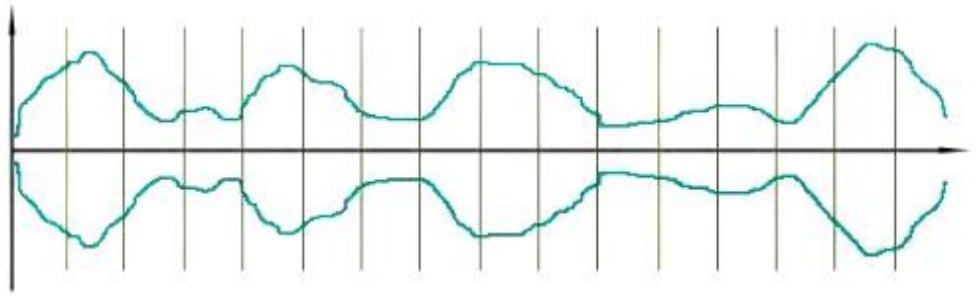
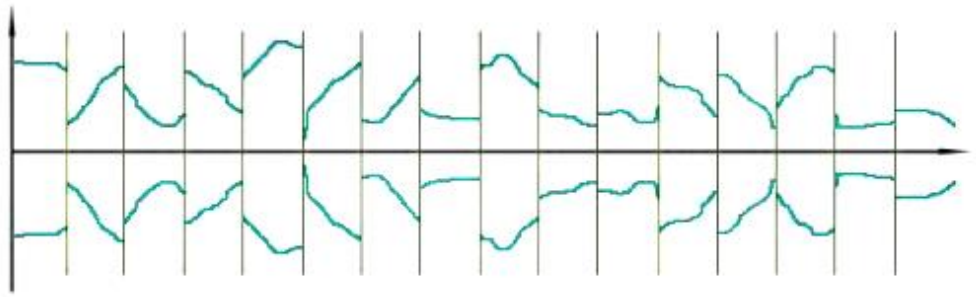
LFSR, PRNG, TRNG

Использование

- Тестовые последовательности
- Криптография
- Скремблирование — обратимое преобразование цифрового потока без изменения скорости передачи с целью получения свойств случайной последовательности
- Генерация случайного джиттера

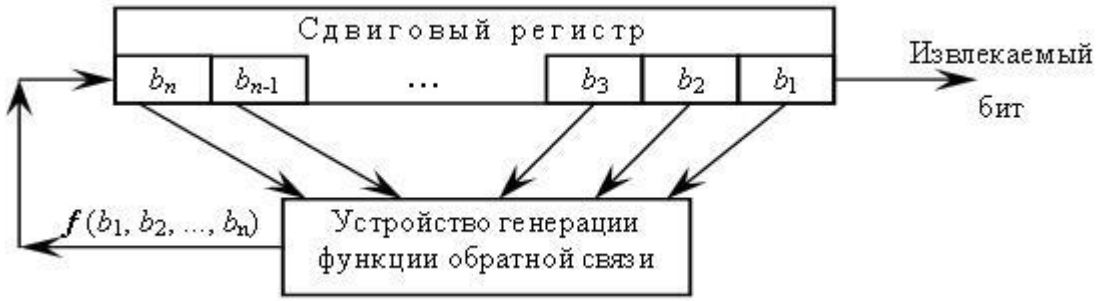


Нормальный вид голосового сообщения



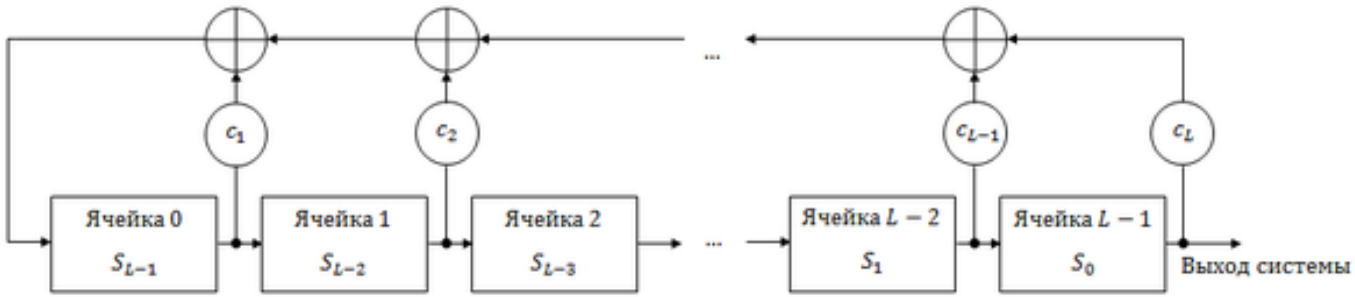
Скремблированное голосовое сообщение

Регистр сдвига с обратной связью



- Линейные $C(x) = c_L x^L + c_{L-1} x^{L-1} + \cdots + c_1 x + 1$
- Нелинейные

LFSR



- Максимальная длинна
- Примитивные многочлены

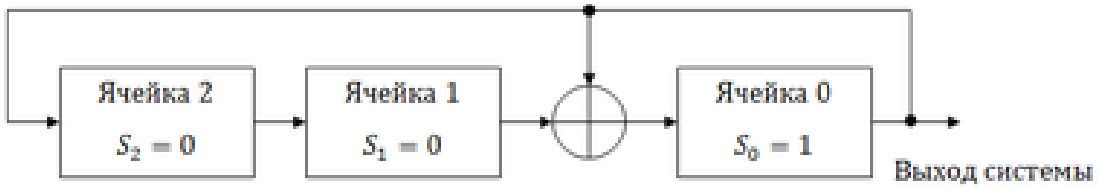
Примитивные многочлены

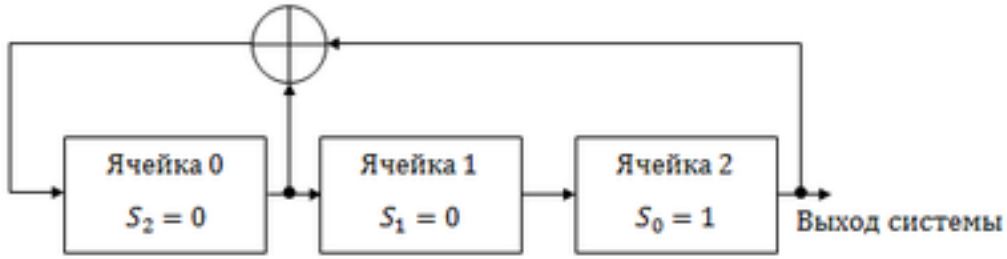
- Максимум 2^m-1
- Необходимые условия:
  - чётное число отводов;
  - номера отводов, взятые все вместе, а не попарно, взаимно просты.

If tap sequence of *n*-bit LFSR generating primitive polynomial is ***n, m, l, k, ..., 0*** then the tap sequence *n - n, n - m, n - l, n - k, ..., n - 0* i.e.
0, n - m, n - l, n - k, ..., n will also give primitive polynomial.

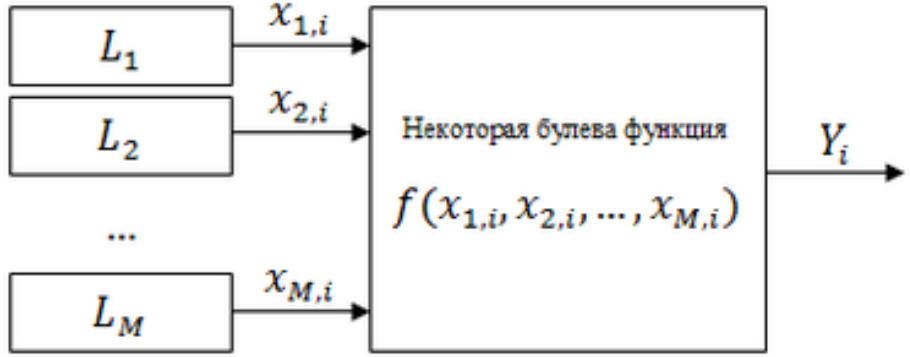
Биты, n	Примитивный многочлен	Период, $2^n - 1$	Число примитивных многочленов
2	$x^2 + x + 1$	3	1
3	$x^3 + x^2 + 1$	7	2
4	$x^4 + x^3 + 1$	15	2
5	$x^5 + x^3 + 1$	31	6
6	$x^6 + x^5 + 1$	63	6
7	$x^7 + x^6 + 1$	127	18
8	$x^8 + x^6 + x^5 + x^4 + 1$	255	16
9	$x^9 + x^5 + 1$	511	48
10	$x^{10} + x^7 + 1$	1023	60
11	$x^{11} + x^9 + 1$	2047	176
12	$x^{12} + x^{11} + x^{10} + x^4 + 1$	4095	144
13	$x^{13} + x^{12} + x^{11} + x^8 + 1$	8191	630
14	$x^{14} + x^{13} + x^{12} + x^2 + 1$	16383	756
15	$x^{15} + x^{14} + 1$	32767	1800
16	$x^{16} + x^{14} + x^{13} + x^{11} + 1$	65535	2048
17	$x^{17} + x^{14} + 1$	131071	7710
18	$x^{18} + x^{11} + 1$	262143	7776
19	$x^{19} + x^{18} + x^{17} + x^{14} + 1$	524287	27594

Конфигурация Галуа и Фибоначи



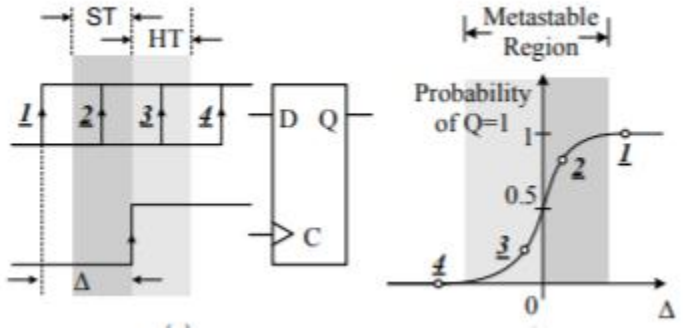


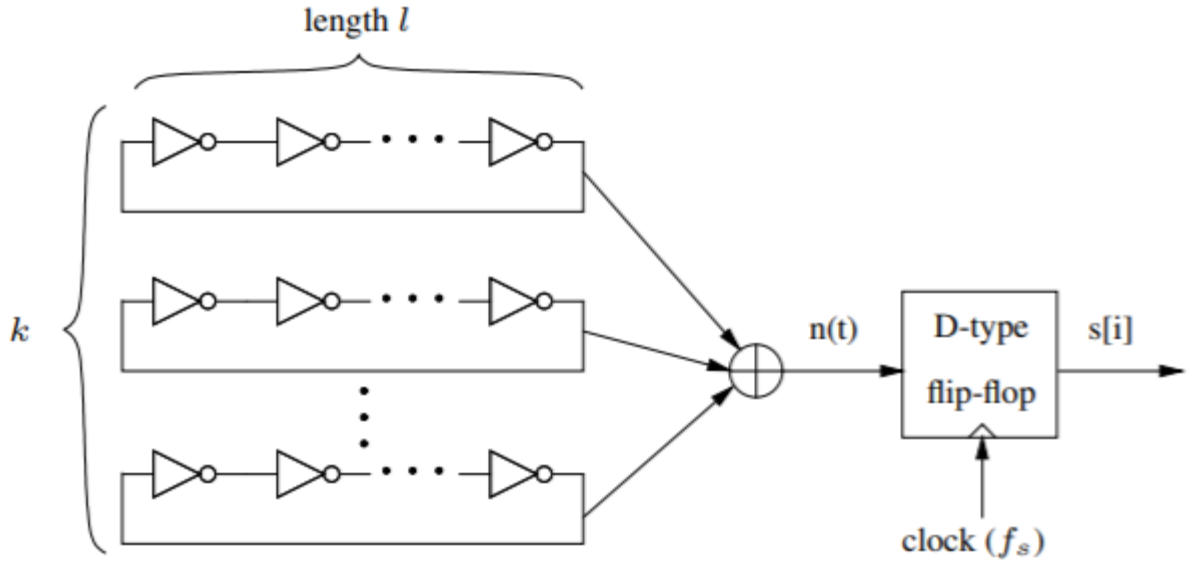
- Счетчики
- Скремблирование
- У объединения размеры регистров взаимно просты



TRNG

- По статье FPGA VENDOR AGNOSTIC TRUE RANDOM NUMBER GENERATOR
- По метастабильности триггера





TRNG параметры

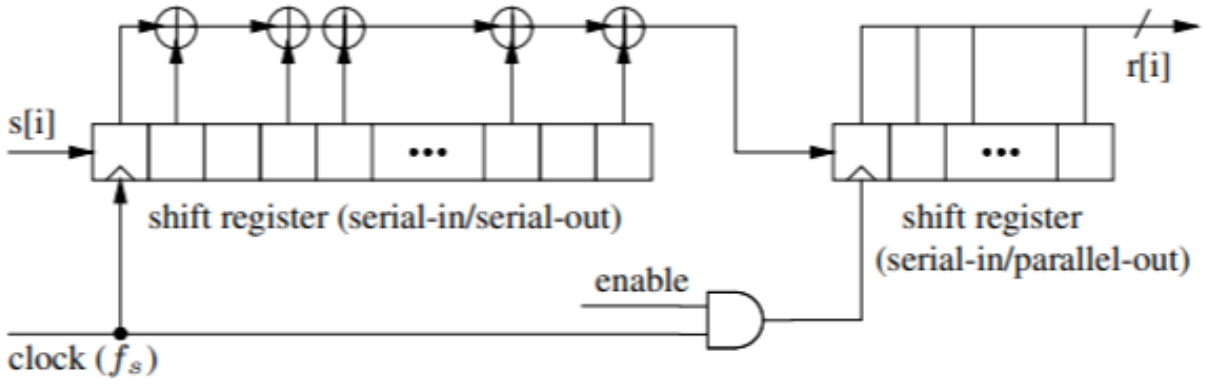
- Одинаковая длина КГ
- Коэффициент заполнения

length l	25	41	57	67	83	101
jitter/period (%)	1.46	0.91	0.67	0.57	0.56	0.49

jitter/ period	fill rate f 0.50	0.55	0.60	0.65	0.70	0.75	0.80	0.85	0.90	0.95
4%	45	53	59	70	79	94	107	133	158	231
2%	83	96	110	127	146	169	198	236	292	393
1%	158	182	210	241	277	320	374	445	548	733

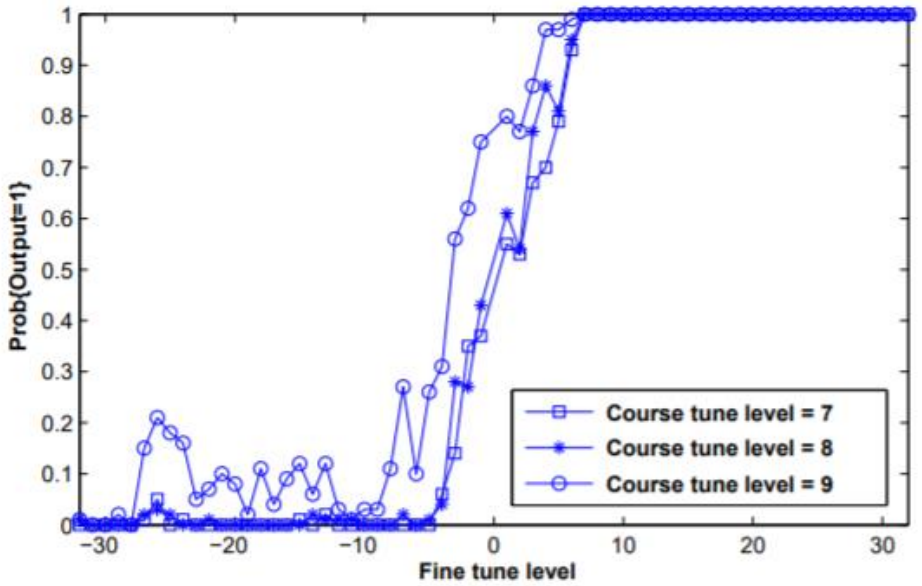
Постобработка

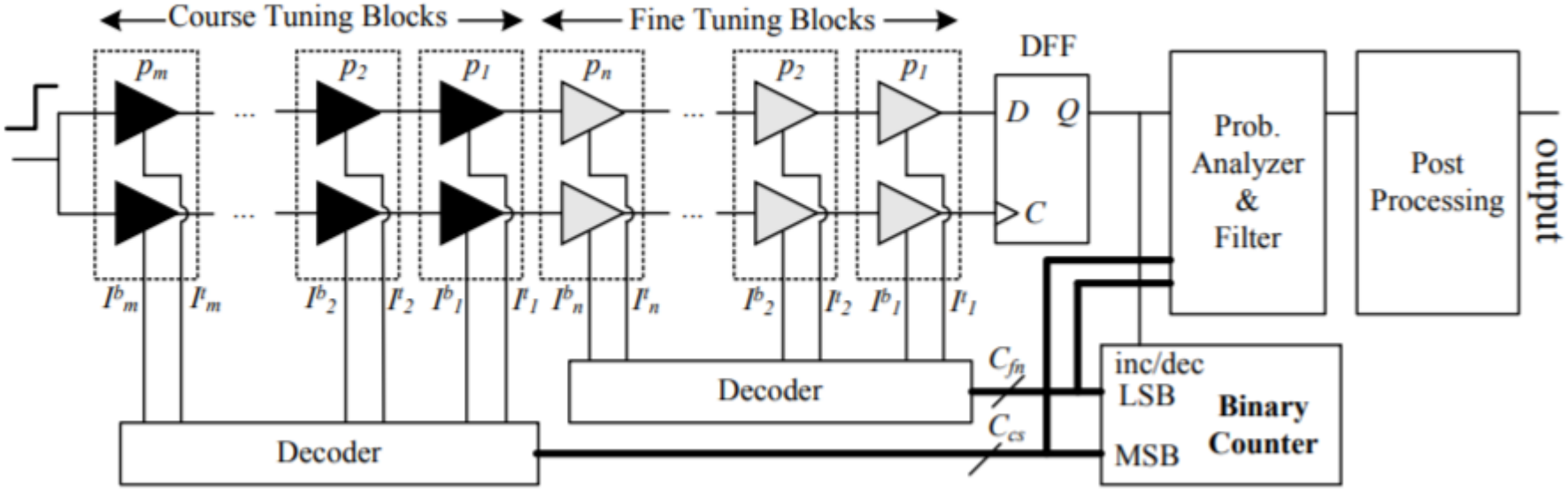
- Использовать один TRNG
- Использовать несколько TRNG



Еще TRNG

- Обратная связь
- Линия Вернье





Нормальное распределение

- Box–Muller transform
- ЦПТ
- LUT

$$z_0 = \cos(2\pi\varphi)\sqrt{-2\ln r},$$
$$z_1 = \sin(2\pi\varphi)\sqrt{-2\ln r}.$$