Нерегулярный рандомизационный способ

Представленные в Таблице 1 и на графиках (Рис.1, Рис.2) 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 1

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 - $3\cdot 10^4$ **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.

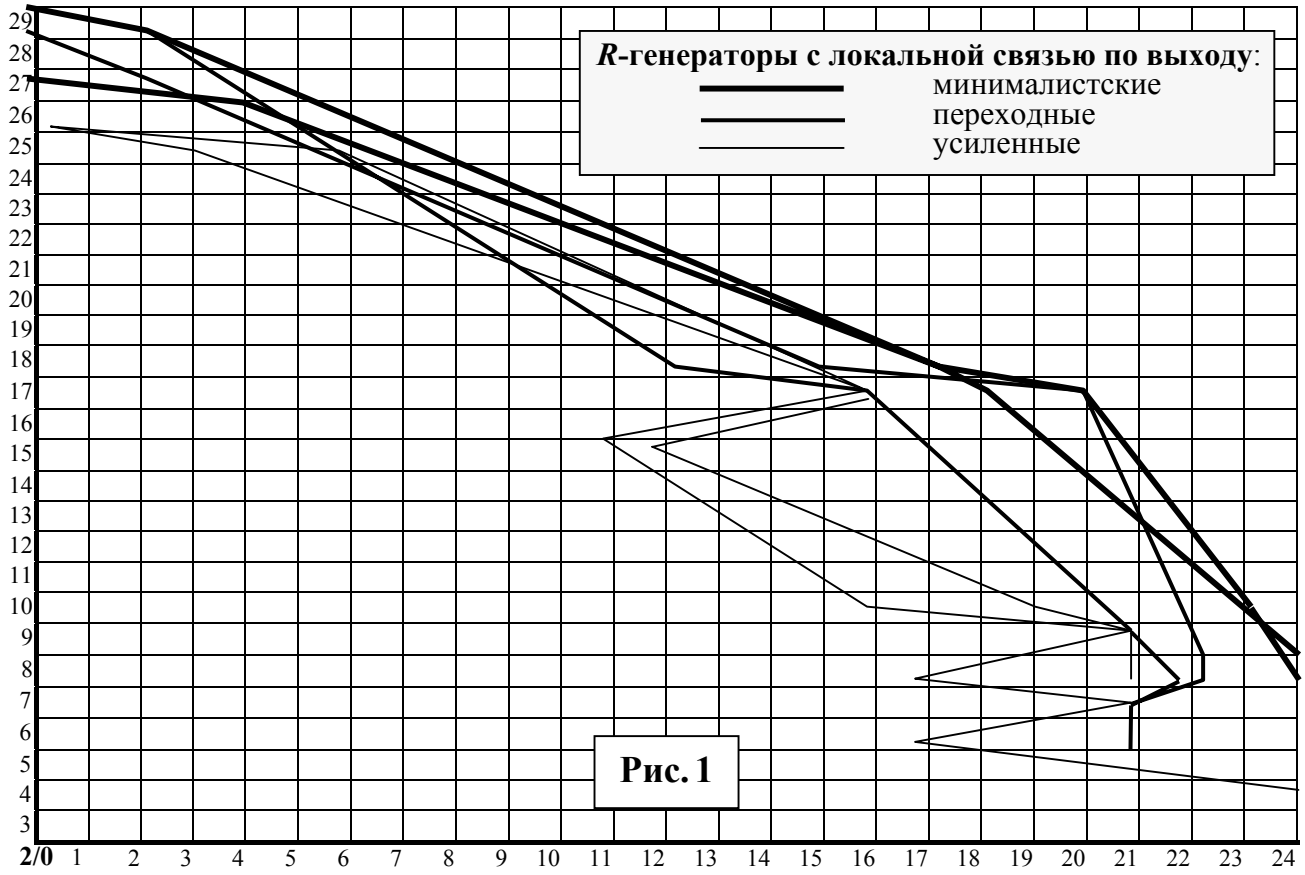

Рис. 1

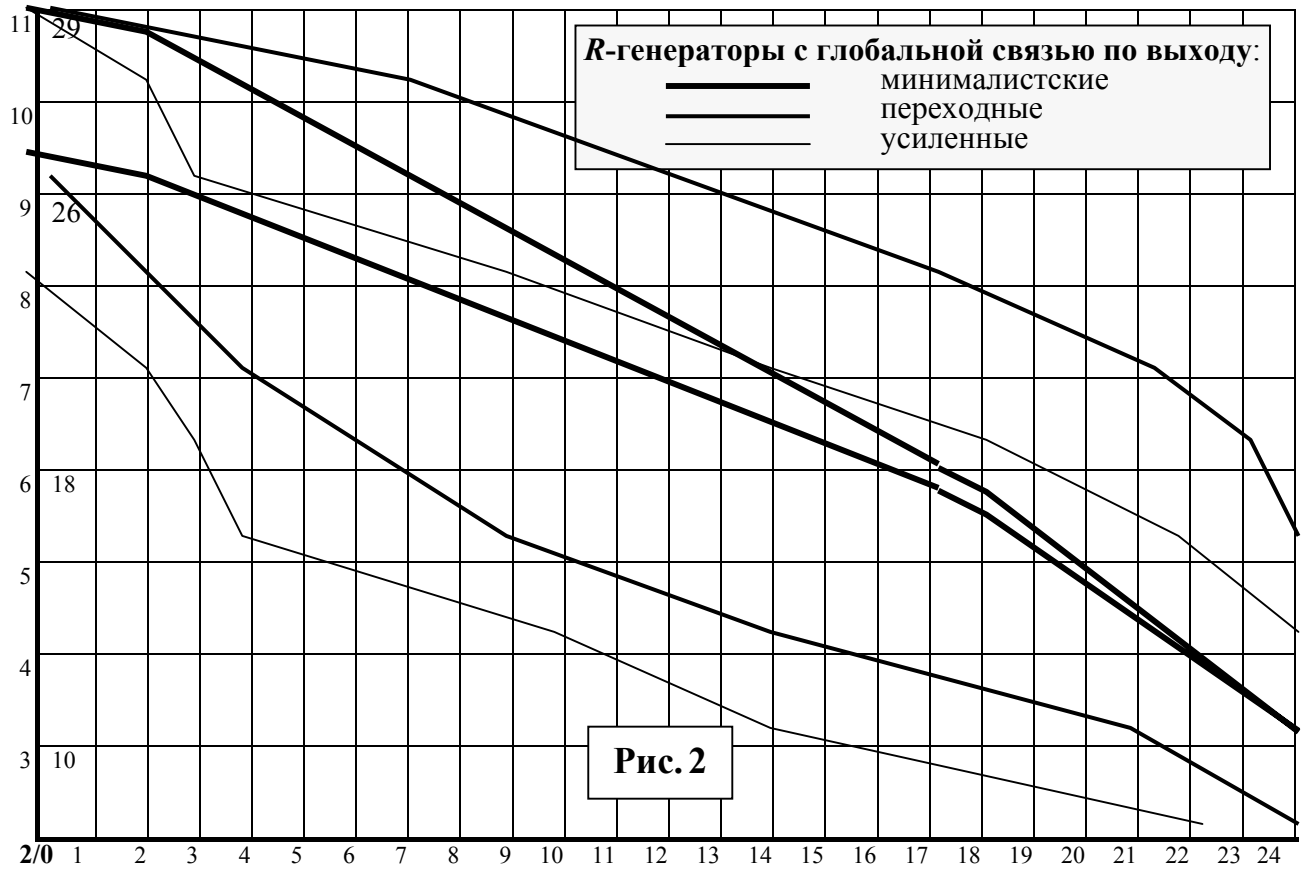

Рис. 2

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.