РусКрипто

XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

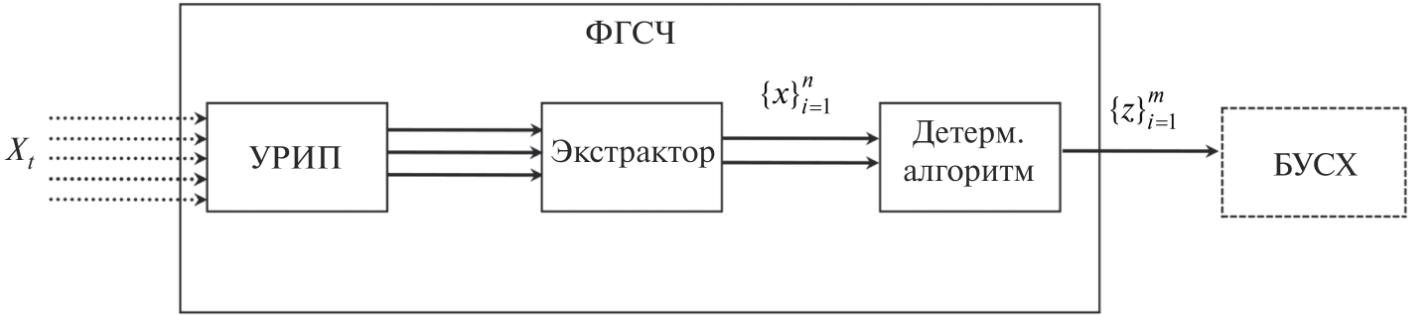
ТЕОРЕТИКО-ВЕРОЯТНОСТНЫЕ МОДЕЛИ ФИЗИЧЕСКИХ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ

РусКрипто

Богданов Дмитрий Сергеевич
Миронкин Владимир Олегович
Логачев Александр Станиславович

ТЕОРЕТИКО-ВЕРОЯТНОСТНЫЕ МОДЕЛИ ФИЗИЧЕСКИХ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ

РусКрипто



- X_t – исходный физический случайный процесс
- УРИП – устройство регистрации исходного процесса
- Экстрактор – устройство формирования сырой последовательности
- БУСХ – блок улучшения статистических характеристик

ТВМ и ТВО ФГСЧ

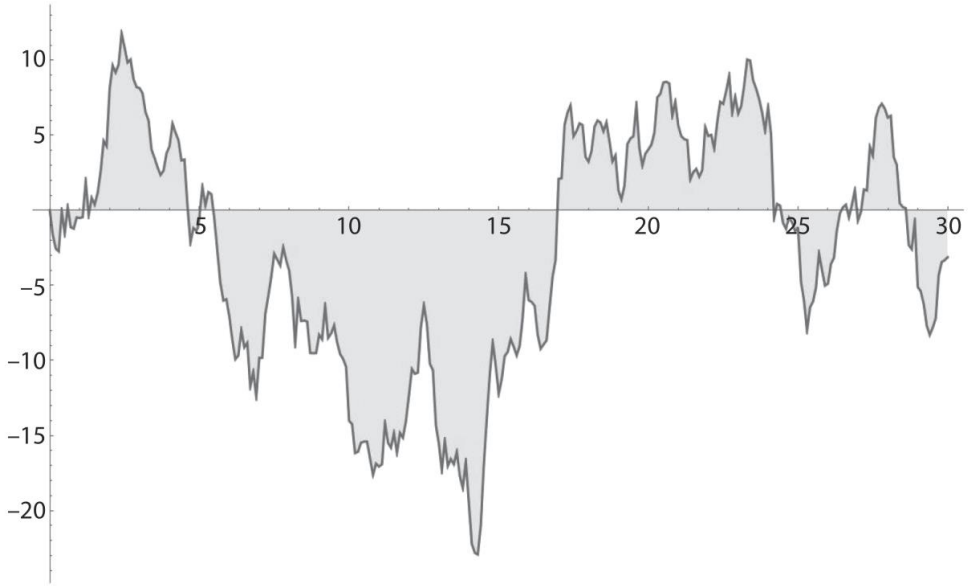
РусКрипто

ФТМ → ТВМ и ТВО → Криптография

- Случайные процессы
- Гауссовские процессы
- Процессы восстановления

- Неравновероятная модель
- Практическая секретность ключа
- Трудоёмкость методов опробования

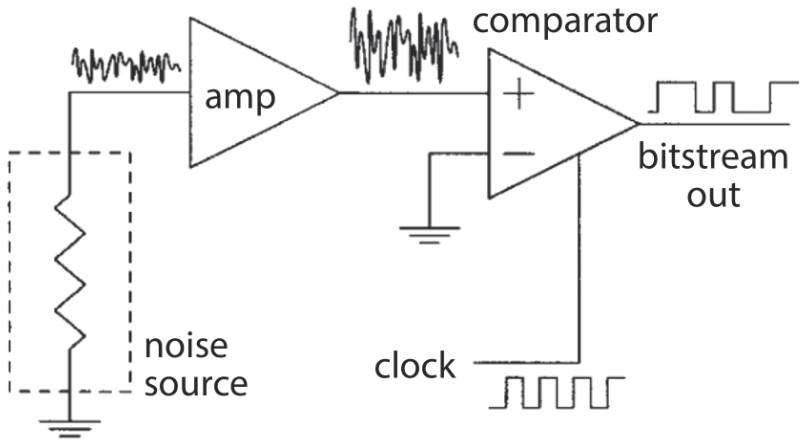
Схема мгновенных значений



- $X_t, t \geq 0$ – случайный процесс
- $f \geq 0$ – частота регистрации
- $x_1 = X_{\frac{1}{f}}, \quad x_2 = X_{\frac{2}{f}}, \quad x_3 = X_{\frac{3}{f}}, \ldots$ – «сырая» последовательность

РусКрипто

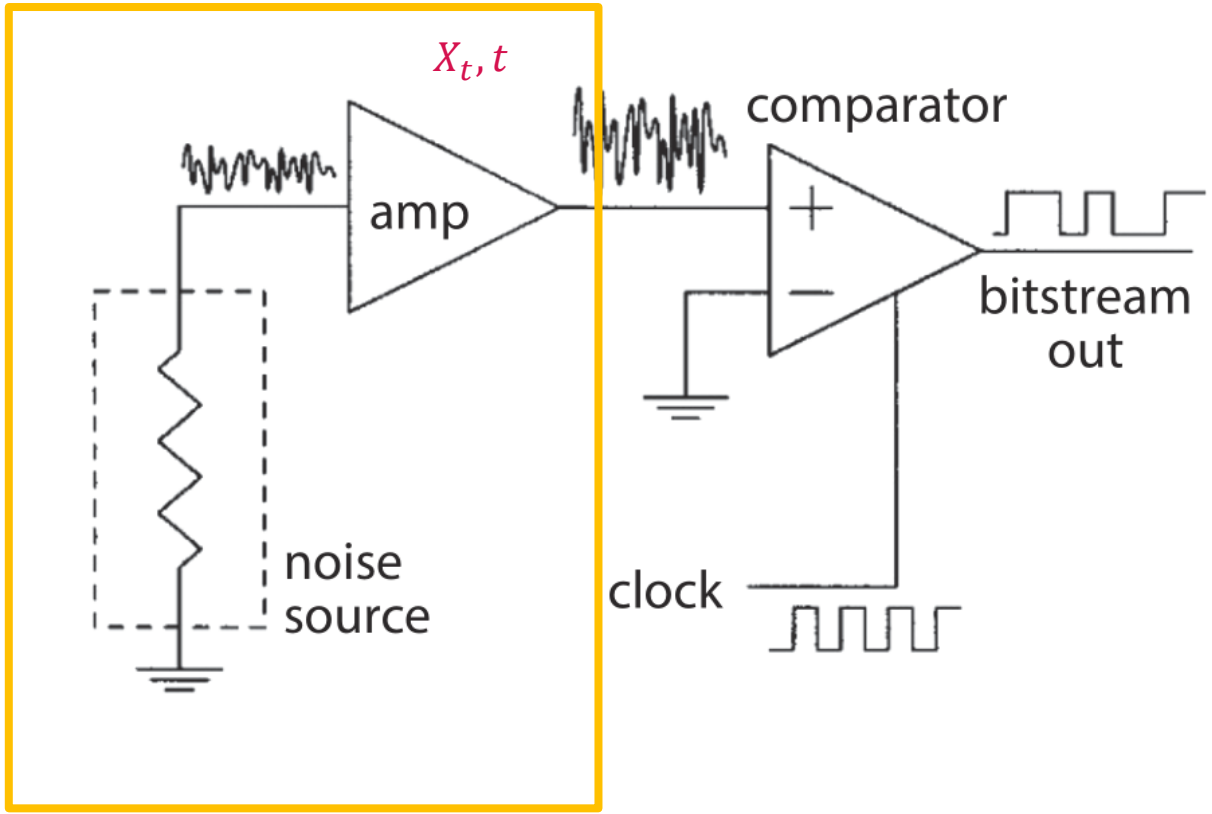
Схема мгновенных значений



[1] Petrie C. S., Connelly J. A. A noise-based IC random number generator for applications in cryptography // IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications. 2000. Vol. 47. № 5. Pp. 615–621.

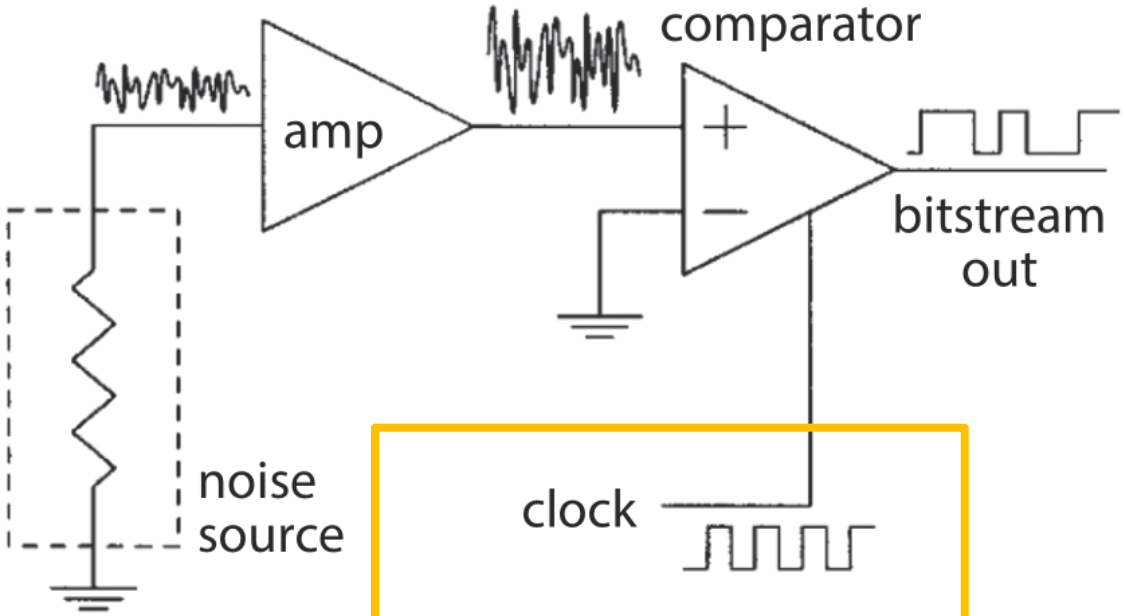
РусКрипто

Схема мгновенных значений



РусКрипто

Схема мгновенных значений

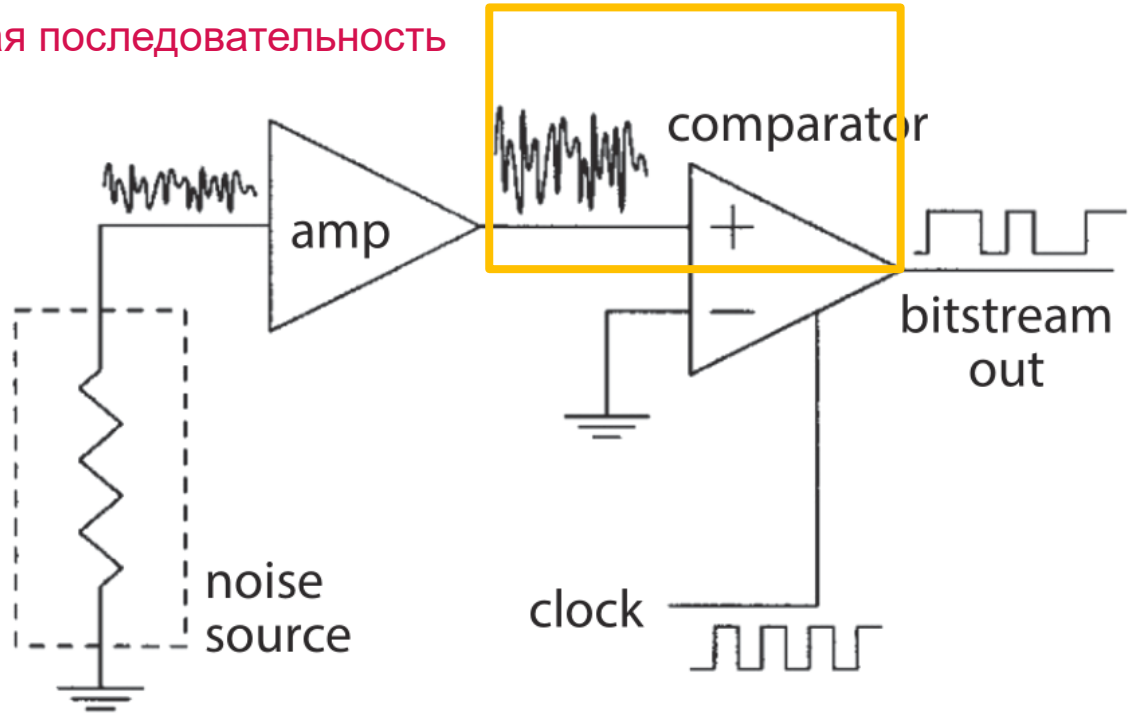


f – частота регистрации сигнала

РусКрипто

Схема мгновенных значений

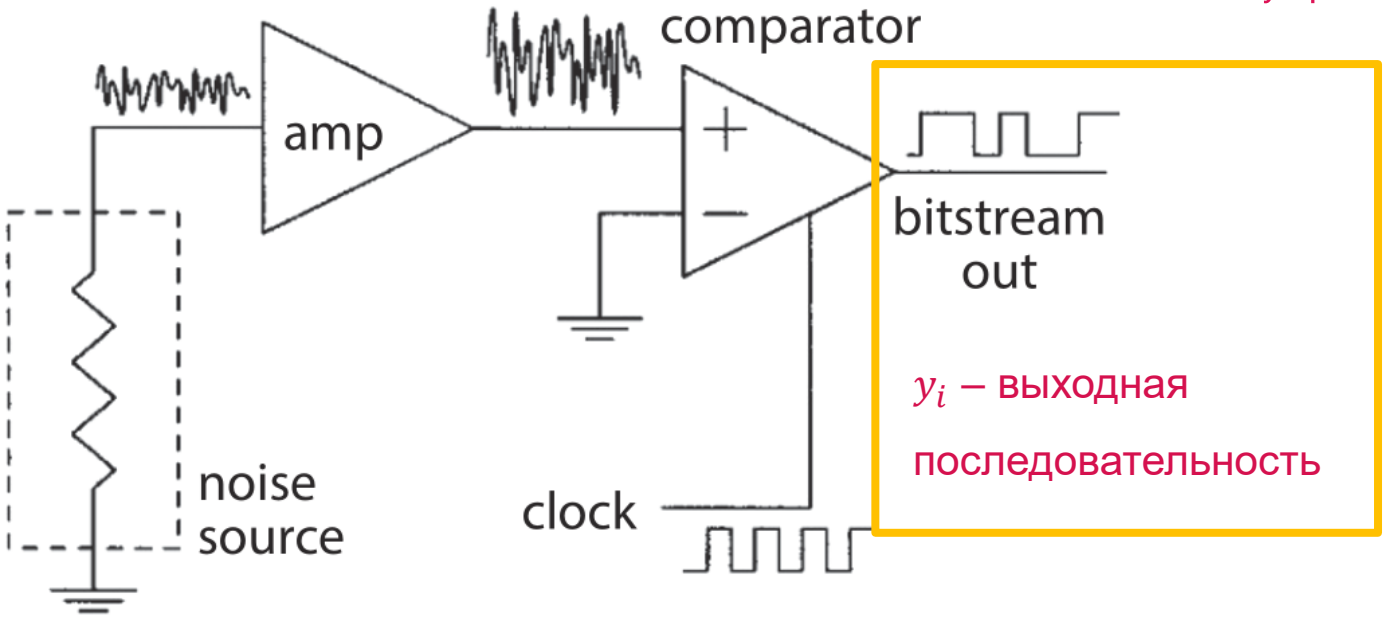
x_i – сырая последовательность



РусКрипто

Схема мгновенных значений

РусКрипто



y_i – выходная последовательность

Схема мгновенных значений

Достоинства

- Простая ТВМ
- Простой вид x_i – сырой последовательности
- Скорость формирования выходной последовательности

РусКрипто

Схема мгновенных значений

РусКрипто

Достоинства

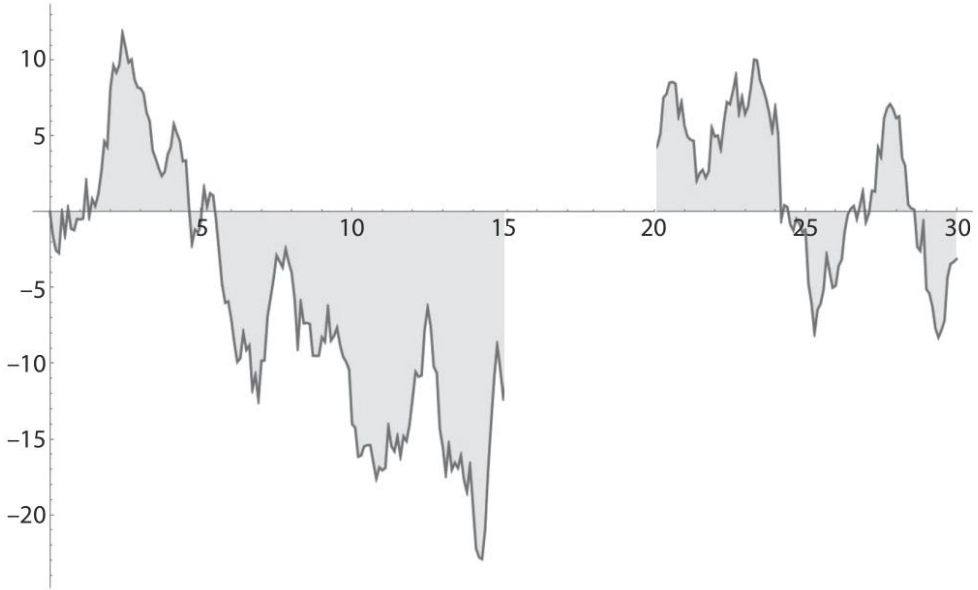
- Простая ТВМ
- Простой вид x_i – сырой последовательности
- Скорость формирования выходной последовательности

Недостатки

- Зависимость значений x_i
- Можем «предсказывать» пропущенное значение

Схема мгновенных значений

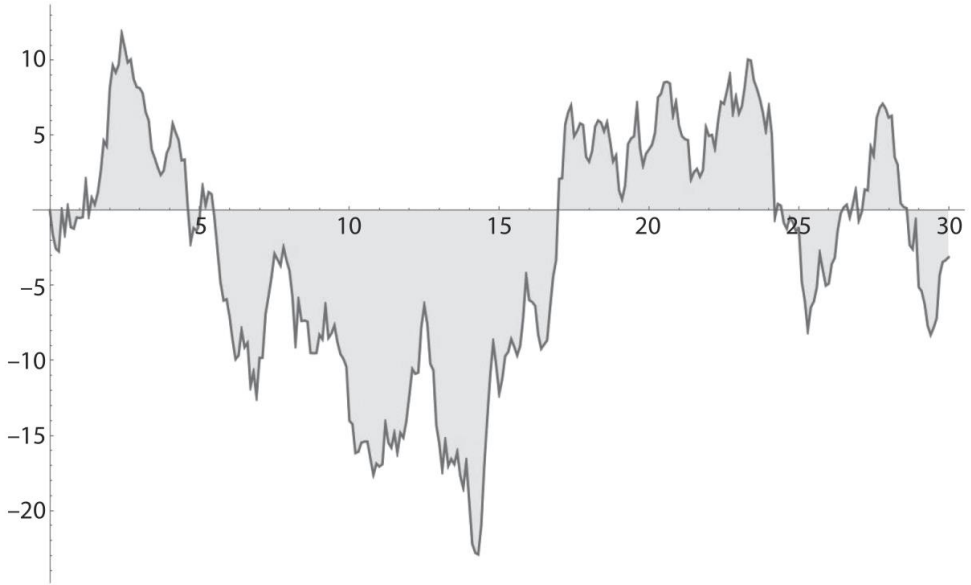
«Предсказывание»



РусКрипто

Схема мгновенных значений

«Предсказывание»



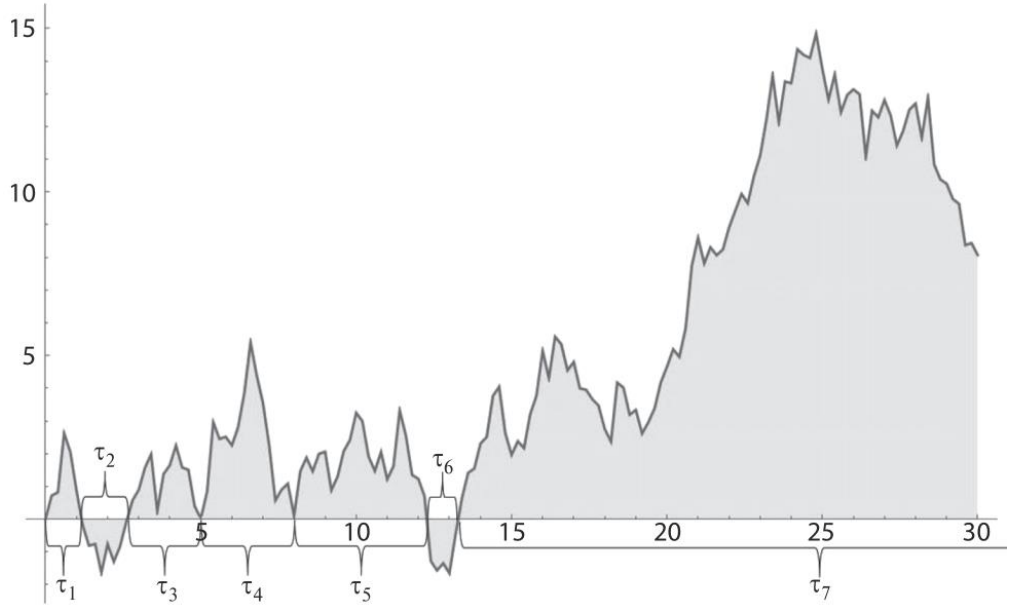
РусКрипто

Чем плохо «предсказывание»?

РусКрипто

- Обычно x_i проще для изучения.
- Умеем «предсказывать» x_i → умеем «предсказывать» y_i.
- Умеем «предсказывать» y_i → совместное распределение **не равновероятное!**

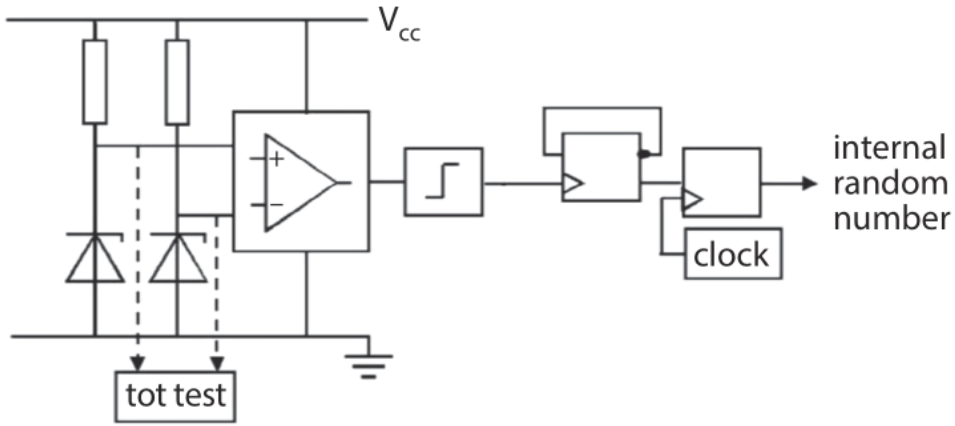
Схема интервалов



- $X_t, t \geq 0$ – случайный процесс
- τ_i – время «блуждания» до *i*-того возвращения в ноль
- $x_1 = \tau_1, \quad x_2 = \tau_2, \quad x_3 = \tau_3, \ldots$ – «сырая» последовательность

РусКрипто

Схема интервалов



[2] Killmann W., Schindler W. A design for a physical RNG with robust entropy estimators. Cryptographic Hardware and Embedded Systems (CHES2008): 10th International Workshop, Washington, DC, USA, August 10–13, 2008. Proceedings 10. Springer Berlin Heidelberg, 2008, pp. 146–163

РусКрипто

Схема интервалов

Два диода

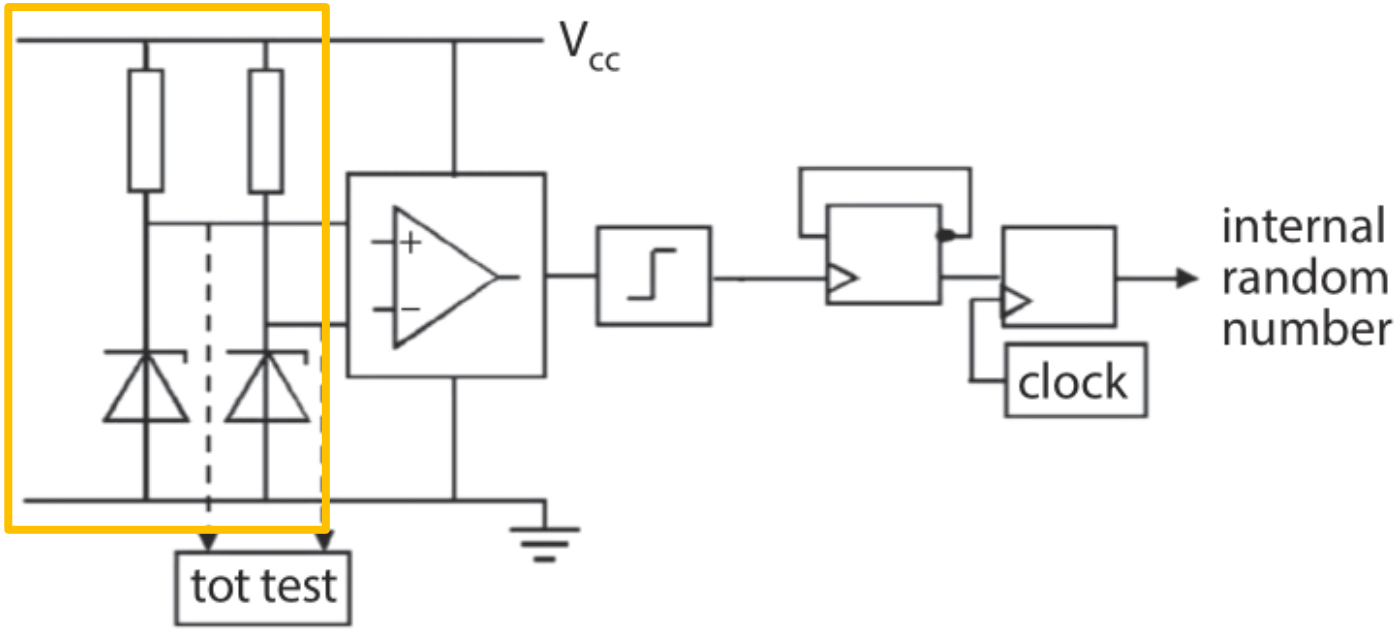
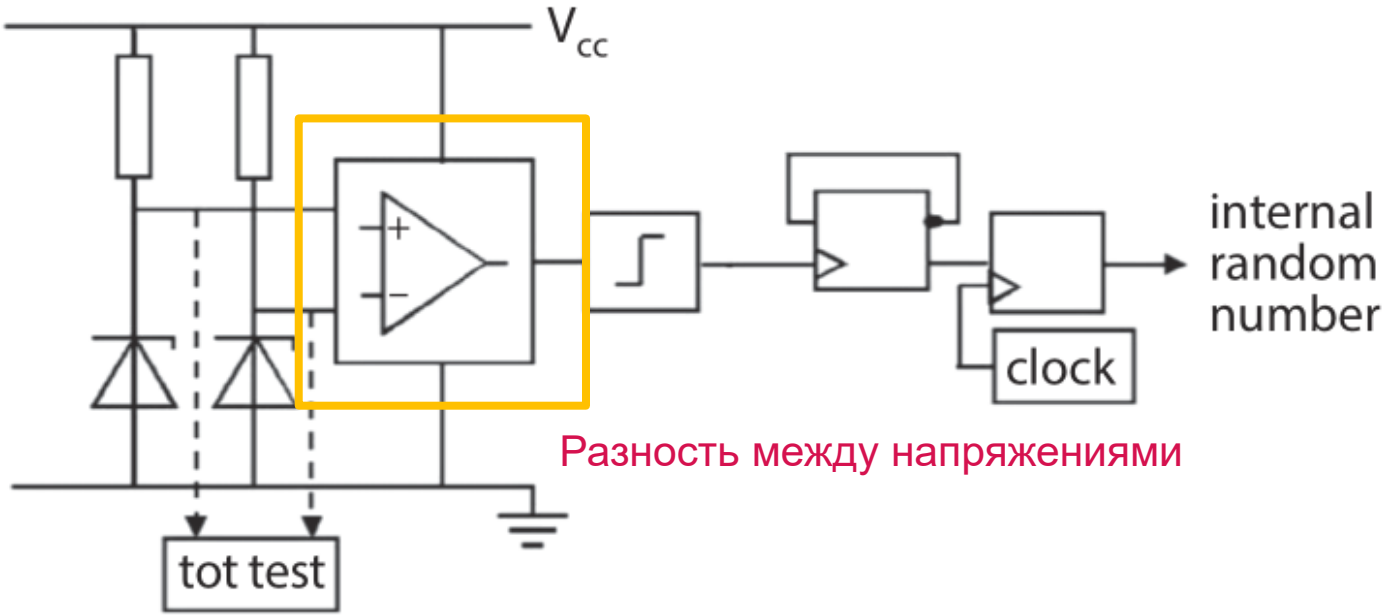
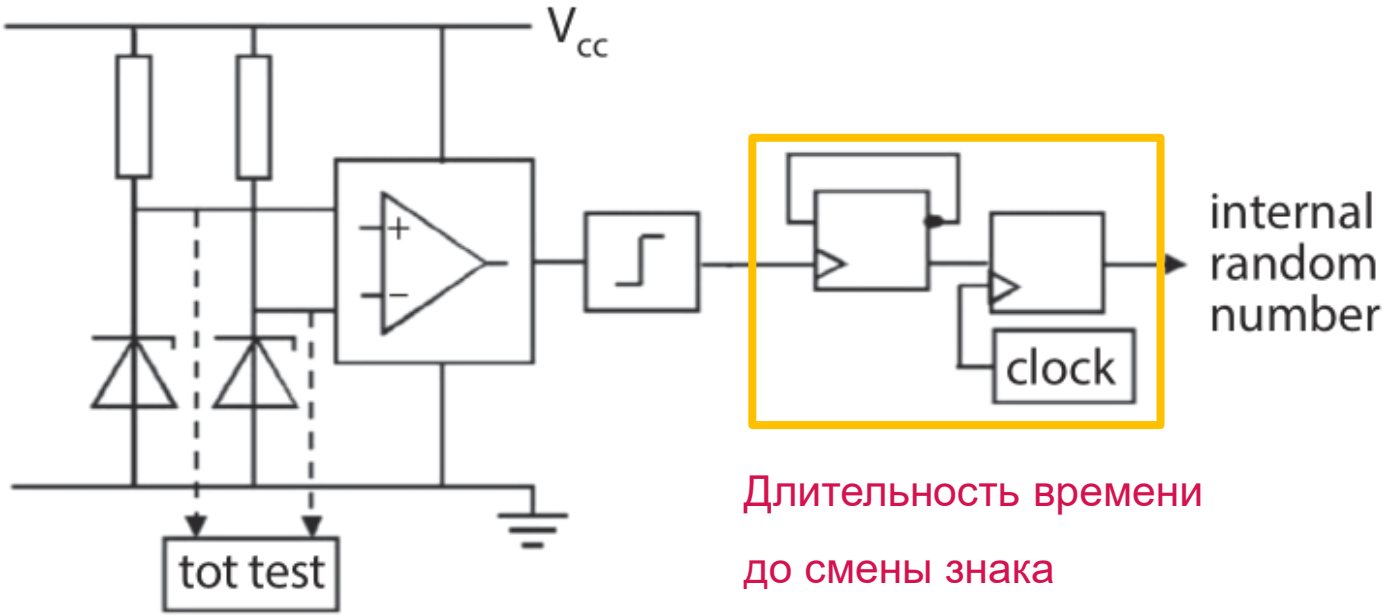


Схема интервалов



Разность между напряжениями

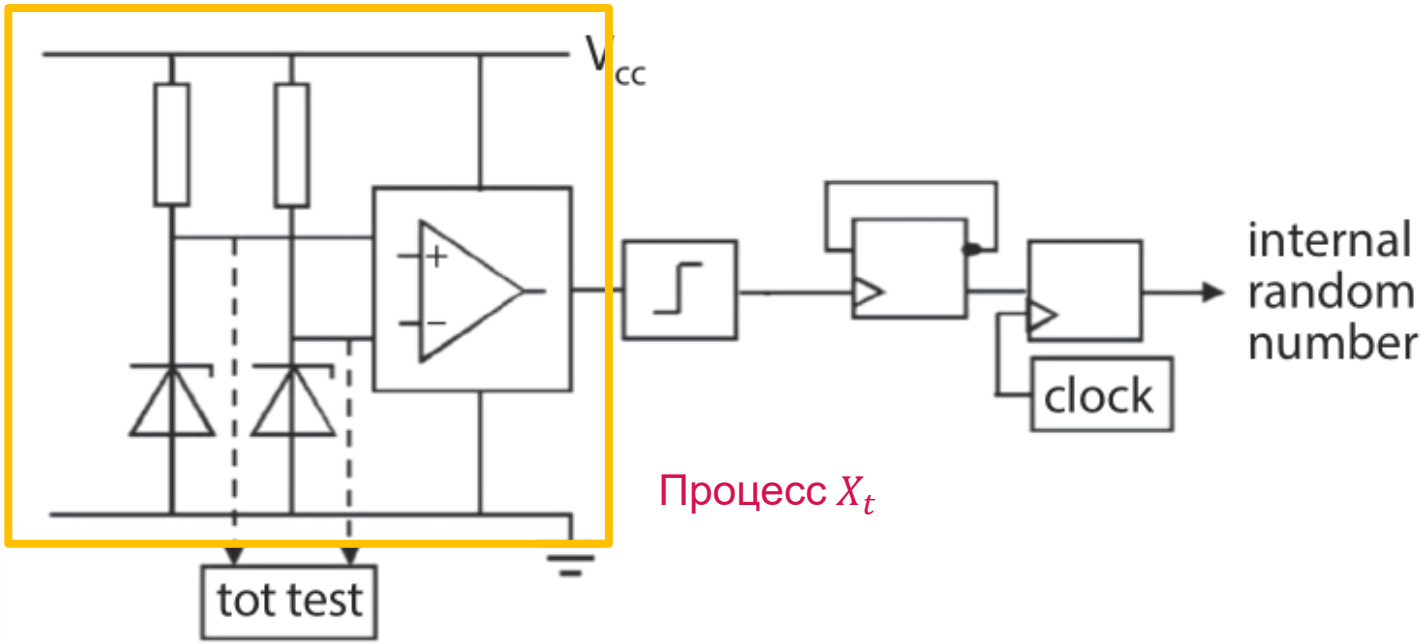
Схема интервалов



Длительность времени

до смены знака

Схема интервалов



Процесс X_t

Схема интервалов

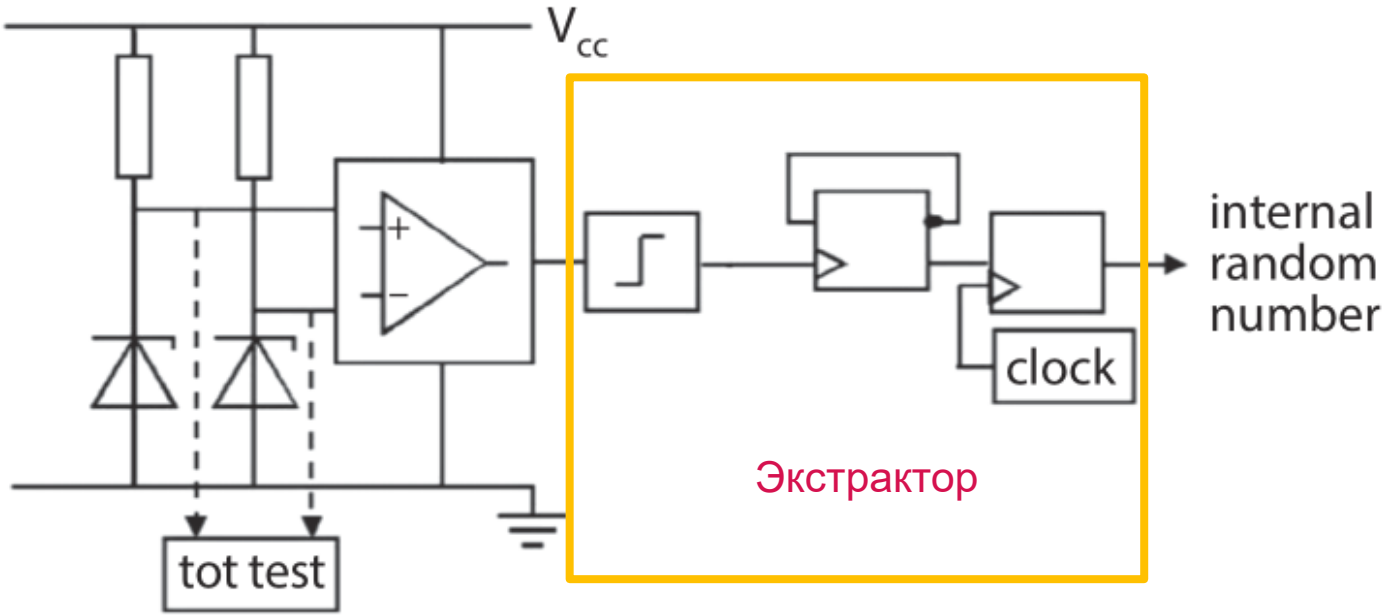
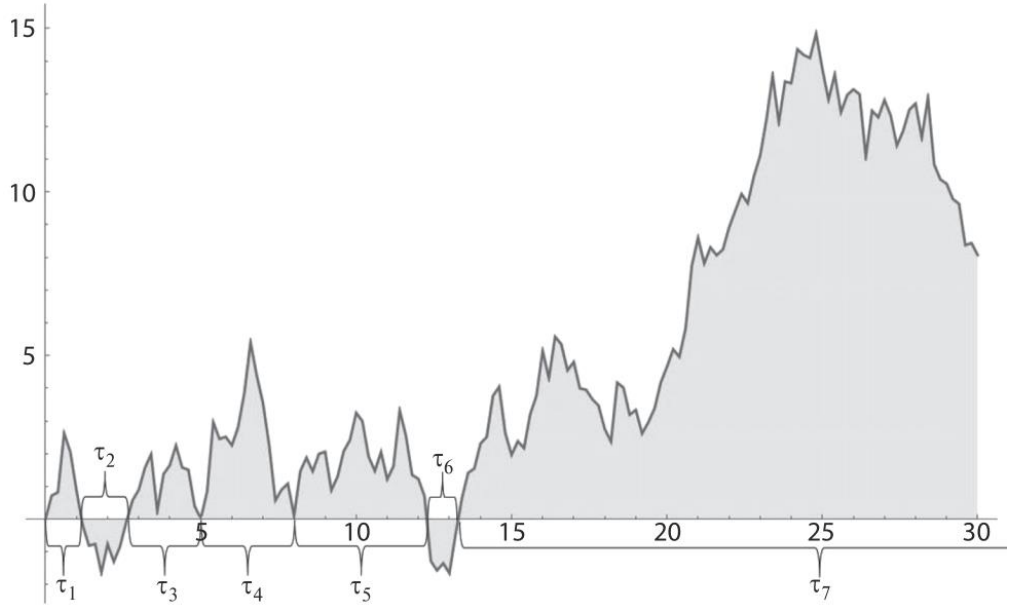


Схема интервалов



- $X_t, t \geq 0$ – разность напряжений
- τ_i – время до возвращения в ноль
- $x_1 = \tau_1, \quad x_2 = \tau_2, \quad x_3 = \tau_3, \ldots$ – «сырая» последовательность

РусКрипто

Схема интервалов

Достоинства

- Можно подобрать «хороший» процесс
- x_i – одинаково распределены
- x_i – независимы

РусКрипто

Схема интервалов

Достоинства

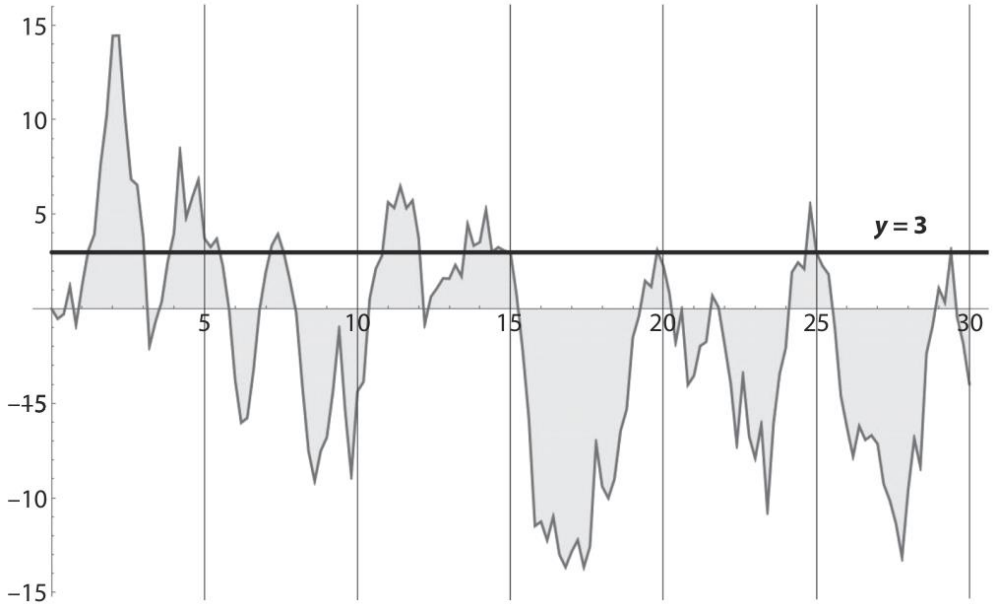
- Можно подобрать «хороший» процесс
- x_i – одинаково распределены
- x_i – независимы

Недостатки

- Дискретность времени может приводить к зависимости и неоднородности
- Время формирования знака – случайная величина

РусКрипто

Схема выбросов



- $X_t, t \geq 0$ – случайный процесс
- ω_j – момент пересечения уровня снизу вверх
- $\mathrm{x}_1 = \#\{\omega_j \in [(i-1)T; iT]\}$– «сырая» последовательность

РусКрипто

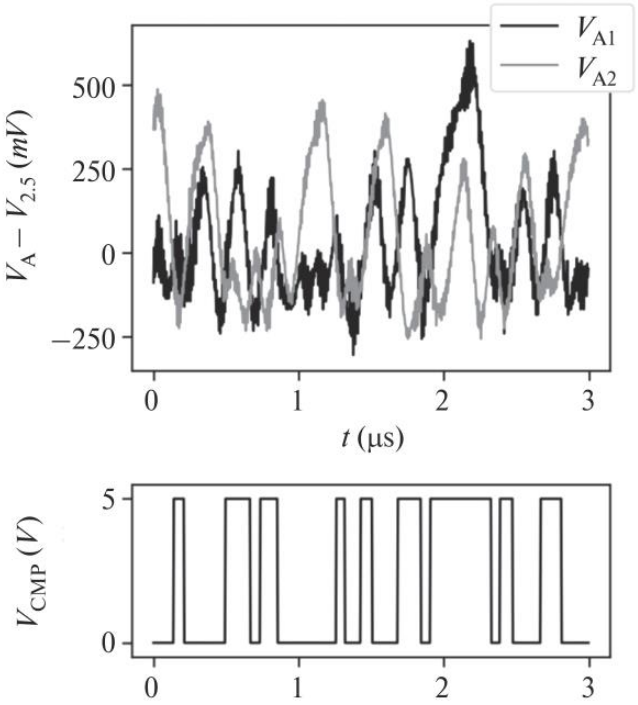
Схема выбросов

РусКрипто

- Два диода
- Измеряется разность напряжений между ними
- ω_j – момент пересечения уровня снизу вверх
- $x_1 = \#\{\omega_j \in [(i-1)T; iT]\}$– «сырая» последовательность

[3] Guerrer G. RAVA: An Open Hardware True Random Number Generator Based on Avalanche Noise. IEEE Access. 2023. Vol. 11, pp. 119568–119583.

Схема выбросов



[3] Guerrer G. RAVA: An Open Hardware True Random Number Generator Based on Avalanche Noise. IEEE Access. 2023. Vol. 11, pp. 119568–119583.

РусКрипто

Схема выбросов

Достоинства

РусКрипто

- Можно подобрать «хороший» процесс
- x_i – стремятся к дискретному гауссовскому распределению [4]

[4] Хименко, В.И. “Выбросы случайных процессов и проблема пересечений уровней”, М.: Техносфера, 2022. 582 с.

Схема выбросов

Достоинства

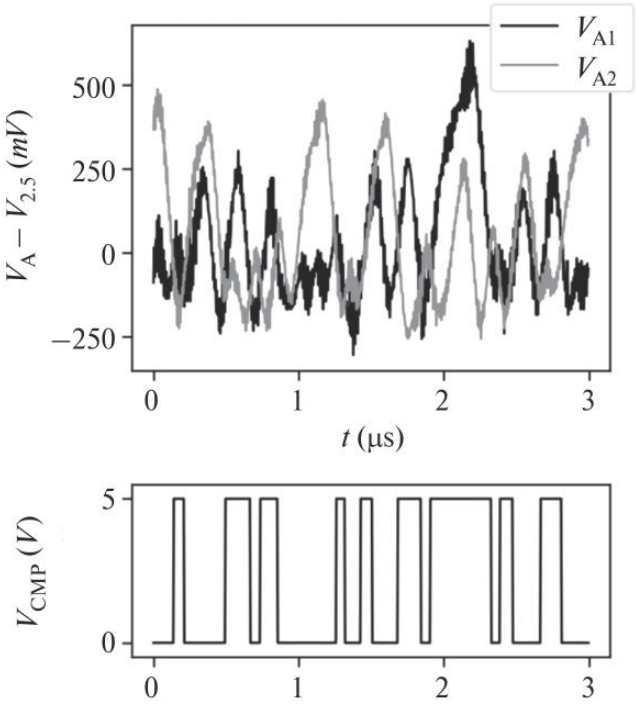
- Можно подобрать «хороший» процесс
- x_i – стремятся к дискретному гауссовскому распределению [4]

Недостатки

- Неоднородность x_i
- Зависимость x_i

РусКрипто

Схема выбросов



[3] Guerrer G. RAVA: An Open Hardware True Random Number Generator Based on Avalanche Noise. IEEE Access. 2023. Vol. 11, pp. 119568–119583.

РусКрипто

Итоги

Три схемы

- Схема мгновенных значений
- Схема интервалов
- Схема выбросов

«Источник» случайности указан в названии схемы

РусКрипто

Итоги

Задачи аналитика

- Построить ТВМ
- Изучить **совместное** распределение y_i (или x_i)

Важное!

- Зависимость или неоднородность $\neq$ плохой ФГСЧ!
- Не учитывать зависимость или неоднородность $=$ плохое ТВО!

РусКрипто

РусКрипто

СПАСИБО
ЗА ВНИМАНИЕ