Регулярный рандомизационный способ

Представленные в Таблице 1 и на графиках (Рис.1, Рис.2) варианты, построенные на основе ***регулярного рандомизационного способа*** (см. также ***нерегулярный рандомизационный способ***), охватывают приложения, в том числе и реализации на основе нелинейных регистров с обратной связью – NFSR, с одной стороны, рассчитанные на среды с крайним дефицитом ресурса, порядка 175-250 логических элементов (GE, 4 транзистора), а с другой, на сверхскоростную обработку информационных потоков, с производительностью в десятки и сотни Гбит/сек.

Таблица 1

ОЦЕНКИ $n/\min\{k\}$ КОМПЛЕКСИРОВАНИЯ n-разрядных ***Dh***-счетчиков и ***Dh***-генераторов, с k-разрядными **LFSR**, удовлетворяющие статист. тестам **DIEHARD**					
КОМПЛЕКСИРОВАНИЕ ГЕНЕРАТОРОВ с гарантированным периодом $T_{n/k} = 2^n \cdot \max\{1, 2^k - 1\}$			**ПОТОКОВЫЕ ВАРИАНТЫ**	**БЛОЧНЫЕ ВАРИАНТЫ**	
				ПРОСТЫЕ	**С ПАМЯТЬЮ n-бит**
		Число триггеров:		$2 \cdot n + k + 1$	$3 \cdot n + k + 1$
ОДНО РАЗРЯДНОЕ	***Dh*-счетчики**		**нет решений** $n_{\min} = \infty$	17/12 30/2 **31**	13/12 16/9 26/5 $n_{\min} =$ **27**
	***Dh*-генераторы**		$n/k =$ 9/16 13/12 16/10 24/2 **25**	13/13 30/2 **31**	11/14 13/12 16/9 25/2 **27**
Затраты на XOR + нелинейный регистр		**счетчики**	$(n + 2 + c_k) + 2.5 \cdot n$	$7.5 \cdot n + 1 + c_k$	$8.5 \cdot n + 1 + c_k$
		генераторы	$4.5 \cdot n + c_k$ (**GE**)	$8.5 \cdot n - 1 + c_k$	$9.5 \cdot n - 1 + c_k$
ПОЛНО РАЗРЯДНОЕ	***Dh*-счетчики**		4/23 8/18 13/12	7/18 8/17 13/13 16/10 30/2 **31**	6/19 8/17 13/12 16/9 26/4 **27**
	***Dh*-генераторы**		4/21 8/17 13/12 16/10 24/2 **25**	7/18 8/17 13/13 16/10 30/2 **31**	5/19 8/16 13/12 16/9 26/4 **27**
Затраты на XOR + нелинейный регистр		**счетчики**	$3.5 \cdot n + 2 + g_{n,k}$	$7.5 \cdot n + 1 + g_{n,k}$	$8.5 \cdot n + 1 + g_{n,k}$
		генераторы	$4.5 \cdot n + g_{n,k}$	$8.5 \cdot n - 1 + g_{n,k}$	$9.5 \cdot n - 1 + g_{n,k}$
Мощность ключевого пр-ва 2^w			$w = v \cdot (n - 1) + k$	$v \cdot (n - 1) + n + k$	$v \cdot (n - 1) + 2 \cdot n + k$

Условные обозначения: $1 \le v \le 4$ – коэффициент разнообразия генерируемых R-последовательностей, $c_k = 0$ без комплексирования с **LFSR**, $c_k = 1$ для примитивных одночленов и 3, для трехчленов **LFSR**, $g_{n,k} = \min\{n,k\} + c_k$ – число бит **LFSR** комплексируемых с битами ***Dh***-генератора, увеличенное на c_k.
Примечание: Затраты на элементы типа **XOR** даны для конфигураций с памятью хранения ключей, рассчитанной только на считывание (**RO**), при этом показатель 2^w характеризует глубину тотального перебора, необходимую для вскрытия внутреннего состояния представленных R-генераторов.

Пример 1. Для реализации на основе CMOS технологий блока аутентификации (защиты от подделки) дешевых (1-5 цента) пассивных меток радиочастотной идентификации (**RFID**) типа **RO** (только на считывание), с длиной платформы $n = 16$ бит, требуется $2 \cdot n + 1 = 33$ триггера и около $4.5 \cdot n = 72$ (GE) логических элементов (288 транзисторов), против $0.5 \cdot 10^3$ - 10^4 **GE** у известных промышленных прототипов (**BRIDGE**, **RFIDSec**). При этом глубина тотального перебора, необходимая для вскрытия внутреннего состояния метки, составляет порядка 2^{60}.

Пример 2. Для реализации на основе CMOS технологий потокового генератора с однопразрядным выходом, периодом 2^{32}, глубиной тотального перебора порядка 2^{93} и с длиной платформы $n = 32$ бит, без учета затрат на хранение и обновление ключей, требуется $2 \cdot n + 1 = 65$ триггеров и около $4.5 \cdot n = 144$ (GE) логических элементов (576 транзисторов).

Пример 3. Для реализации на основе CMOS технологий высококачественного $n = 32$ разрядного генератора гаммы (псевдослучайных чисел) с периодом 2^{32} и глубиной тотального перебора порядка 2^{157}, без учета затрат на хранение и обновление ключей, требуется $3 \cdot n + 1 = 97$ триггеров и около $9.5 \cdot n - 1 = 303$ (GE) логических элементов (1212 транзисторов).

Для обеспечения необходимого уровня аналитической сложности, могут использоваться, как много раундовые преобразования (однонаправленные функции и операторы), так и усечение много разрядного выхода генератора. Последнее наиболее эффективно при несущественно малой части усекаемых бит. В общем, при длинах блоков гаммы 32 и 64 бит, пропускная способность при использовании 1.2 - 0.13μm CMOS технологий, рассчитанная исходя из быстродействия триггеров, может составлять порядка 15 – 425 и 30 – 850, или (0.5 -13) n Гбит/сек.

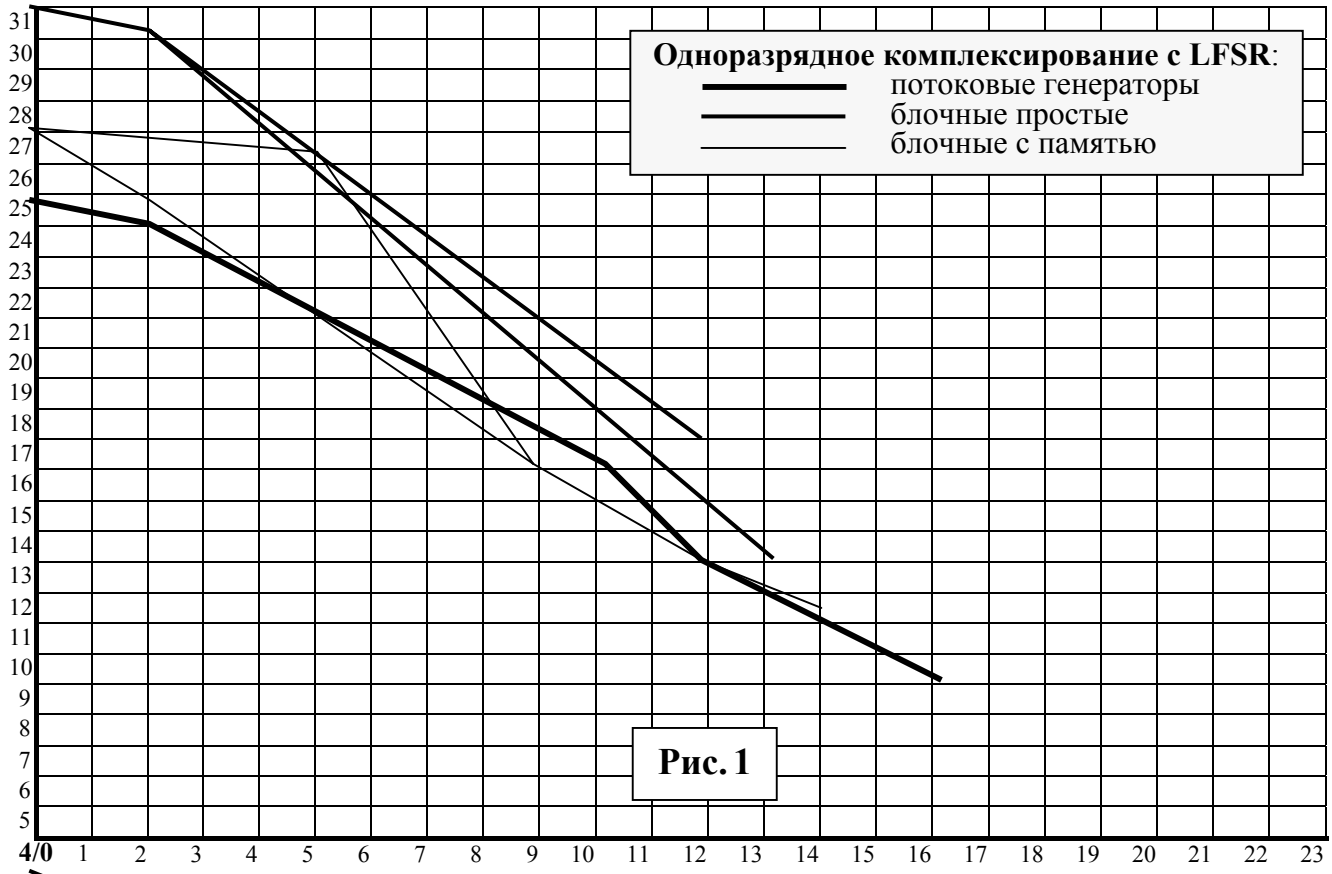


Рис. 1

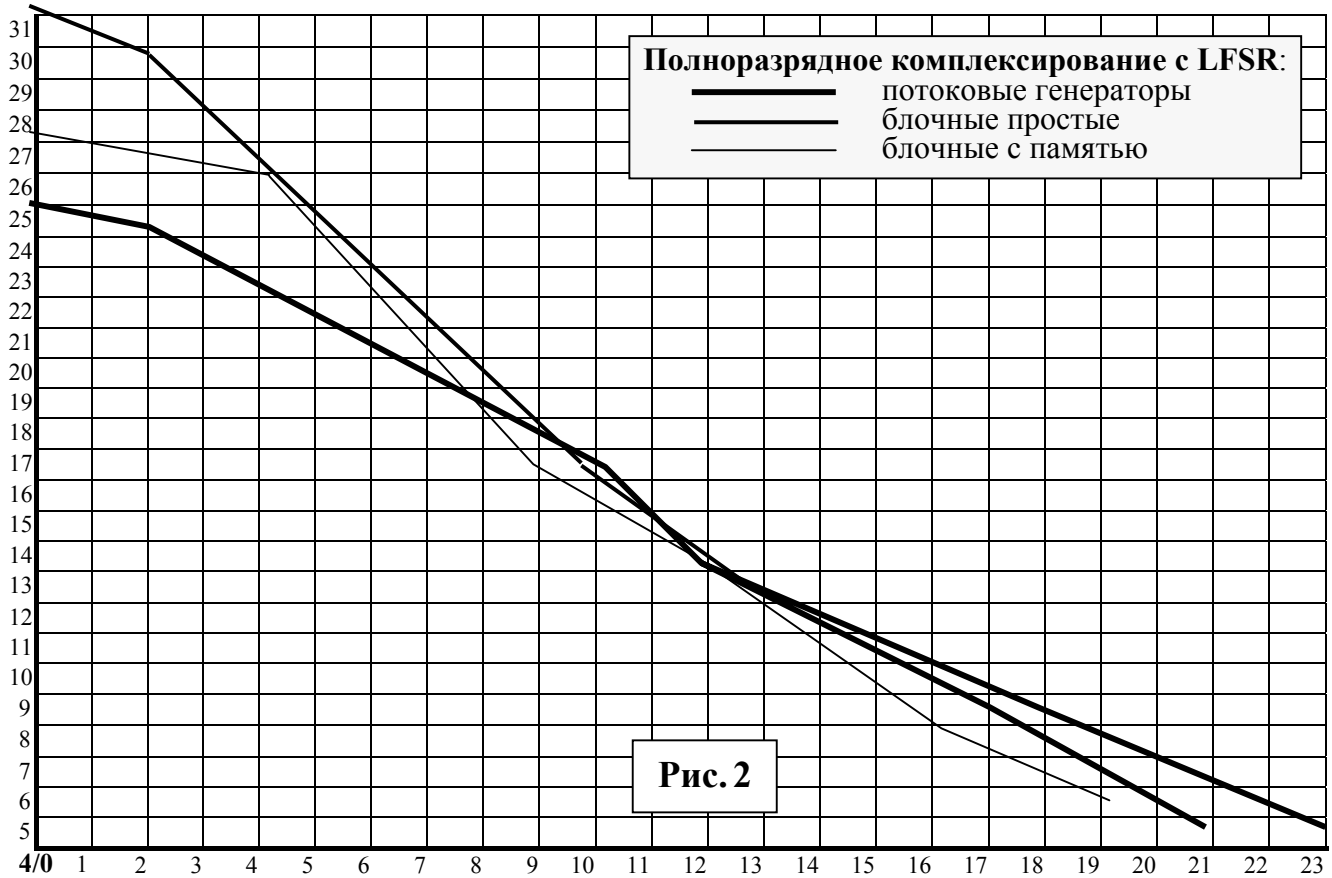


Рис. 2

Примечание. К основным недостаткам регулярного рандомизационного способа относятся однонаправленный (ламинарный) характер изменения старших значащих бит и относительно медленное распространение влияния младших битов на старшие.

Ко всему, представляемая регулярным рандомизационным способом генерация бесповторных, так называемых последовательностей ключевого потока (идентификаторов, ключей, паролей и пр.), разрядностью от 8 - 256, до 512 - 2048 и более бит, производительностью сотни миллионов и десятки миллиардов ключей в секунду, требует особого рассмотрения.

Нерегулярный рандомизационный способ

Представленные в Таблице 2 и на графиках (Рис.3, Рис.4) варианты, построенные на основе ***нерегулярного рандомизационного способа*** (см. также ***регулярный рандомизационый способ***), охватывают приложения, с одной стороны, рассчитанные на среды с крайним дефицитом ресурса, порядка 200-275 логических элементов (GE, 4 транзистора), а с другой, на контроль целостности и сверхскоростную обработку информационных потоков, с производительностью в сотни и тысячи Гбит/сек.

Таблица 2

ОЦЕНКИ $n/\min\{k\}$ КОМПЛЕКСИРОВАНИЯ n-разрядных ***R***-счетчиков и ***R***-генераторов, с k-разрядными **LFSR**, удовлетворяющие статистич. тестам **DIEHARD**

КОМПЛЕКСИРОВАНИЕ генераторов с периодом $\mathbf{T}_{n/k} = \mathbf{T}_n \cdot \max\{1, 2^k - 1\}$		**ПРОТОТИПЫ РЕАЛИЗАЦИЙ**		
		МИНИМАЛИСТСКИЕ	**ПЕРЕХОДНЫЕ**	**УСИЛЕННЫЕ**
С ЛОКАЛЬНОЙ СВЯЗЬЮ ПО ВЫХОДУ	***R*-счетчики**	n/k = 8/24 16/18 17/17 28/2 $n_{\min}$= **29**	5/21 8/21 16/16 17/12 28/2 **29**	4/24 8/21 16/16 24/6 **25**
	***R*-генераторы**	7/24 8/23 16/20 17/17 26/4 **27**	5/22 8/22 16/20 17/15 27/2 **28**	7/21 8/21 16/16 24/3 **25**
С ГЛОБАЛЬНОЙ СВЯЗЬЮ ПО ВЫХОДУ	***R*-счетчики**	10/24 16/18 17/17 28/2 **29**	2/24 4/14 5/9 7/4 8/2 **9**	2/22 3/14 4/10 5/4 6/3 7/2 **8**
	***R*-генераторы**	10/24 16/20 17/17 26/6 **27**	5/24 6/23 7/21 8/17 10/7 **11**	4/24 6/18 7/14 8/9 9/3 10/2 **11**
Затраты (GE)	**счетчики**	$(3.5 \div 4.5)\cdot n + g_{n,k}$	$5.5\cdot n + g_{n,k}$	$6.5\cdot n + g_{n,k}$
	генераторы	$(4.5 \div 5.5)\cdot n + g_{n,k}$	$6.5\cdot n + g_{n,k}$	$7.5\cdot n + g_{n,k}$
Число триггеров		$2\cdot n + k$	$3\cdot n + k$	$4\cdot n + k$
Мощность ключевого пр-ва 2^w		$w = v\cdot n + k$	$w = v\cdot n + n + k$	$w = v\cdot n + 2\cdot n + k$

Обозначения: $\mathbf{T}_n = 2^u$ – гарантированный, с вероятностью $1 - 2^{-u}$, период *R*-генератора, при $k = 0$ и $u = n\cdot\max\{1, 24/n_{\min}\}$; $1 \le v \le 4$ – коэффициент разнообразия генерируемых *R*-последовательностей; $g_{n,k} = \min\{n,k\} + c_k$ – число бит **LFSR** комплексируемых с битами опорного *R*-генератора, где $c_k = 0$ без комплексирования с **LFSR**, $c_k = 1$ для примитивных одночленов и 3, для трехчленов **LFSR**.
Примечание: Затраты на элементы типа **XOR** даны для конфигураций с памятью хранения ключей, рассчитанной только на считывание (**RO**), при этом показатель 2^w характеризует глубину тотального перебора, необходимую для вскрытия внутреннего состояния представленных *R*-генераторов.

Пример 1. Для реализации на основе CMOS технологий блока аутентификации (защиты от подделки) дешевых пассивных радиочастотных смарт-карт с длиной платформы $n = 32$ бит, требуется, без учета затрат на хранение и обновление ключей, $2\cdot n = 64$ триггера и около $4.5\cdot n = 144$ (GE) логических элементов (576 транзисторов), против 10^3 - $3\cdot10^4$ **GE** у известных промышленных прототипов (**NESSIE**). При этом глубина тотального перебора, необходимая для вскрытия внутреннего состояния смарт-карты, составляет порядка 2^{128}.

Пример 2. Для реализации на основе CMOS технологий потокового генератора с одноразрядным выходом, периодом порядка 2^{64}, глубиной тотального перебора порядка 2^{256} и с длиной платформы $n = 64$ бит, требуется, без учета затрат на хранение и обновление ключей, $2\cdot n = 128$ триггеров и около $4.5\cdot n = 288$ (GE) логических элементов (1152 транзистора).

Пример 3. Для реализации на основе CMOS технологий высококачественного $n = 128$ разрядного генератора гаммы (псевдослучайных чисел) с периодом порядка 2^{280} и глубиной тотального перебора порядка 2^{512}, требуется, без учета затрат на хранение и обновление ключей, $3\cdot n = 384$ триггера и около $6.5\cdot n = 832$ (GE) логических элементов (3328 транзисторов).

Для обеспечения необходимого уровня сложности, могут использоваться, как много раундовые преобразования, так и усечение выхода генератора. Последнее наиболее эффективно при несущественно малой части усекаемых бит.

В общем, при длинах блоков гаммы 64 и 128 бит, пропускная способность при использовании 1.2 - 0.13μm CMOS технологий, рассчитанная исходя из быстродействия триггеров, составляет порядка 30 - 850 и 60 - 1700, или (0.5 -13) n Гбит/сек.

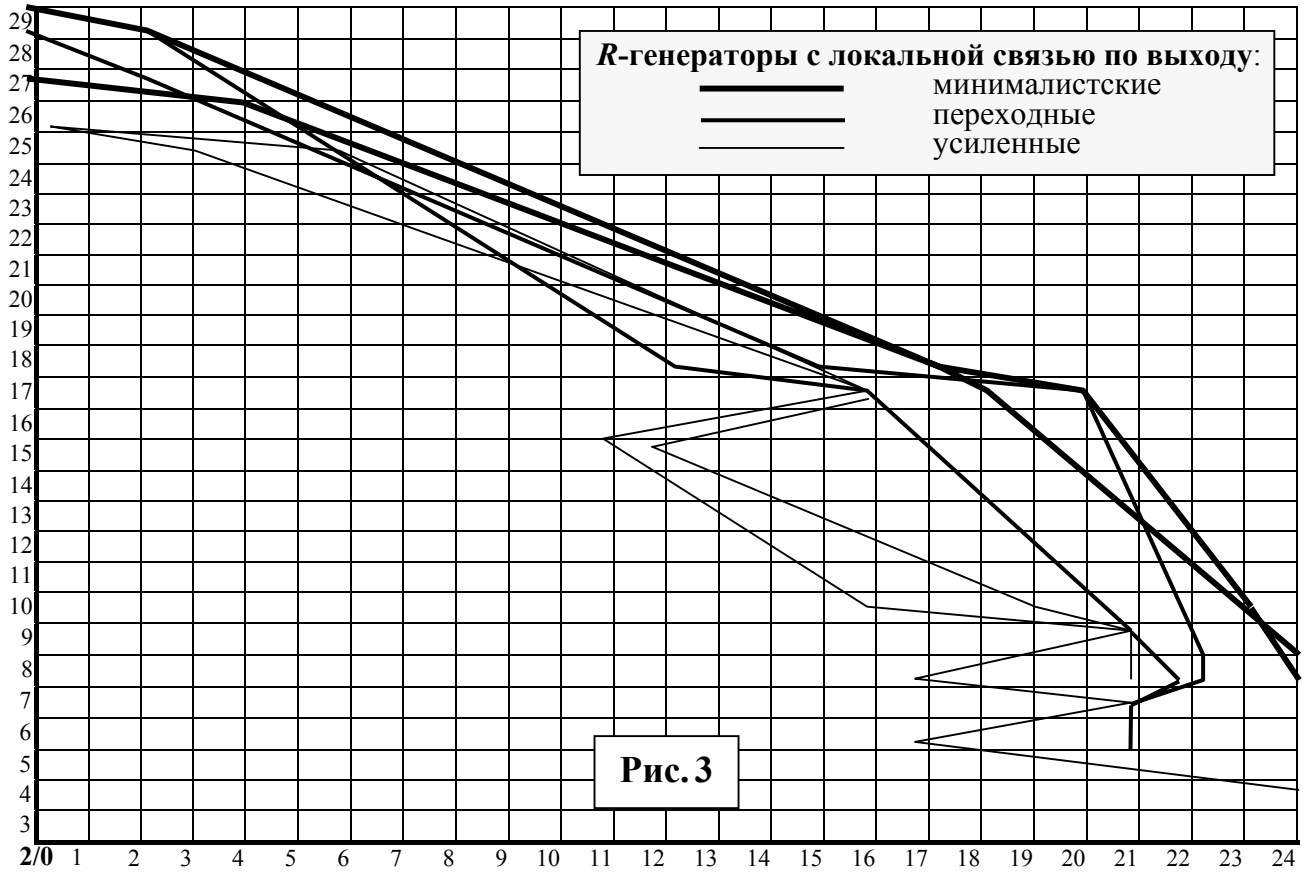


Рис. 3

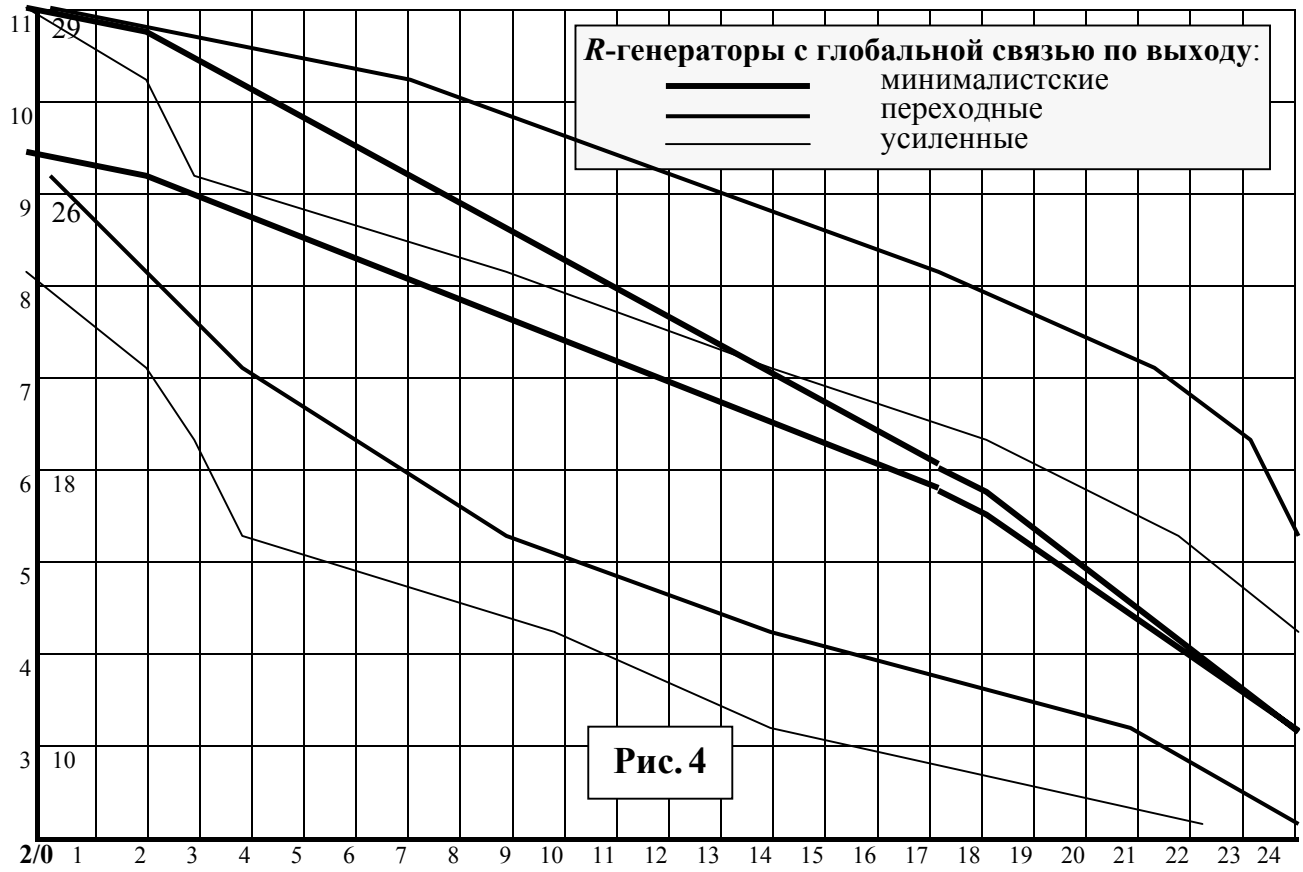


Рис. 4

Примечание. К основным недостаткам нерегулярного рандомизационного способа, не усиленного линейным рекуррентным способом, представляемого полем Галуа GF(2), относятся возможность их вырождения, в нашем случае до периода $\mathbf{T}_n$, пропорциональным $\boldsymbol{n}$, хотя и вероятность такого вырождения чрезвычайно, а при комплексировании с **LFSR** исчезающе, мала.

Ко всему, представляемые нерегулярным рандомизационным способом варианты реализаций могут выступать в качестве высокоэффективных прототипов однонаправленных функций, в частности, хеш-функций и MAC, используемых для контроля целостности информации.

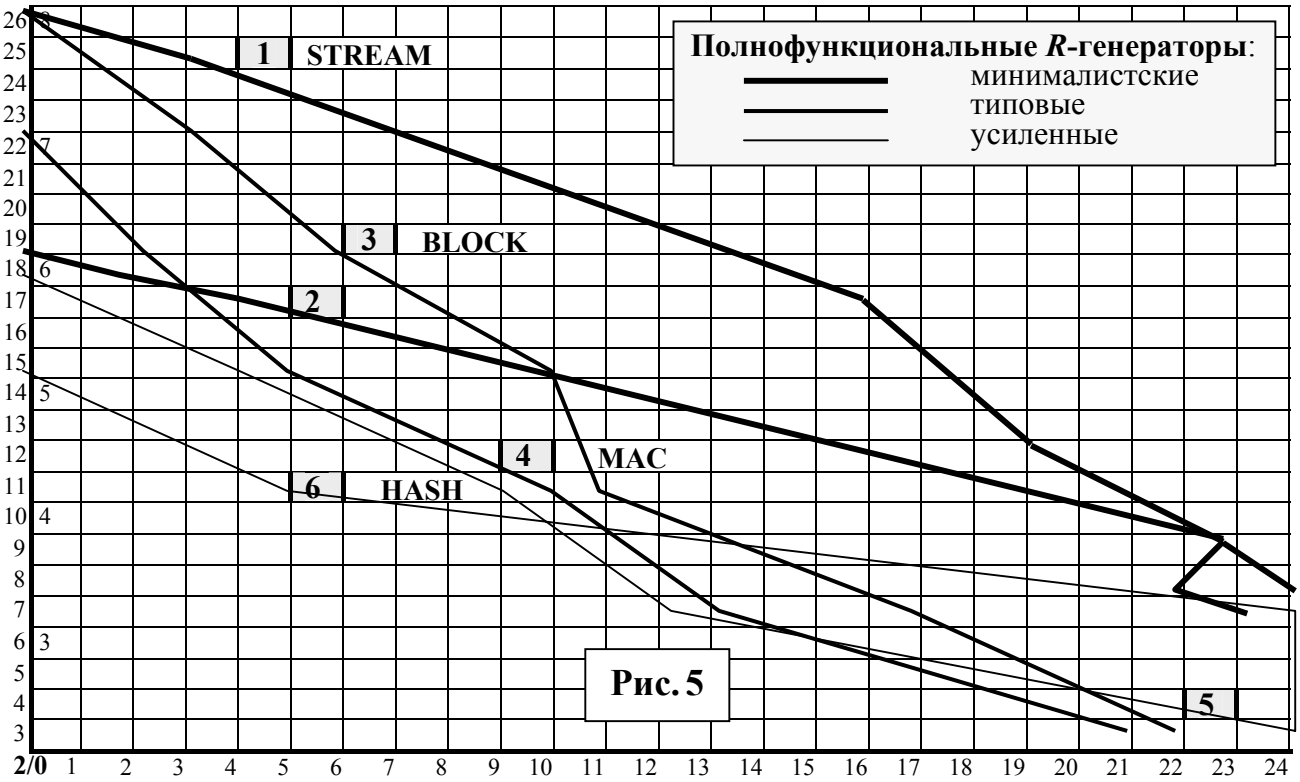
Рандомизационный метод предполагает развитие, без заметного увеличения аппаратных затрат. В качестве примера, в Таблице 3 и на Рис.5 приведены, построенные на его основе более качественные, по отношению к упомянутым вариантам, полнофункциональные *R*-генераторы.

Таблица 3

ОЦЕНКИ $n/\min\{k\}$ **КОМПЛЕКСИРОВАНИЯ** по **DIEHARD** полнофункциональных n-разрядных ***R***-генераторов с нелинейной связью по выходу, с k-разрядными **LFSR**

КОМПЛЕКСИРОВАНИЕ генераторов с периодом $T_{n/k} = T_n \cdot \max\{1,2^k-1\}$	**ПРОТОТИПЫ РЕАЛИЗАЦИЙ**		
	МИНИМАЛИСТСКИЕ	**ТИПОВЫЕ**	**УСИЛЕННЫЕ**
ОДНОЭЛЕМЕНТНАЯ нелинейная обратная связь	7/24 8/23 12/19 16/16 25/3 **26**	2/22 3/17 4/11 5/10 6/6 7/3 **8**	2/24 3/12 4/9 5/4 **6**
Затраты (GE)	$(4.5\div5.5)\cdot n+6+g_{n,k}$	$6.5\cdot n+6+g_{n,k}$	$7.5\cdot n+6+g_{n,k}$
Число триггеров	**1** $2\cdot n+1+k$	**3** $3\cdot n+1+k$	**5** $4\cdot n+1+k$
ПОЛНОЭЛЕМЕНТНАЯ нелинейная обратная связь	6/23 7/22 8/23 16/4 17/2 **18**	2/21 3/13 4/10 5/5 6/2 **7**	2/24 3/24 4/5 **5**
Затраты (GE)	$9.5\cdot n+g_{n,k}$	$10.5\cdot n+g_{n,k}$	$11.5\cdot n+g_{n,k}$
Число триггеров	**2** $3\cdot n+k$	**4** $4\cdot n+k$	**6** $5\cdot n+k$
Мощность пр-ва ключей 2^w	$w=v\cdot n+k$	$w=v\cdot n+n+k$	$w=v\cdot n+2\cdot n+k$

Примечание: Затраты на элементы типа **XOR** даны без учета затрат на хранение и обновление ключей.



Выводы. Как следует из указанных результатов, представляемые ***рандомизационным способом*** односторонние функции и генераторы, по своим статистическим показателям, периоду, силе лавинных эффектов, функциональной сложности и присущей им существенной нелинейности, не уступают уровню имеющихся разработок. Причем, представленные в Таблице 3 варианты **1**, **2**, **5**, **6** не только не уступают лучшим аналогам, таким, как **Grain**, **Trivium**, (**AES**, **ГОСТ** 28147-89), **SHA** и **ГОСТ** Р 34.11-94 и др., соответственно, но и не в ущерб функциональной сложности и при минимальном уровне аппаратных затрат, превосходят их по упомянутым показателям.

Рандомизационные генераторы строятся на единой, рассчитанной на бессрочную перспективу, технологической базе, охватывают все известные платформы и приложения, требуют в десятки раз меньших аппаратных и энергетических затрат, обладают в сотни раз более высокой производительностью, что дает возможность осуществить качественный скачек в области стохастических технологий и систем передачи и обработки информации (**random-art.ru**).