратном исполнении отличаются малой себестоимостью и предельно высоким быстродействием. Так, при аппаратной реализации скорость функционирования генераторов гаммы, может быть соизмерима со скоростью выполнения одной операции *XOR*, а скорость функционирования генераторов ключевого потока от одной до трех, реже до 4-6 таких операций, вне зависимости от длины платформы указанных генераторов.

3. Схемы реализации прозрачны для анализа, носят высоко динамичный параметрический, скрытый от внешней среды многомерный, существенно выраженный нелинейный и недетерминированный характер, рассчитаны на использование ключей переменной и очень большой длины. Как показывает анализ, такие реализации способны обладать достаточно высокой, необходимой для практических приложений функциональной надежностью и криптографической стойкостью.

4. ***RA***-генераторы могут иметь любой, не меньший наперед заданного период повторения, на основе дихотомических генераторов и систем способны образовывать структурные композиции любой сложности, могут быть функционально неразрешимыми по существу и при этом сохранять присущие составляющим их элементам стохастические свойства.

5. ***RA***-генераторы закладывают основу для развития стохастической и сетевой симметричной криптографии, а также технологий построения распределенных многомерных, параметрических, целостных, структурно сложных криптографических средств и систем нового поколения, ориентированных на сетевые решения любой сложности, сверхскоростную и высоконадежную обработку.

6. ***RA***-генераторы и представленные ими технологии обеспечивают высокий уровень унификации и стандартизации, за счет универсального и однородного характера используемых криптографических модулей и компонент.

7. Представленные технологии сохраняют преемственность и носят не проходящий по времени характер, за счет фундаментального характера теоретической базы и их концептуальной связи с процессами и явлениями присущими реальным динамическим системам. Беспроцессорные высоко продуктивные параллельные и высокорентабельные последовательные способы обработки положенные в основу технологий, позволяют говорить о высокоэффективном и энергетически экономичном характере физики вычислений. Что особенно актуально на современном этапе в области развития нано-, голографической, квантовой и радиочастотной криптографической обработки.

Ключевые слова: Стохастическая система. Симметричная криптография. Генератор случайных чисел. Дихотомический генератор. Рандомизационный способ. Рандомизационный оператор. Рандомизационный генератор. Генератор ключей. Генератор гаммы. Однонаправленная функция.

ЛИТЕРАТУРА

1. И.А. Кулаков, “Способ придания реальному объекту рандомизационных свойств и рандомизационная система”. Заявка на международный патент.
2. И.А. Кулаков, Дихотомические последовательности и их свойства. Рукопись статьи представленная на 3-ю Центрально-европейскую конференцию, TATRACRYPT 2003, Братислава, 28 июня 2003.
3. И.А. Кулаков, Дихотомические генераторы и их свойства. Рукопись статьи представленная на 6-ю Международную конференцию по информационной безопасности и криптологии, ICISC 2003, Сеул, 27 ноября 2003
4. B. Schneier, APPLIED CRYPTOGRAPHY. Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc, 1996.
5. G.Marsaglia, Пакет статистических тестов DIEHARD, 1997, geo@stat.fsu.edu

Приложение, Таблица 2. ФУНКЦИОНАЛЬНЫЙ АНАЛИЗ ОПЕРАТОРОВ КАТЕНАЦИИ БИТОВ БЛОКА ГЕНЕРАТОРОВ КЛЮЧЕВОГО ПОТОКА

байт	бит	ротационный порядок катенации каналов генератора: первый раунд	2-ой раунд перед катенацией	ω	период $\geq 2^{\omega}$		торнадный порядок катенации каналов генератора: первый раунд	2-ой раунд перед катенацией	ω	период $\geq 2^{\omega}$
	32	$02 \oplus 29 \oplus (03 \wedge 30) \oplus 32^{*}_{29}$	0	IV	$\mathbf{29}\ldots32^{*}_{29}, 32^{\circ\circ}_{08}$		$10 \oplus 29 \oplus (11 \wedge 30) \oplus 32^{*}_{21}$	0	IV	$\mathbf{29}\ldots32^{*}_{29}, 32^{\circ\circ}_{08}$
	31	$01 \oplus 28 \oplus (02 \wedge 29) \oplus 32^{*}_{28}$	$02 \oplus 29 \oplus (03 \wedge 30) \oplus 32^{*}_{29}$		$\mathbf{28}\ldots32^{*}_{28,29}, 32^{**}_{07}$		$09 \oplus 28 \oplus (10 \wedge 29) \oplus 32^{*}_{20}$	$10 \oplus 29 \oplus (11 \wedge 30) \oplus 32^{*}_{21}$		$\mathbf{28}\ldots32^{*}_{28,29}, 32^{**}_{07}$
	30	$08 \oplus 27 \oplus (01 \wedge 28) \oplus 32^{*}_{27}$	$01 \oplus 28 \oplus (02 \wedge 29) \oplus 32^{*}_{28}$		$\mathbf{27}\ldots32^{*}_{27,28}, 32^{**}_{06}$		$16 \oplus 27 \oplus (09 \wedge 28) \oplus 32^{*}_{19}$	$09 \oplus 28 \oplus (10 \wedge 29) \oplus 32^{*}_{20}$		$\mathbf{27}\ldots32^{*}_{27,28}, 32^{**}_{06}$
	29	$07 \oplus 26 \oplus (08 \wedge 27) \oplus 32^{*}_{26}$	$08 \oplus 27 \oplus (01 \wedge 28) \oplus 32^{*}_{27}$		$\mathbf{26}\ldots32^{*}_{26,27}, 32^{**}_{05}$		$15 \oplus 26 \oplus (16 \wedge 27) \oplus 32^{*}_{18}$	$16 \oplus 27 \oplus (09 \wedge 28) \oplus 32^{*}_{19}$		$\mathbf{26}\ldots32^{*}_{26,27}, 32^{**}_{05}$
	28	$06 \oplus 25 \oplus (07 \wedge 26) \oplus 32^{*}_{25}$	$07 \oplus 26 \oplus (08 \wedge 27) \oplus 32^{*}_{26}$		$\mathbf{25}\ldots32^{*}_{25,26}, 32^{**}_{04}$		$14 \oplus 25 \oplus (15 \wedge 26) \oplus 32^{*}_{17}$	$15 \oplus 26 \oplus (16 \wedge 27) \oplus 32^{*}_{18}$		$\mathbf{25}\ldots32^{*}_{25,26}, 32^{**}_{04}$
	27	$05 \oplus 32 \oplus (25 \wedge 26) \oplus 32^{*}_{32} \oplus 28$	$06 \oplus 25 \oplus (07 \wedge 26) \oplus 32^{*}_{25}$		$\mathbf{28}\ldots32^{*}_{25,32}, 32^{**}_{03}$		$13 \oplus 32 \oplus (25 \wedge 26) \oplus 32^{*}_{24} \oplus 28$	$14 \oplus 25 \oplus (15 \wedge 26) \oplus 32^{*}_{17}$		$\mathbf{28}\ldots32^{*}_{25,32}, 32^{**}_{03}$
	26	$04 \oplus 31 \oplus (05 \wedge 32) \oplus 32^{*}_{31}$	$05 \oplus 32 \oplus (25 \wedge 26) \oplus 32^{*}_{32} \oplus 28$		$\mathbf{31}\ldots32^{*}_{31,32}, 32^{**}_{02}$		$12 \oplus 31 \oplus (13 \wedge 32) \oplus 32^{*}_{23}$	$13 \oplus 32 \oplus (25 \wedge 26) \oplus 32^{*}_{24} \oplus 28$		$\mathbf{31}\ldots32^{*}_{31,32}, 32^{**}_{02}$
	25	$03 \oplus 30 \oplus (04 \wedge 31) \oplus 32^{*}_{30}$	$04 \oplus 31 \oplus (05 \wedge 32) \oplus 32^{*}_{31}$		$\mathbf{30}\ldots32^{*}_{30,31}, 32^{**}_{01}$		$11 \oplus 30 \oplus (12 \wedge 31) \oplus 32^{*}_{32}$	$12 \oplus 31 \oplus (13 \wedge 32) \oplus 32^{*}_{23}$		$\mathbf{30}\ldots32^{*}_{30,31}, 32^{**}_{01}$
II	24	$32 \oplus 32^{\circ}_{08}$	$29 \oplus (31 \wedge \neg 31) \oplus 32^{*}_{05}$	I	$\mathbf{29}\ldots32^{*}_{05}, 8^{**}_{16}$		$32 \oplus 32^{\circ}_{08}$	$29 \oplus (31 \wedge \neg 31) \oplus 32^{*}_{05}$	II	$\mathbf{29}\ldots32^{*}_{05}, 16^{**}_{16}$
	23	$31 \oplus 32 \oplus 32^{*}_{07}$	$28 \oplus (31 \wedge \neg 30) \oplus 32^{*}_{04}$		$\mathbf{28}\ldots32^{*}_{04}, 8^{**}_{15}$		$31 \oplus 32 \oplus 32^{*}_{07}$	$28 \oplus (31 \wedge \neg 30) \oplus 32^{*}_{04}$		$\mathbf{28}\ldots32^{*}_{04}, 16^{**}_{15}$
	22	$30 \oplus (31 \wedge \neg 32) \oplus 32^{*}_{06}$	$27 \oplus (31 \wedge \neg 29) \oplus 32^{*}_{03}$		$\mathbf{27}\ldots32^{*}_{03}, 8^{**}_{14}$		$30 \oplus (31 \wedge \neg 32) \oplus 32^{*}_{06}$	$27 \oplus (31 \wedge \neg 29) \oplus 32^{*}_{03}$		$\mathbf{27}\ldots32^{*}_{03}, 16^{**}_{14}$
	21	$29 \oplus (31 \wedge \neg 31) \oplus 32^{*}_{05}$	$26 \oplus (31 \wedge \neg 28) \oplus 32^{*}_{02}$		$\mathbf{26}\ldots32^{*}_{02}, 8^{**}_{13}$		$29 \oplus (31 \wedge \neg 31) \oplus 32^{*}_{05}$	$26 \oplus (31 \wedge \neg 28) \oplus 32^{*}_{02}$		$\mathbf{26}\ldots32^{*}_{02}, 16^{**}_{13}$
	20	$28 \oplus (31 \wedge \neg 30) \oplus 32^{*}_{04}$	$25 \oplus (31 \wedge \neg 27) \oplus 32^{*}_{01}$		$\mathbf{25}\ldots32^{*}_{01}, 8^{**}_{12}$		$28 \oplus (31 \wedge \neg 30) \oplus 32^{*}_{04}$	$25 \oplus (31 \wedge \neg 27) \oplus 32^{*}_{01}$		$\mathbf{25}\ldots32^{*}_{01}, 16^{**}_{12}$
	19	$27 \oplus (31 \wedge \neg 29) \oplus 32^{*}_{03}$	$32 \oplus 32^{\circ}_{08}$		$\mathbf{32}\ldots32^{\circ}_{08}, 8^{**}_{11}$		$27 \oplus (31 \wedge \neg 29) \oplus 32^{*}_{03}$	$32 \oplus 32^{\circ}_{08}$		$\mathbf{32}\ldots32^{\circ}_{08}, 16^{**}_{11}$
	18	$26 \oplus (31 \wedge \neg 28) \oplus 32^{*}_{02}$	$31 \oplus 32 \oplus 32^{*}_{07}$		$\mathbf{31},32\ldots32^{*}_{07}, 8^{**}_{10}$		$26 \oplus (31 \wedge \neg 28) \oplus 32^{*}_{02}$	$31 \oplus 32 \oplus 32^{*}_{07}$		$\mathbf{31},32\ldots32^{*}_{07}, 16^{**}_{10}$
	17	$25 \oplus (31 \wedge \neg 27) \oplus 32^{*}_{01}$	$29 \oplus (31 \wedge \neg 31) \oplus 32^{*}_{05}$		$\mathbf{29}\ldots32^{*}_{05}, 8^{**}_{09}$		$25 \oplus (31 \wedge \neg 27) \oplus 32^{*}_{01}$	$29 \oplus (31 \wedge \neg 31) \oplus 32^{*}_{05}$		$\mathbf{29}\ldots32^{*}_{05}, 16^{**}_{09}$
II	16	$21 \oplus 08 \oplus (06 \wedge 25) \oplus 08^{*}_{16} \oplus 04$	$18 \oplus 05 \oplus (19 \wedge 06) \oplus 08^{*}_{13}$	III	$\mathbf{28}\ldots24^{**}_{24}$		$21 \oplus 16 \oplus (14 \wedge 25) \oplus 16^{*}_{16} \oplus 12$	$18 \oplus 13 \oplus (19 \wedge 14) \oplus 16^{*}_{13}$	IV	$\mathbf{25}\ldots32^{**}_{32}$
	15	$20 \oplus 07 \oplus (21 \wedge 08) \oplus 08^{*}_{15}$	$17 \oplus 04 \oplus (18 \wedge 05) \oplus 08^{*}_{12}$		$\mathbf{31}\ldots24^{**}_{23}$		$20 \oplus 15 \oplus (21 \wedge 16) \oplus 16^{*}_{15}$	$17 \oplus 12 \oplus (18 \wedge 13) \oplus 16^{*}_{12}$		$\mathbf{28}\ldots32^{**}_{31}$
	14	$19 \oplus 06 \oplus (20 \wedge 07) \oplus 08^{*}_{14}$	$24 \oplus 03 \oplus (17 \wedge 04) \oplus 08^{*}_{11}$		$\mathbf{30}\ldots24^{**}_{22}$		$19 \oplus 14 \oplus (20 \wedge 15) \oplus 16^{*}_{14}$	$24 \oplus 11 \oplus (17 \wedge 12) \oplus 16^{*}_{11}$		$\mathbf{27}\ldots32^{**}_{30}$
	13	$18 \oplus 05 \oplus (19 \wedge 06) \oplus 08^{*}_{13}$	$23 \oplus 02 \oplus (24 \wedge 03) \oplus 08^{*}_{10}$		$\mathbf{29}\ldots24^{**}_{21}$		$18 \oplus 13 \oplus (19 \wedge 14) \oplus 16^{*}_{13}$	$23 \oplus 10 \oplus (24 \wedge 11) \oplus 16^{*}_{10}$		$\mathbf{26}\ldots32^{**}_{29}$
	12	$17 \oplus 04 \oplus (18 \wedge 05) \oplus 08^{*}_{12}$	$22 \oplus 01 \oplus (23 \wedge 02) \oplus 08^{*}_{09}$		$\mathbf{28}\ldots24^{**}_{20}$		$17 \oplus 12 \oplus (18 \wedge 13) \oplus 16^{*}_{12}$	$22 \oplus 09 \oplus (23 \wedge 10) \oplus 16^{*}_{09}$		$\mathbf{25}\ldots32^{**}_{28}$
	11	$24 \oplus 03 \oplus (17 \wedge 04) \oplus 08^{*}_{11}$	$21 \oplus 08 \oplus (06 \wedge 25) \oplus 08^{*}_{16} \oplus 04$		$\mathbf{27}\ldots24^{**}_{19}$		$24 \oplus 11 \oplus (17 \wedge 12) \oplus 16^{*}_{11}$	$21 \oplus 16 \oplus (14 \wedge 25) \oplus 16^{*}_{16} \oplus 12$		$\mathbf{28}\ldots32^{**}_{27}$
	10	$23 \oplus 02 \oplus (24 \wedge 03) \oplus 08^{*}_{10}$	$20 \oplus 07 \oplus (21 \wedge 08) \oplus 08^{*}_{15}$		$\mathbf{26}\ldots24^{**}_{18}$		$23 \oplus 10 \oplus (24 \wedge 11) \oplus 16^{*}_{10}$	$20 \oplus 15 \oplus (21 \wedge 16) \oplus 16^{*}_{15}$		$\mathbf{31}\ldots32^{**}_{26}$
	9	$22 \oplus 01 \oplus (23 \wedge 02) \oplus 08^{*}_{09}$	$19 \oplus 06 \oplus (20 \wedge 07) \oplus 08^{*}_{14}$		$\mathbf{25}\ldots24^{**}_{17}$		$22 \oplus 09 \oplus (23 \wedge 10) \oplus 16^{*}_{09}$	$19 \oplus 14 \oplus (20 \wedge 15) \oplus 16^{*}_{14}$		$\mathbf{30}\ldots32^{**}_{25}$
I	8	$13 \oplus 24 \oplus (22 \wedge 01) \oplus 24^{*}_{24} \oplus 20$	$10 \oplus 21 \oplus (11 \wedge 22) \oplus 24^{*}_{21}$	IV	$\mathbf{25}\ldots32^{**}_{32}$		$05 \oplus 24 \oplus (17 \wedge 22) \oplus 24^{*}_{32} \oplus 20$	$02 \oplus 21 \oplus (03 \wedge 22) \oplus 24^{*}_{29}$	III	$\mathbf{28}\ldots24^{**}_{32}$
	7	$12 \oplus 23 \oplus (13 \wedge 24) \oplus 24^{*}_{23}$	$09 \oplus 20 \oplus (10 \wedge 21) \oplus 24^{*}_{20}$		$\mathbf{28}\ldots32^{**}_{31}$		$04 \oplus 23 \oplus (05 \wedge 24) \oplus 24^{*}_{31}$	$01 \oplus 20 \oplus (02 \wedge 21) \oplus 24^{*}_{28}$		$\mathbf{31}\ldots24^{**}_{31}$
	6	$11 \oplus 22 \oplus (12 \wedge 23) \oplus 24^{*}_{22}$	$16 \oplus 19 \oplus (09 \wedge 20) \oplus 24^{*}_{19}$		$\mathbf{27}\ldots32^{**}_{30}$		$03 \oplus 22 \oplus (04 \wedge 23) \oplus 24^{*}_{30}$	$08 \oplus 19 \oplus (01 \wedge 20) \oplus 24^{*}_{27}$		$\mathbf{30}\ldots24^{**}_{30}$
	5	$10 \oplus 21 \oplus (11 \wedge 22) \oplus 24^{*}_{21}$	$15 \oplus 18 \oplus (16 \wedge 19) \oplus 24^{*}_{18}$		$\mathbf{26}\ldots32^{**}_{29}$		$02 \oplus 21 \oplus (03 \wedge 22) \oplus 24^{*}_{29}$	$07 \oplus 18 \oplus (08 \wedge 19) \oplus 24^{*}_{26}$		$\mathbf{29}\ldots24^{**}_{29}$
	4	$09 \oplus 20 \oplus (10 \wedge 21) \oplus 24^{*}_{20}$	$14 \oplus 17 \oplus (15 \wedge 18) \oplus 24^{*}_{17}$		$\mathbf{25}\ldots32^{**}_{28}$		$01 \oplus 20 \oplus (02 \wedge 21) \oplus 24^{*}_{28}$	$06 \oplus 17 \oplus (07 \wedge 18) \oplus 24^{*}_{25}$		$\mathbf{28}\ldots24^{**}_{28}$
	3	$16 \oplus 19 \oplus (09 \wedge 20) \oplus 24^{*}_{19}$	$13 \oplus 24 \oplus (22 \wedge 01) \oplus 24^{*}_{24} \oplus 20$		$\mathbf{28}\ldots32^{**}_{27}$		$08 \oplus 19 \oplus (01 \wedge 20) \oplus 24^{*}_{27}$	$05 \oplus 24 \oplus (17 \wedge 22) \oplus 24^{*}_{32} \oplus 20$		$\mathbf{37}\ldots24^{**}_{27}$
	2	$15 \oplus 18 \oplus (16 \wedge 19) \oplus 24^{*}_{18}$	$12 \oplus 23 \oplus (13 \wedge 24) \oplus 24^{*}_{23}$		$\mathbf{31}\ldots32^{**}_{26}$		$07 \oplus 18 \oplus (08 \wedge 19) \oplus 24^{*}_{26}$	$04 \oplus 23 \oplus (05 \wedge 24) \oplus 24^{*}_{31}$		$\mathbf{26}\ldots24^{**}_{26}$
	1	$14 \oplus 17 \oplus (15 \wedge 18) \oplus 24^{*}_{17}$	$11 \oplus 22 \oplus (12 \wedge 23) \oplus 24^{*}_{22}$		$\mathbf{30}\ldots32^{**}_{25}$		$06 \oplus 17 \oplus (07 \wedge 18) \oplus 24^{*}_{25}$	$03 \oplus 22 \oplus (04 \wedge 23) \oplus 24^{*}_{30}$		$\mathbf{25}\ldots24^{**}_{25}$

$\oplus$, $\wedge$, $\neg$ - побитовые операции XOR, AND, NOT, связывающие биты $k = \overline{1,n}$ платформы N-канального генератора, длиной $n = N \cdot m$. Здесь m - разрядность регистров платформы генерации. $\succ$, $\prec$ - сдвиг битов вправо и влево. **SIGN** $= 2^{m-1}$
AssBlock - ассоциативный вектор, устанавливающий порядок катенации каналов.
KeyBlock - платформа или блок генератора. $\mathbf{H}^{\bullet}$, $\mathbf{H}^{o}$ - вектора модификации блока (* в первом, ** во втором раундах). RotL - циклический сдвиг влево на **SHFL** бит.

```
x = z = *AssBlock[1]; z ≻= 1; g = z ∧ x;     // раунд катенации каналов генератора
*AssBlock[1] = ((z ⊕ x) ⊕ ((x ∧ SIGN) ? H•[1] : Ho[1])) ⊕ (g ≻ 1);
for ( i = 2; i ≤ N; x = q, i++) {  // процедура катенации битов блока генератора
   p = g ⊕ (x ≻ SHFL); rb = AssBlock[i]; q = *rb; z = RotL(q,SHFL); g = z ∧ x;
  *rb = ((z ⊕ x) ⊕ ((x ∧ SIGN) ? H•[i] : Ho[i])) ⊕ ((g ≻ 1) ⊕ (p ≺ (m – 1));
} RotateBlock(KeyBlock,ShfR); // перемещение элементов блока между раундами
```