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.

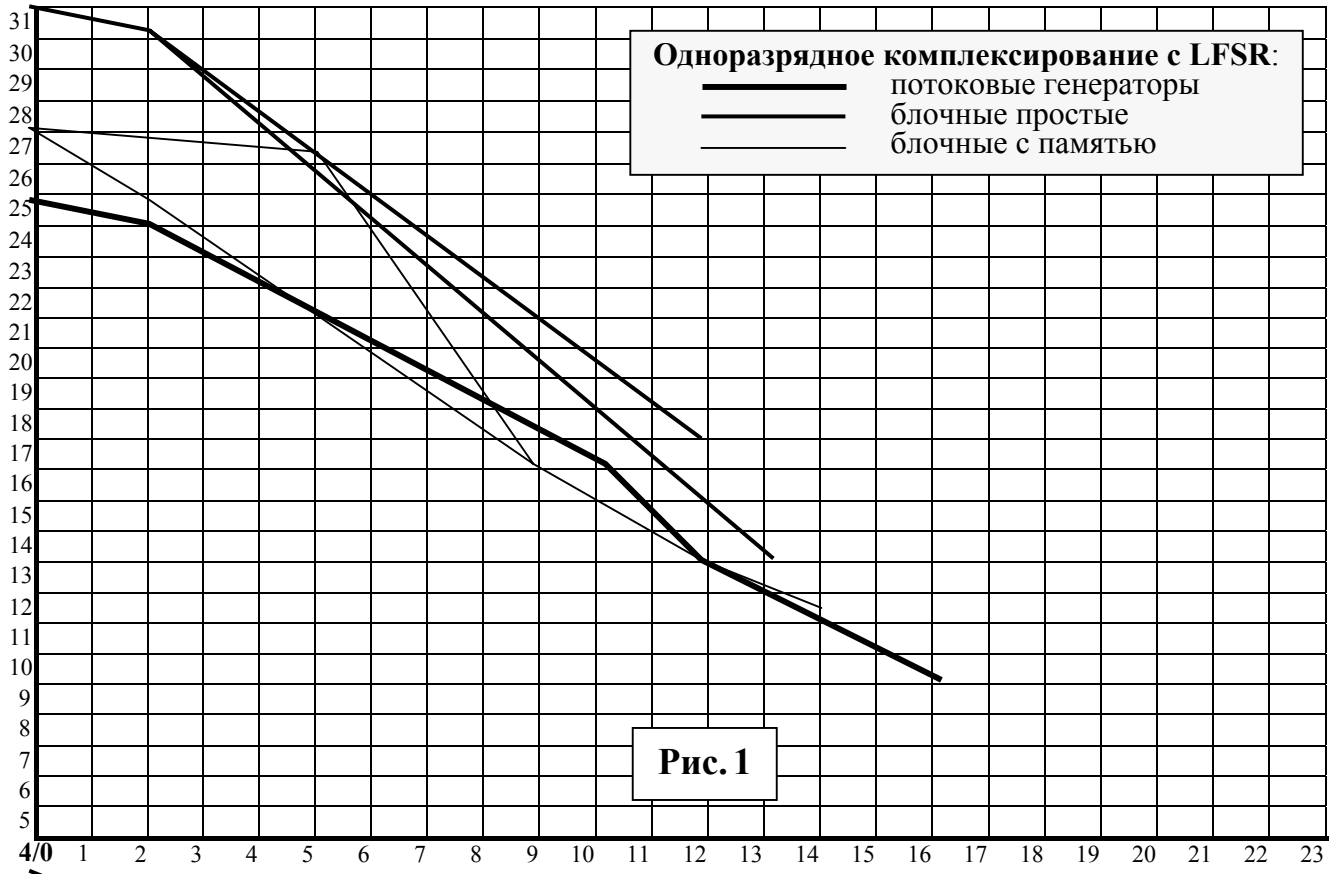

Рис. 1

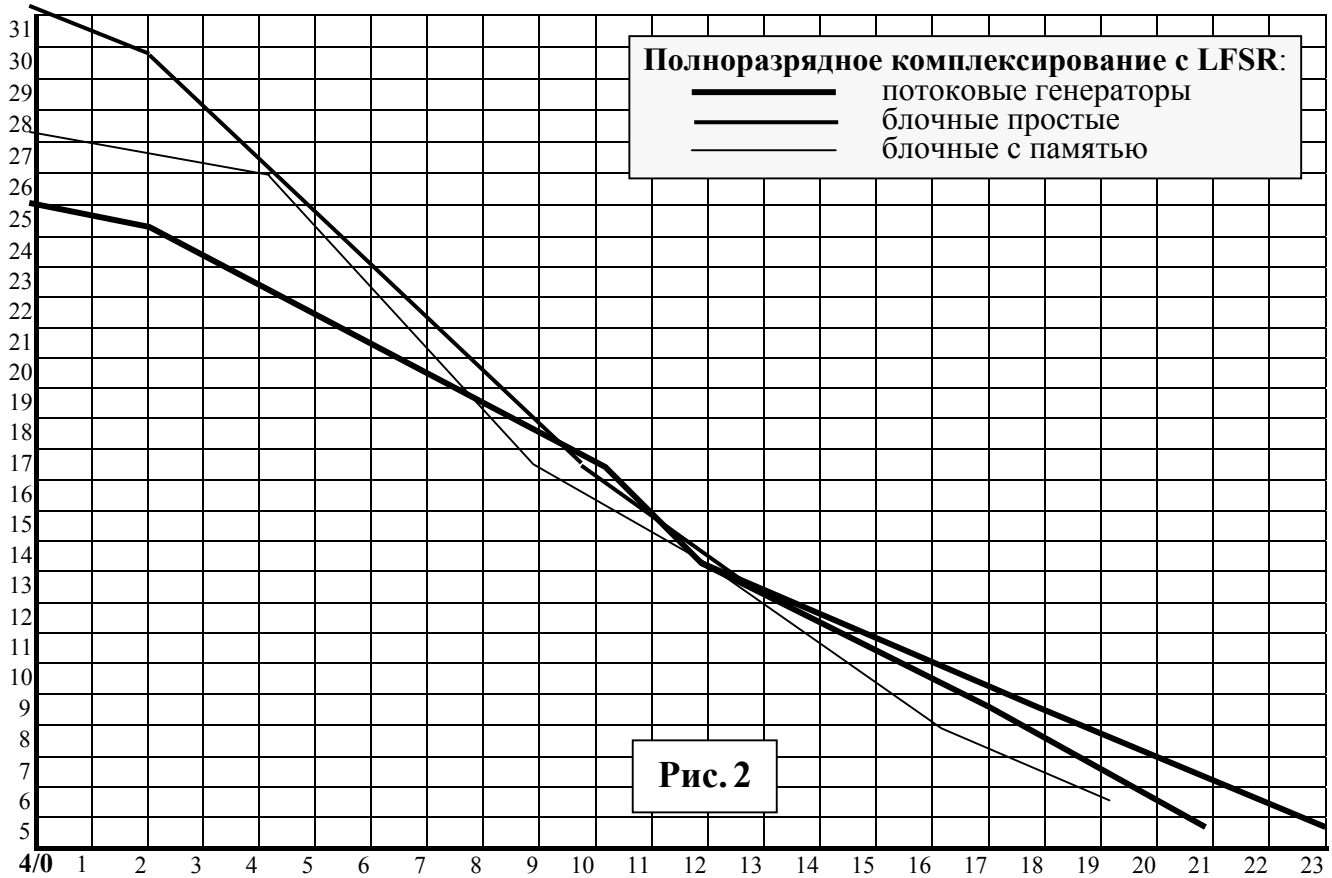

Рис. 2

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.