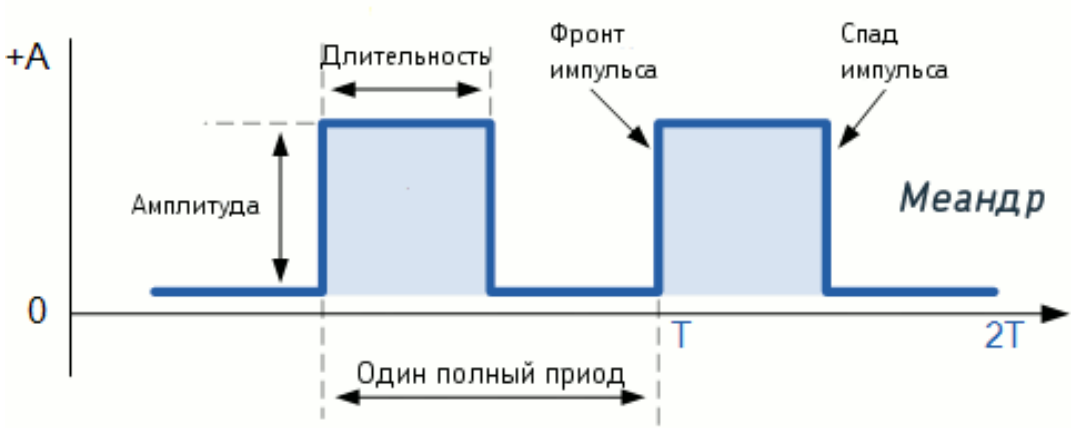
Временные параметры элементов

Синхросигнал

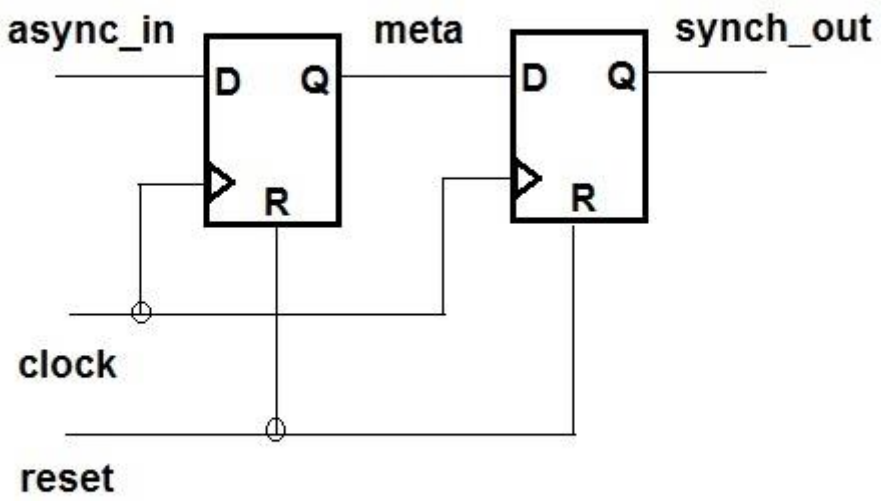
- Тактовый сигнал, или синхросигнал, — сигнал, использующийся для согласования операций одной или более цифровых схем.



Параметры Flip-Flop

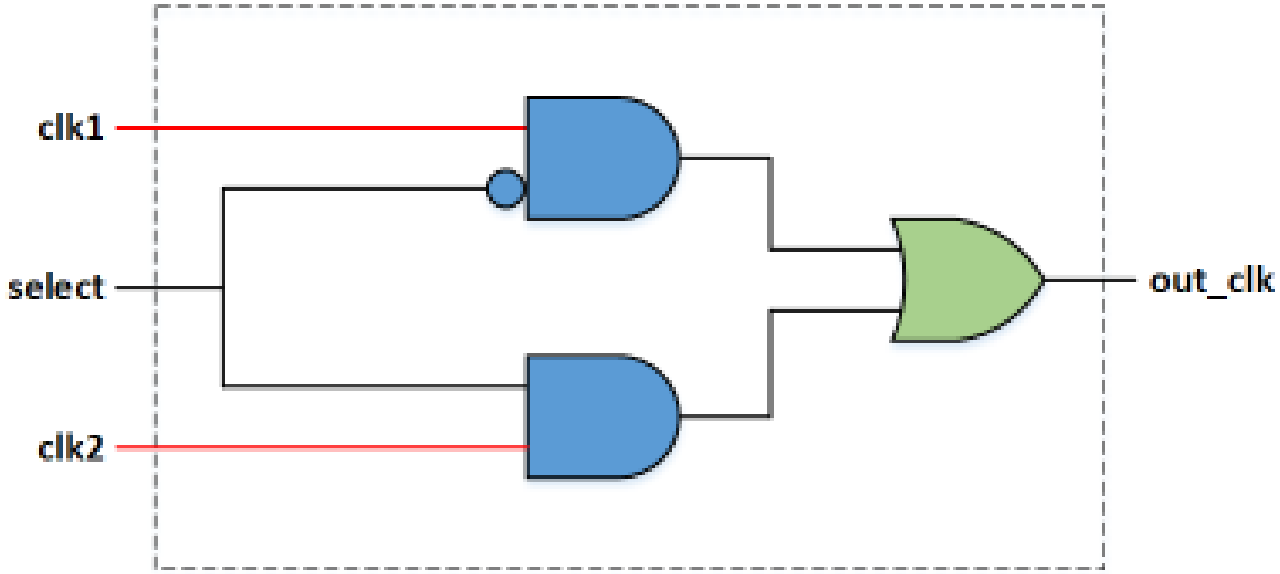
- Propagation time (от CLK до Q)
- T_setup (от D до CLK)
- T_hold (от CLK до D)
- ASYNC RESET:
  - Recovery (release RST to CLK)
  - Removal (CLK to release RST)

Synchronizer

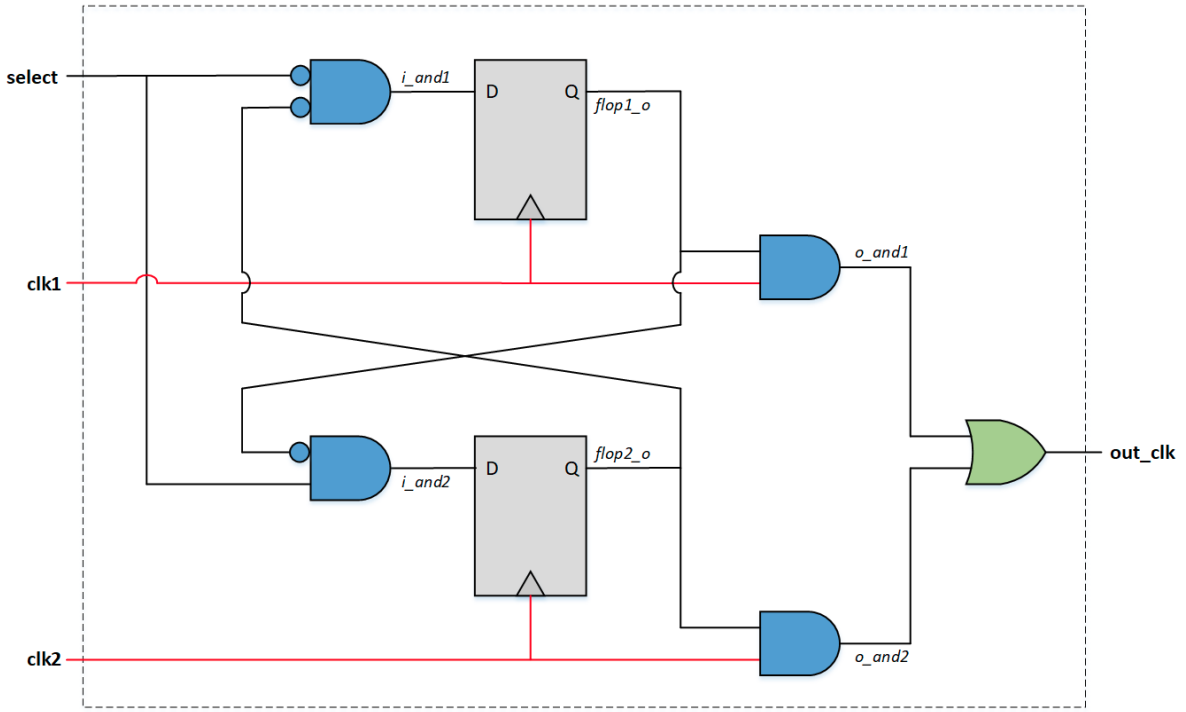


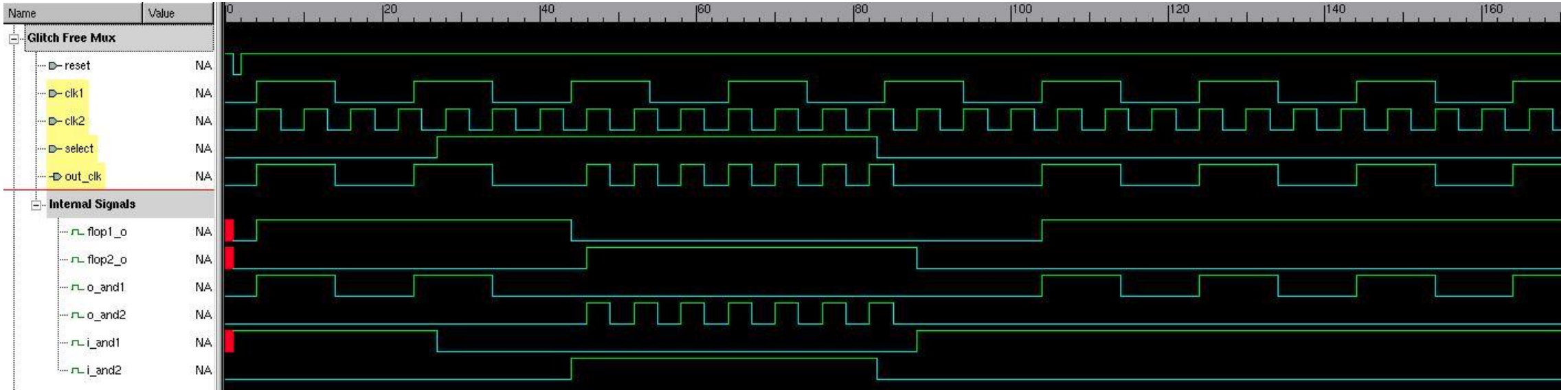
sync_ss

CLKMUX

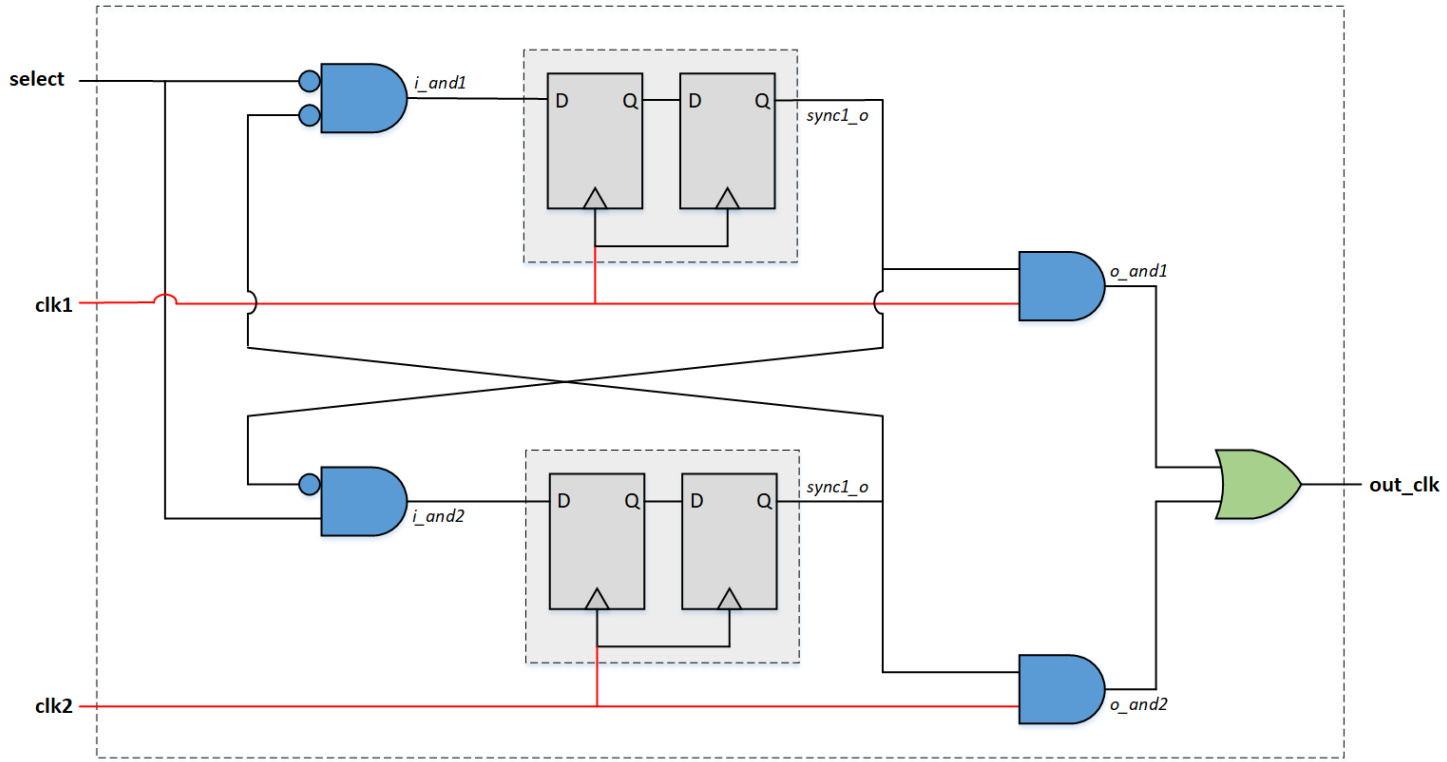


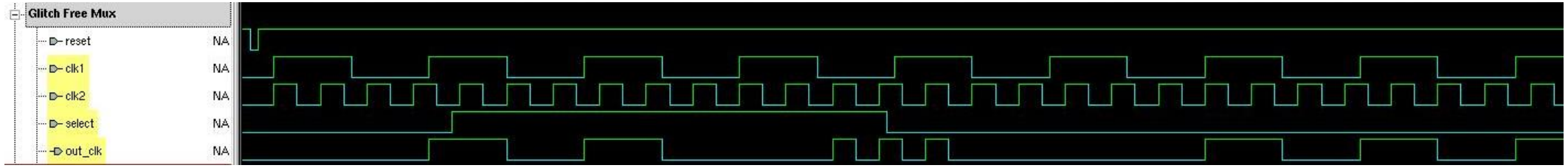
CLKMUX


select
clk1
clk2
i_and1
i_and2
D
Q
flop1_o
flop2_o
o_and1
o_and2
out_clk

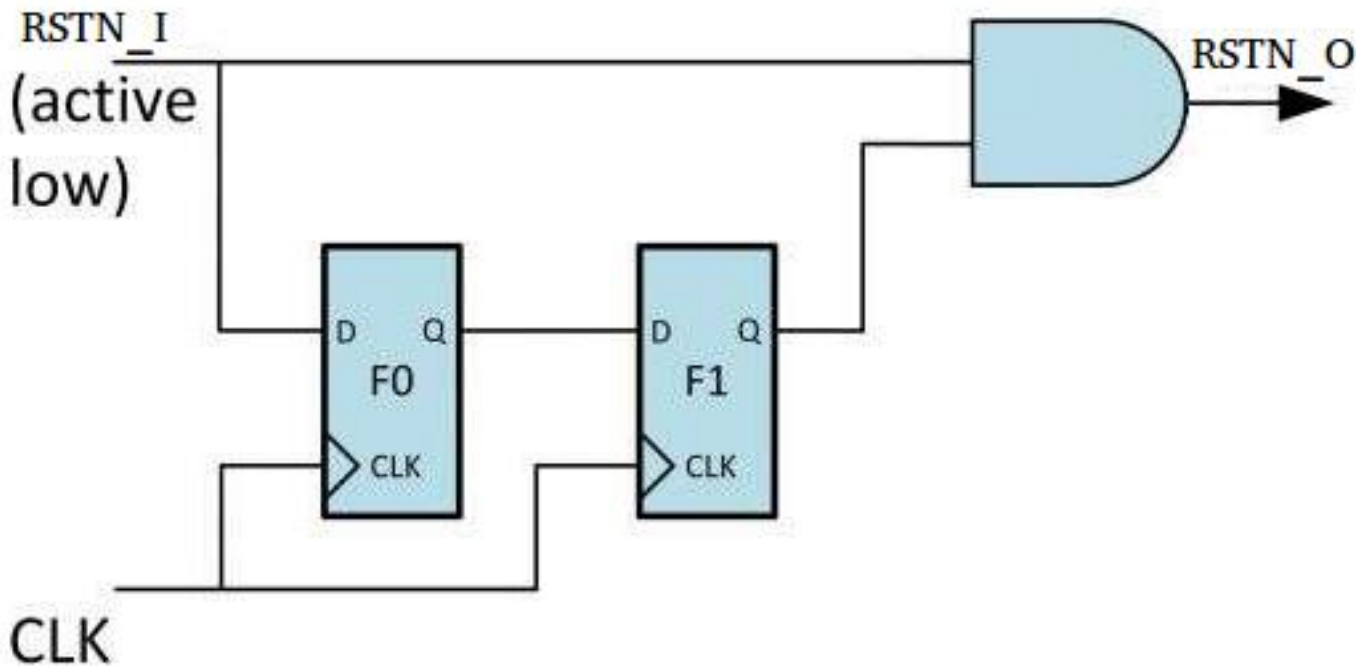

Name
Value
Glitch Free Mux
reset
clk1
clk2
select
out_clk
Internal Signals
flop1_o
flop2_o
o_and1
o_and2
i_and1
i_and2
NA
0
20
40
60
80
100
120
140
160

CLKMUX


select
clk1
clk2
i_and1
i_and2
o_and1
o_and2
sync1_o
sync1_o
D
Q
D
Q
D
Q
D
Q
out_clk


Glitch Free Mux
reset
NA
clk1
NA
clk2
NA
select
NA
out_clk
NA

Async reset



Constraints

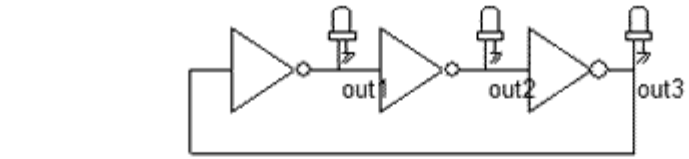
- Формат .sdc
- Описывает временные ограничения и требования к сигналам.
- Описывает ложные пути
- Описывает тестовые сигналы

Примеры

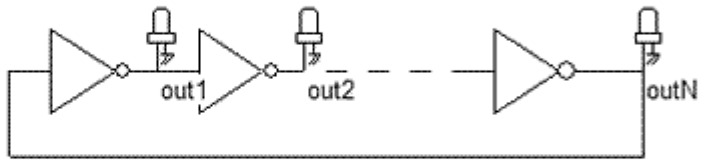
```
create_clock -name {clk} -period 4.000 -waveform { 0.000 2.000 }
[get_ports {clk}]

create_clock -period 10 [get_ports clk]
create_generated_clock -divide_by 2 -source [get_ports clk] -name
clkdiv [get_registers clkdiv]

set_clock_uncertainty -setup -rise_from clk1 -fall_to clk2 200ps
set_max_delay -from [get_clocks clkA] -to [get_clocks clkB] 0.000
set_input_delay -clock clk 1.5 [get_ports myin*]
```

Кольцевой генератор

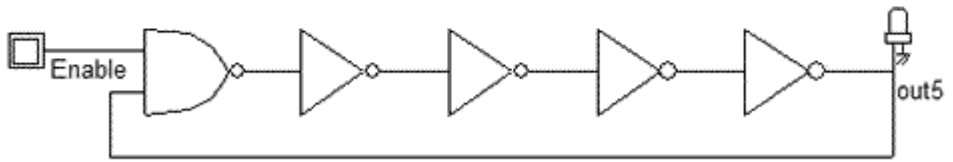
- На инвертирующих элементах
- На неинвертирующих элементах



Ring oscillator with 3 inverters



Ring oscillator with N inverters (Odd number)



5-stage ring oscillator with enable

Измерение. Делитель

- Джиттер на выходе равен джиттеру измеряемого сигнала
- Теряется информация о коэффициенте заполнения сигнала

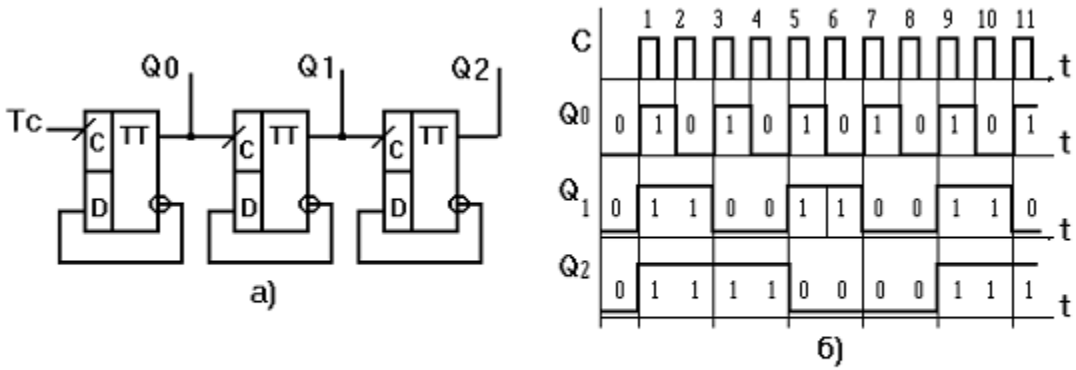


Рис. 3.34. Схема а) и временные диаграммы вычитающего трехразрядного счетчика на D - триггерах

Измерение. Random sampling

Формулировка Закона Больших Чисел [9]:

$$P\left(\left|\frac{\sum \xi}{n} - E\xi\right| \geq \varepsilon\right) \leq \frac{D\xi}{n\varepsilon^2}, \tag{10}$$

где ξ – измеряемая случайная величина, $E\xi$ – ее мат-ожидание, $D\xi$ – ее дисперсия, n – количество измерений, ε – ошибка. Таким образом, закон дает возможность получить значение количества измерений необходимое для того, чтобы вероятность того, что ошибка измеренной величины больше ε была меньше $D\xi/(n\varepsilon^2)$.

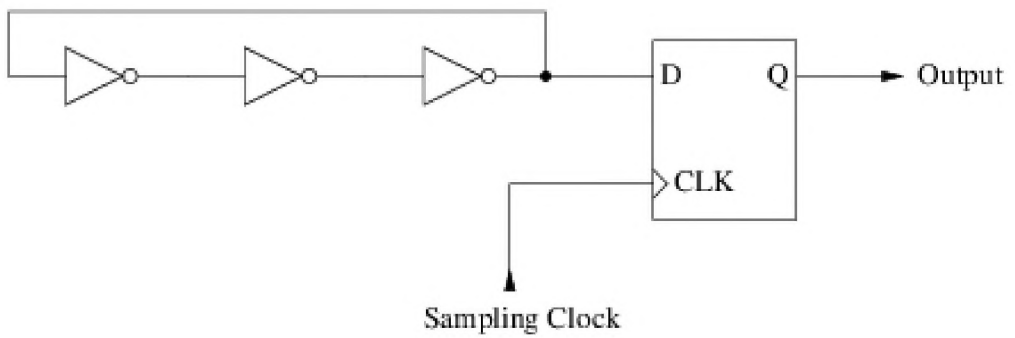
В нашей задаче случайной величиной ξ считается значение одного семпла, n – количество семплов. Сейчас буду считать идеальную задачу, в которой не учитывается возможные ошибки из-за метастабильности семплирующих флип-флопов. В таком случай, если период измеряемого сигнала T_{osc}, время единичного уровня T_h, то понимая под случайной величиной результат одного семпла:

$$E\xi = \frac{T_h}{T_{osc}}, \quad D\xi = E\xi^2 - (E\xi)^2 = E\xi(1 - E\xi); \tag{11}$$

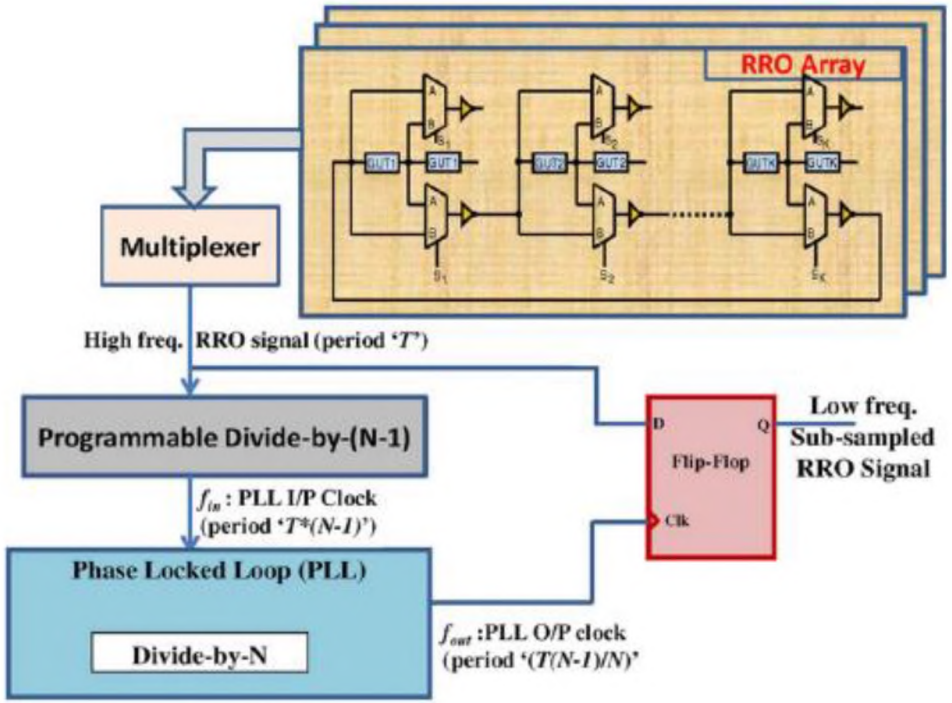
В (10) величина ε суть есть целевая точность измерения, а правая часть неравенства определяет доверительный интервал (уровень доверия) p. Пускай α – целевая относительная ошибка. Тогда, выражение для n в идеальном случае:

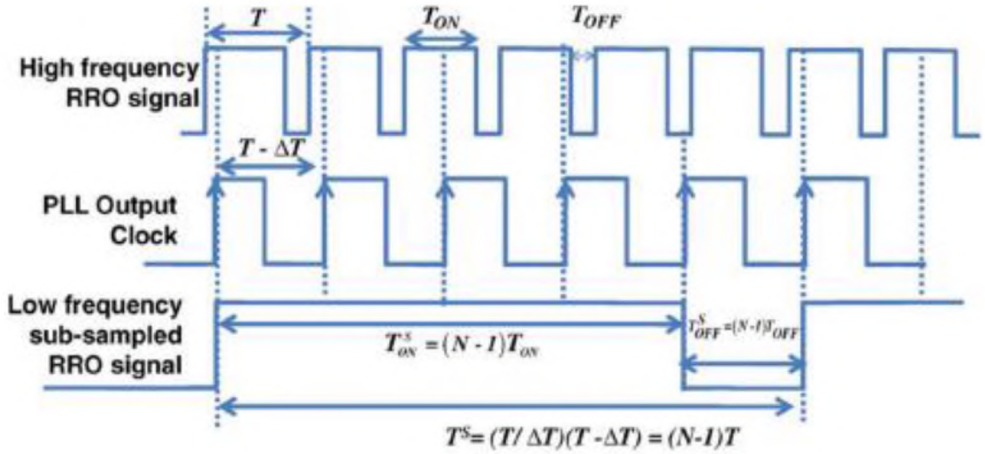
$$\alpha = \frac{\varepsilon}{E\xi}, \quad \Rightarrow \quad p = \frac{E\xi(1 - E\xi)}{n_{ideal}\varepsilon^2} = \frac{1 - E\xi}{n_{ideal}\alpha^2 E\xi} \quad \Rightarrow \tag{12}$$

$$\Rightarrow \quad \boxed{n_{ideal} = \frac{1 - E\xi}{E\xi}\frac{1}{p\alpha^2}} \tag{13}$$



Измерение. Subsampling

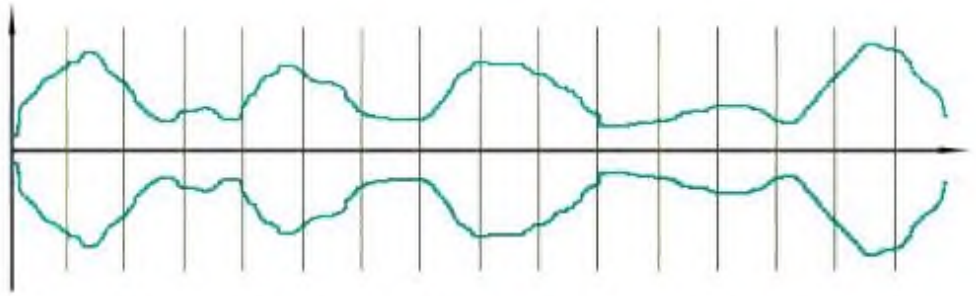




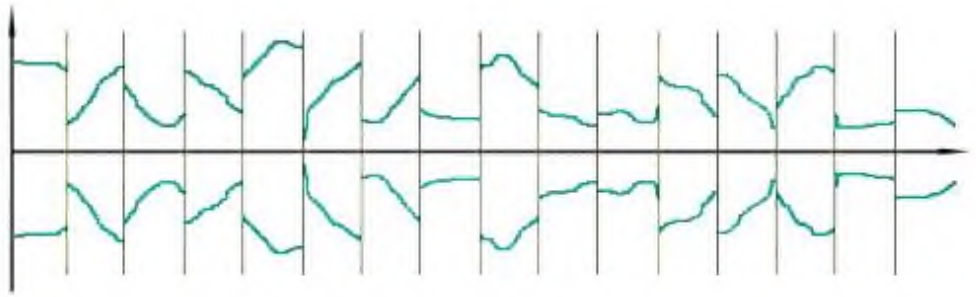
LFSR, PRNG, TRNG

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

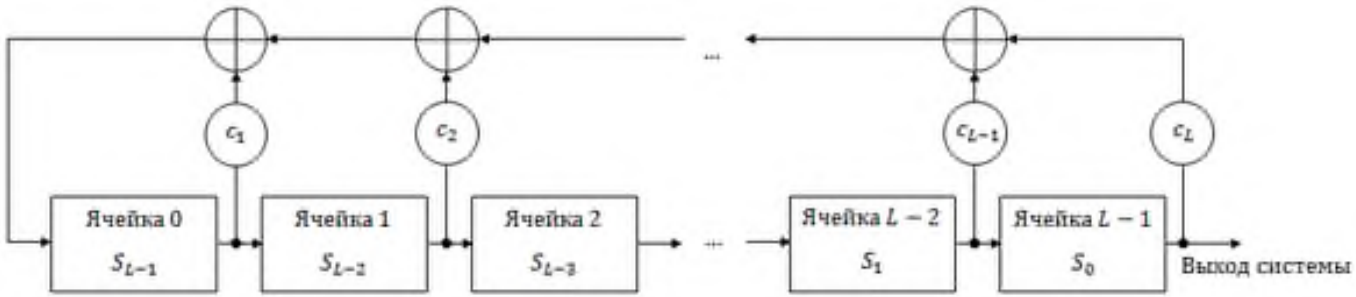


Скремблированное голосовое сообщение

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

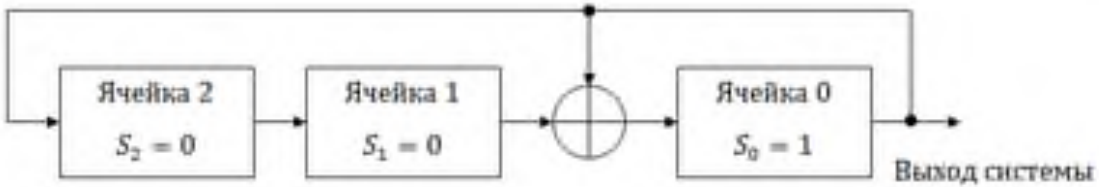
Примитивные многочлены

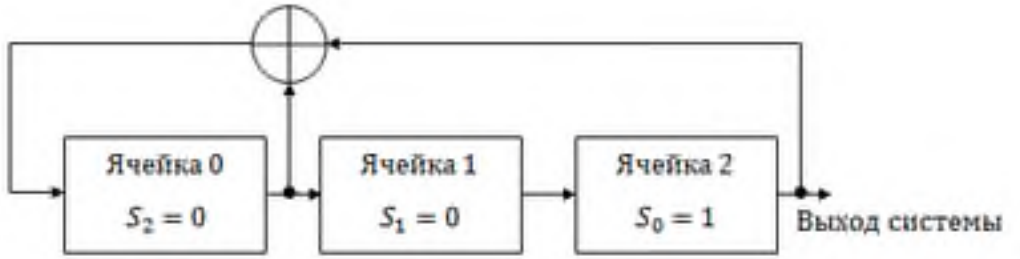
- Максимум 2^m-1
- Необходимые условия:
  - чётное число отводов;
  - номера отводов, взятые все вместе, а не попарно, взаимно просты.

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.

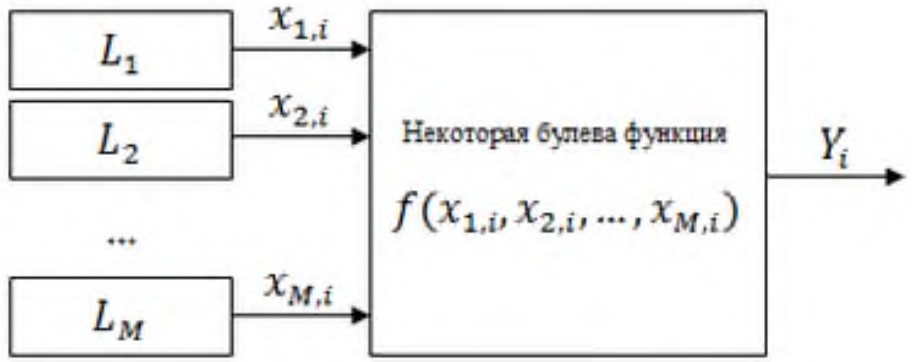
Биты, n	Примитивный многочлен	Период, $2^n - 1$	Число примитивных многочленов
2	$x^2 + x + 1$	3	1
3	$x^3 + x^2 + 1$	7	2
4	$x^4 + x^3 + 1$	15	2
5	$x^5 + x^3 + 1$	31	6
6	$x^6 + x^5 + 1$	63	6
7	$x^7 + x^6 + 1$	127	18
8	$x^8 + x^6 + x^5 + x^4 + 1$	255	16
9	$x^9 + x^5 + 1$	511	48
10	$x^{10} + x^7 + 1$	1023	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



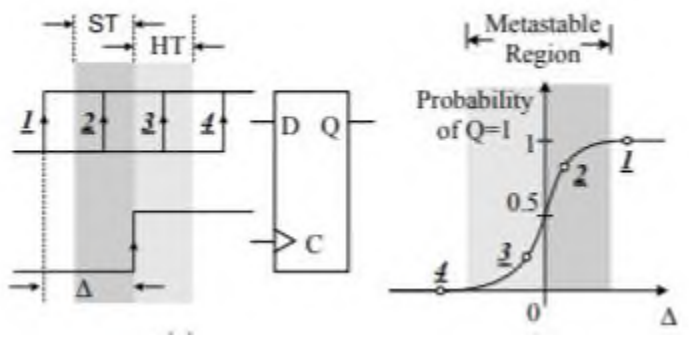


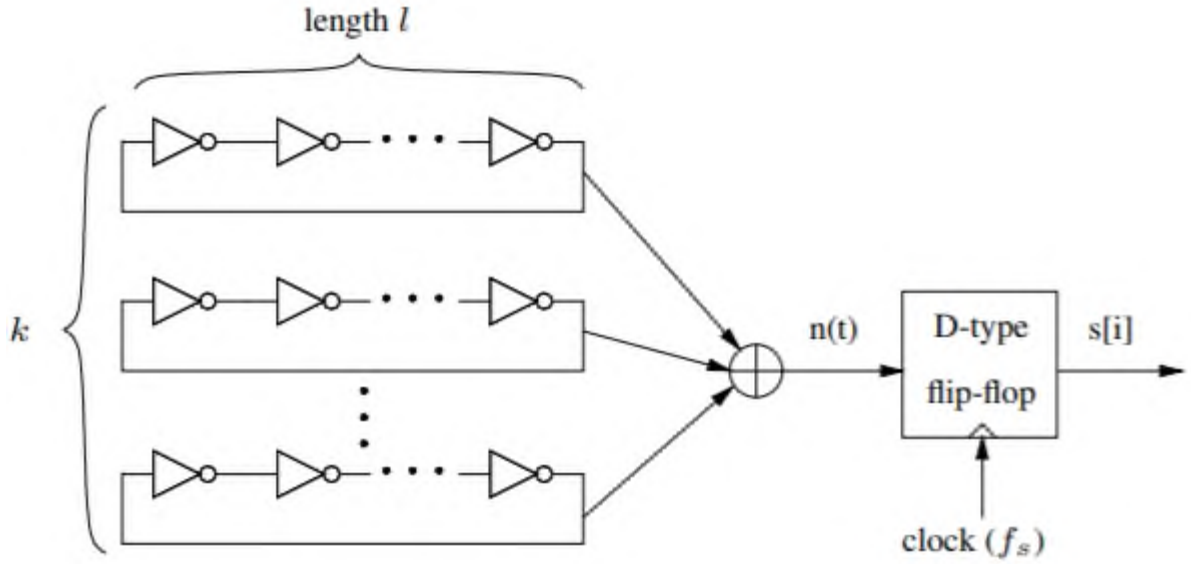
- Счетчики
- Скремблирование
- У объединения размеры регистров взаимно просты



TRNG

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





TRNG параметры

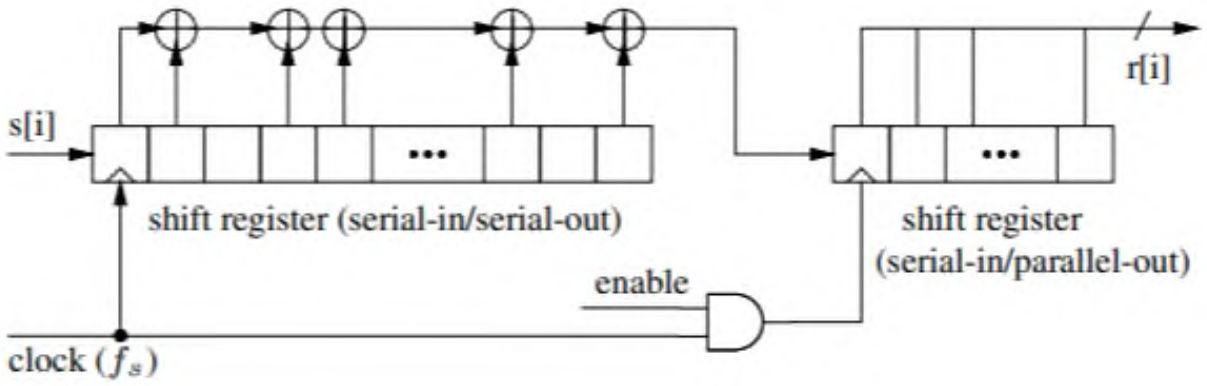
- Одинаковая длина КГ
- Коэффициент заполнения

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

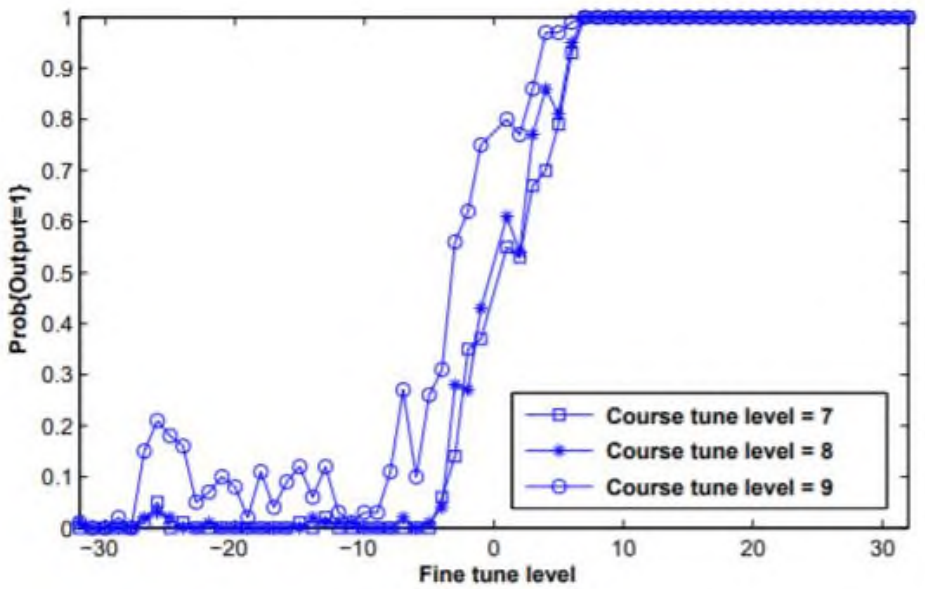
Постобработка

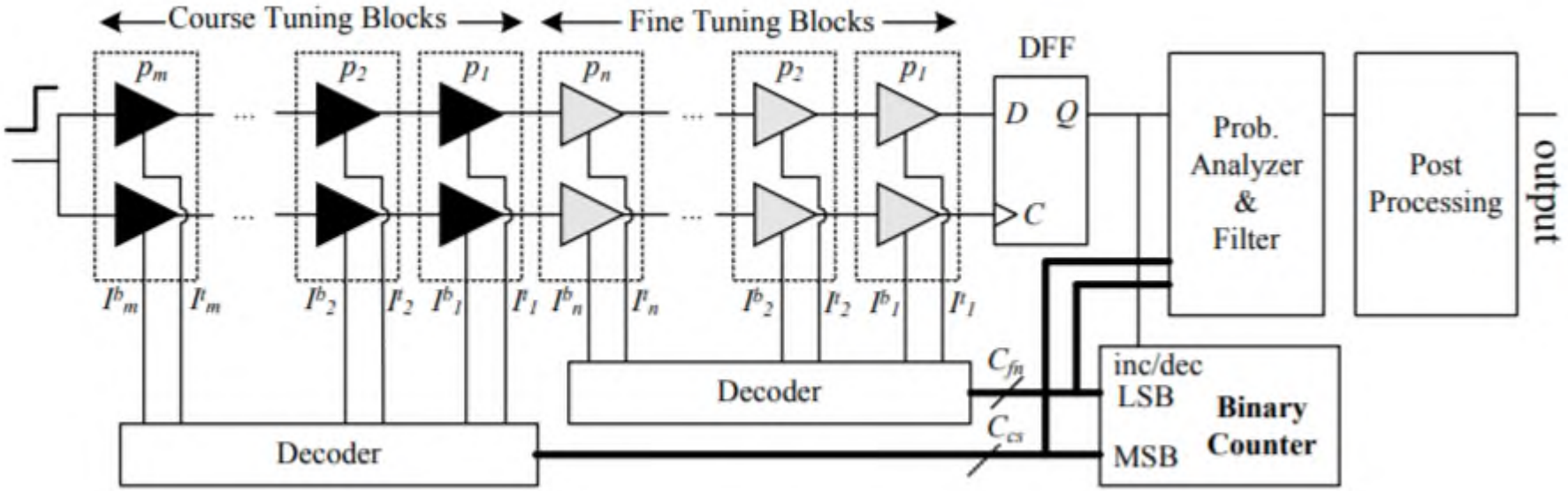
- Использовать один TRNG
- Использовать несколько TRNG



Еще TRNG

- Обратная связь
- Линия Вернье





Нормальное распределение

- Box–Muller transform
- ЦПТ
- LUT

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