

Курсовая работа на тему:

Генератор случайных чисел

*студентки 217 группы
Радовской Виктории Вадимовны*

*Научный руководитель:
Монахов Александр Михайлович
научный сотрудник*

Виды случайностей, получаемых аппаратно

псевдослучайность

- Элементы создаются алгоритмически
- Образование циклов последовательности генерируемых элементов
- Квазиравномерное распределение

случайность

- Используется электронная приставка к машине
- Образование циклов маловероятно
- Квазиравномерное распределение

Методы получения физической случайности:

1) Фиксирование излучения радиоактивных веществ

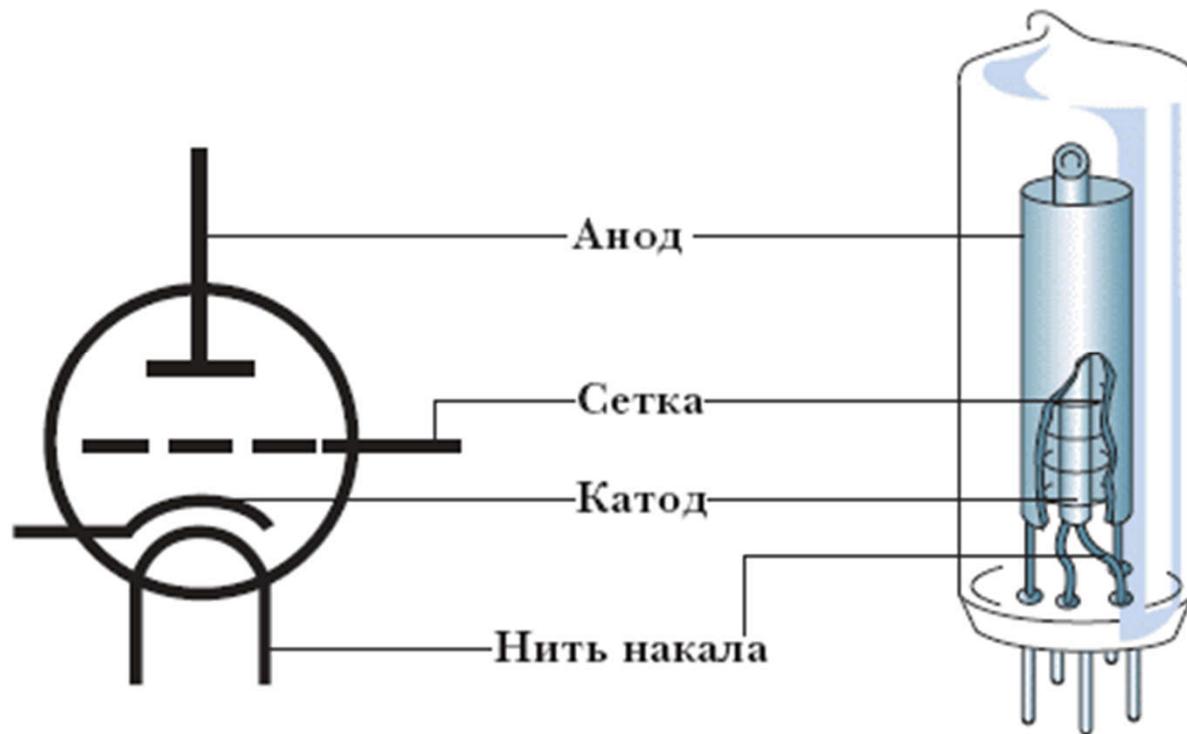
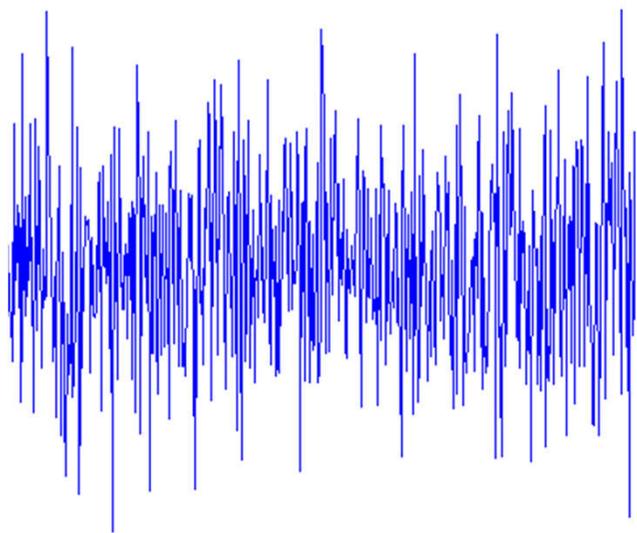
$$W_k = \frac{(\lambda \Delta t)^k}{k!} e^{-\lambda \Delta t}$$



$$p_r = \frac{1 + e^{-2\lambda \Delta t}}{2} \xrightarrow{\Delta t \rightarrow \infty} \frac{1}{2}$$

Методы получения физической случайности:

2) Фиксирование собственных шумов электронной лампы

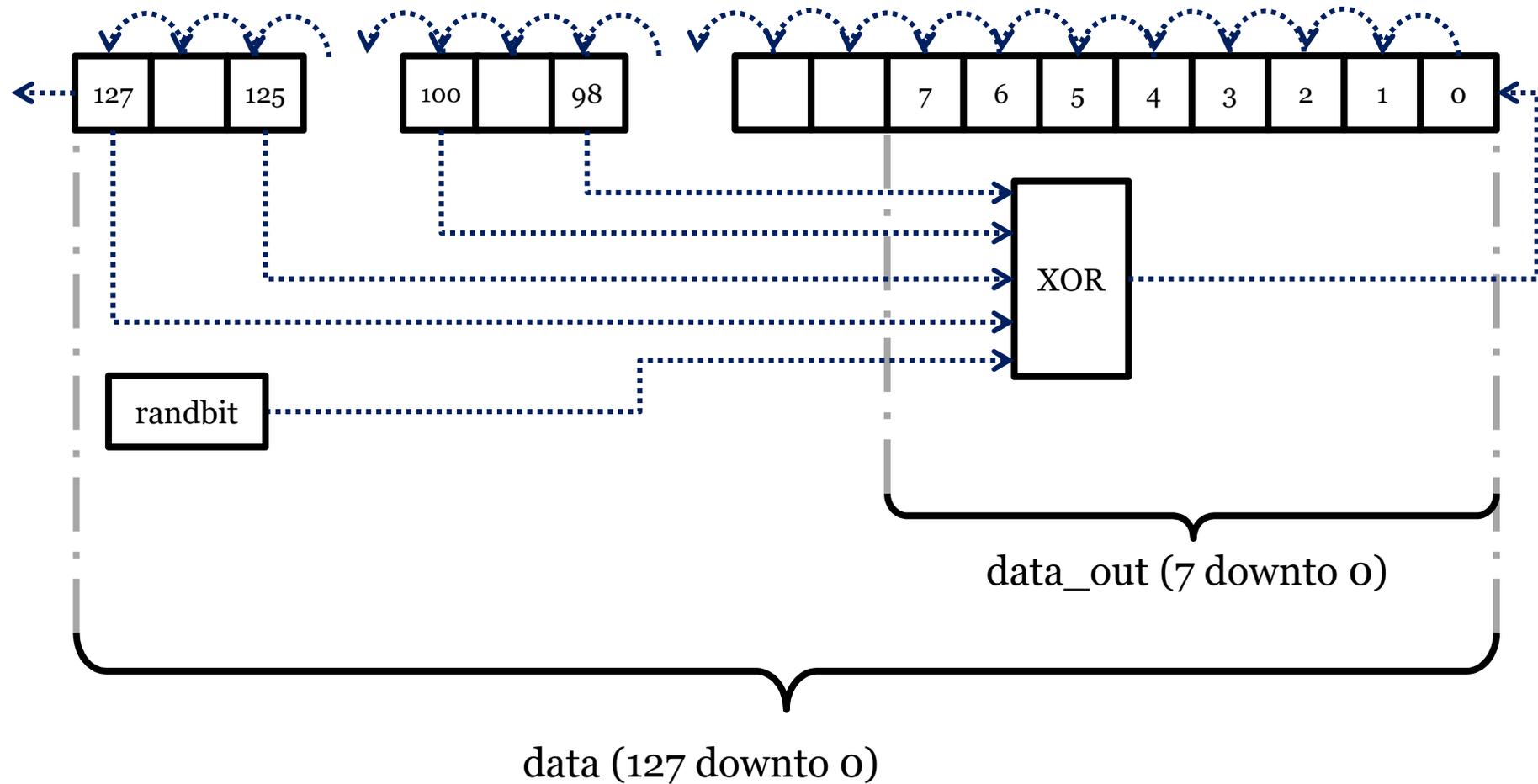


Предлагаемые методы реализации в ПЛИС:

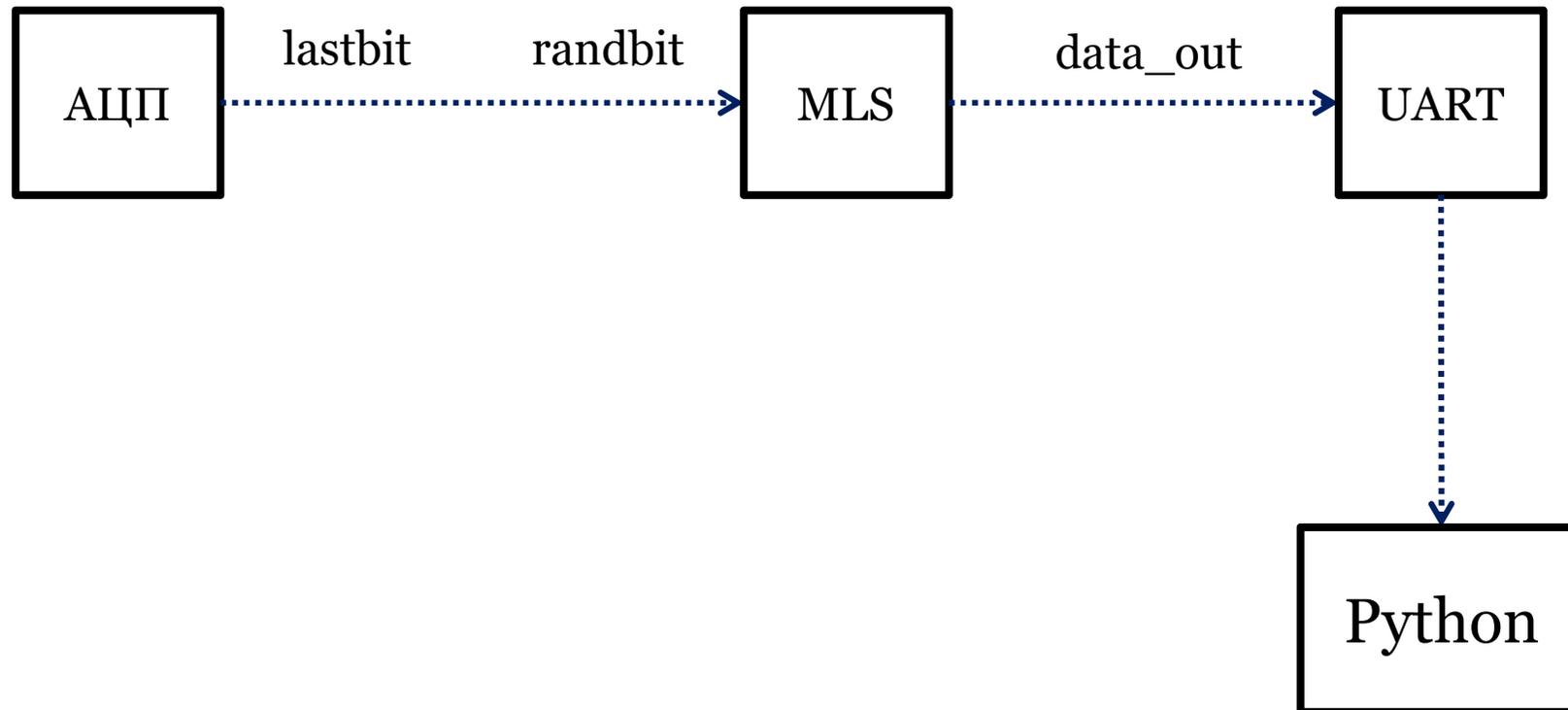
Генерация последовательности максимальной длины, для получения входного бита используется:

- a) шумы АЦП;
- b) «измерение» dt между моментами прихода единицы на последний бит АЦП;
- c) PLL и D-триггер

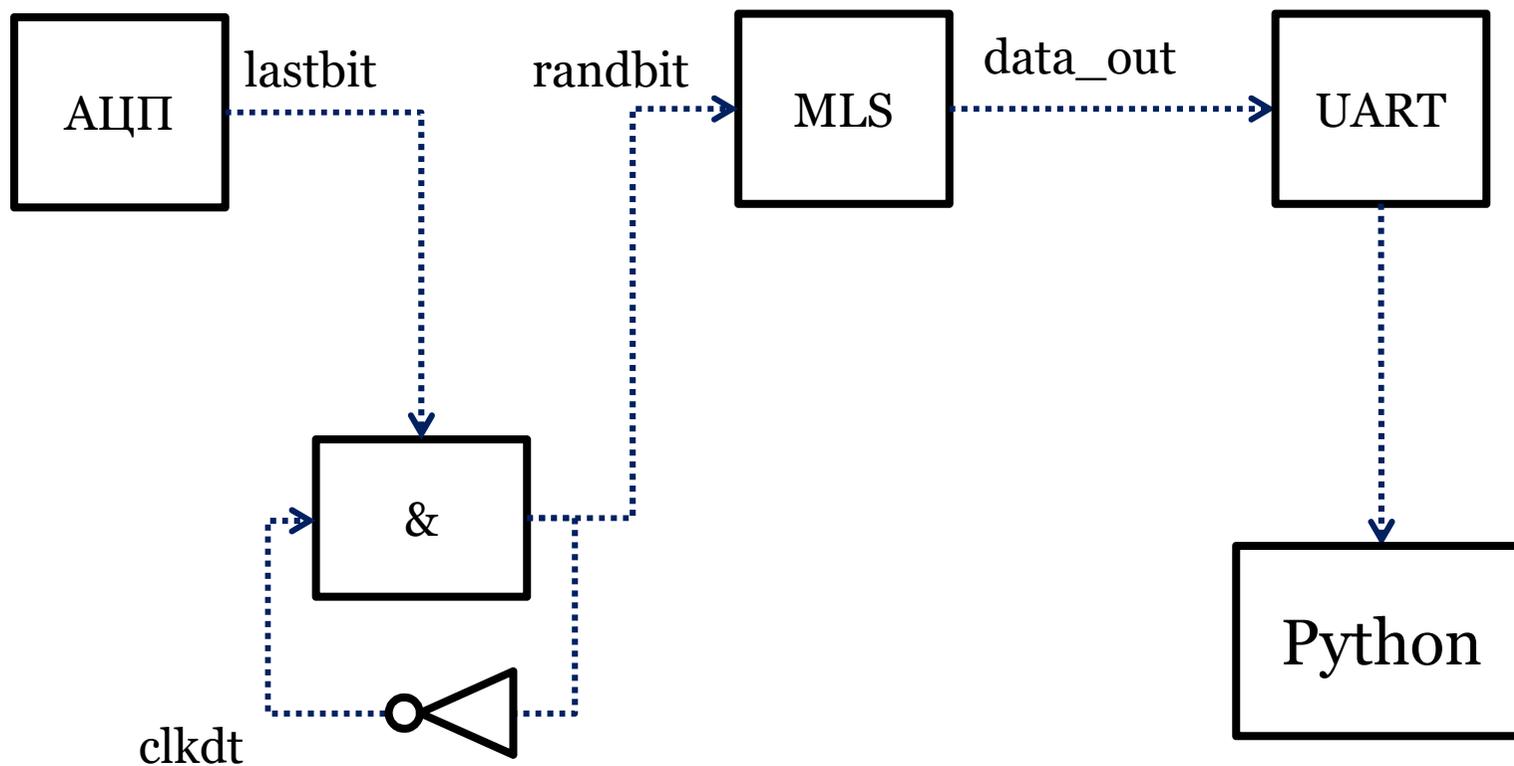
MLS - блок генерации M-последовательности:



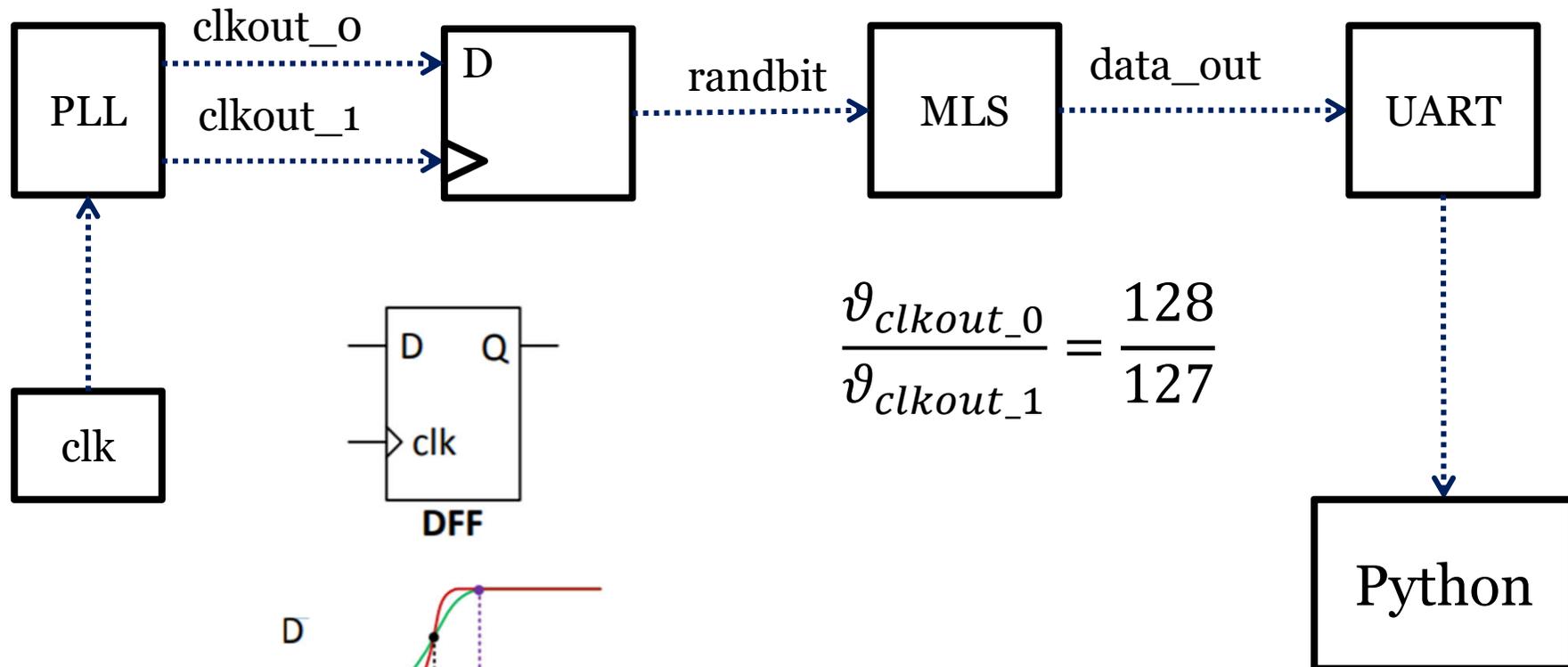
a) шумы АЦП



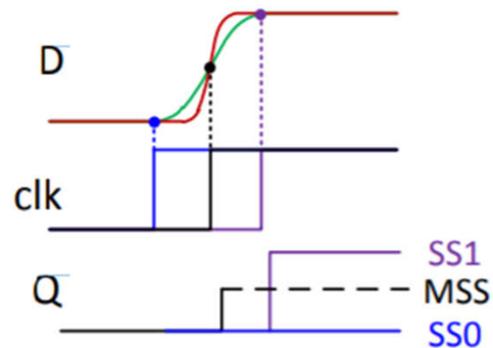
б) «измерение» dt между моментами прихода единицы на последний бит АЦП



в) PLL и D-триггер



$$\frac{\nu_{clkout_0}}{\nu_{clkout_1}} = \frac{128}{127}$$



Проверка на случайность:

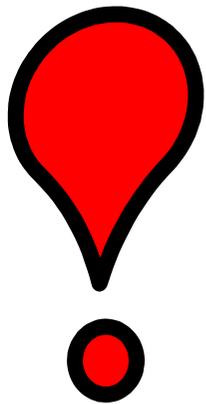
1. Среднее значение
2. Дисперсия
3. Автокорреляционная функция

Среднее и дисперсия:

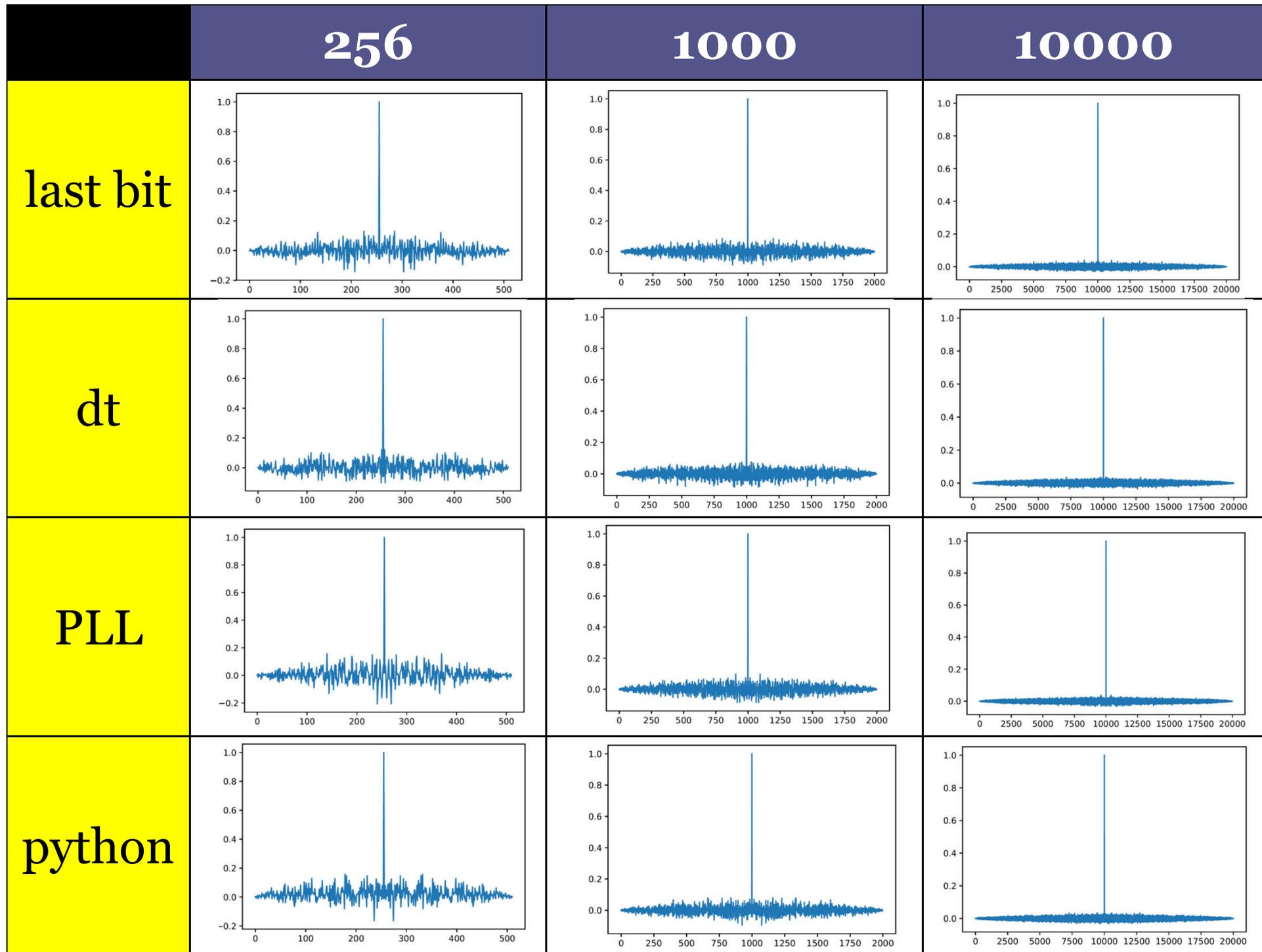
	256		1000		10000	
	middle	disp	middle	disp	middle	disp
ADC noise	124,1	5404,1	131,2	5652,4	127,2	5456,9
dt	130,4	5519,6	126,5	5477,4	128,2	5525,8
PLL	136,5	5654,3	128,3	5486,2	127,9	5496,9
python	112,2	5331,5	126,3	5322,9	127,4	5521,2

Автокорреляционная функция:

$$F_j = \sum_{i=1}^{VALUE-j} (data[i] - \widehat{data}) (data[i+j] - \widehat{data})$$



АКФ белого шума –
дельта-функция





Результаты:

1. Реализовано 3 варианта генератора случайных чисел в ПЛИС.
2. Доказано, что получаемые последовательности близки к белому шуму.