Теоретико-вероятностные модели ФГСЧ

Богданов Дмитрий Сергеевич

24 сентября 2024 г.

Случайные двоичные последовательности и криптография

Что хотим?

Криптографические ключи

- "Случайные"
- "Непредсказуемые"
- В большом количестве

Как устроен ФДСЧ?

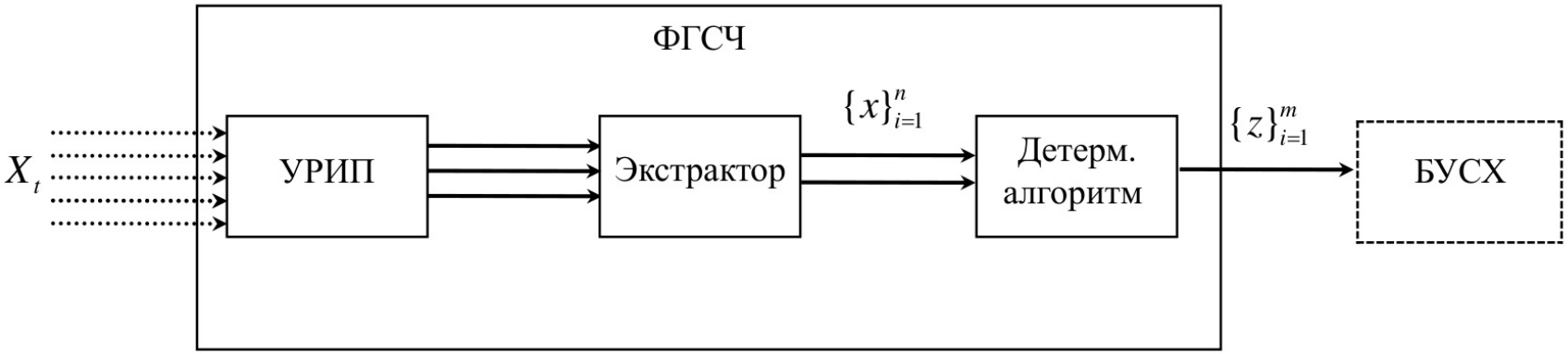


Рис.: Составные элементы ФГСЧ. УРИП - устройство регистрации исходного процесса. БУСХ - блок улучшения статистических характеристик

Примеры исходного физического процесса

- Тепловой шум
- Лавинный пробой p-n перехода
- Лавинный пробой база-эмиттерного перехода биполярного транзистора
- Нестабильность фазы в кольце инверторов
- Вакуумные флуктуации на выходе оптического светоделителя
- Время между приёмом фотонов фотодетектором
- Нестабильность оптического излучения лазера
- Радиоактивный распад
- Нестабильность начальных условий нелинейных динамических систем

Как устроен ФДСЧ?

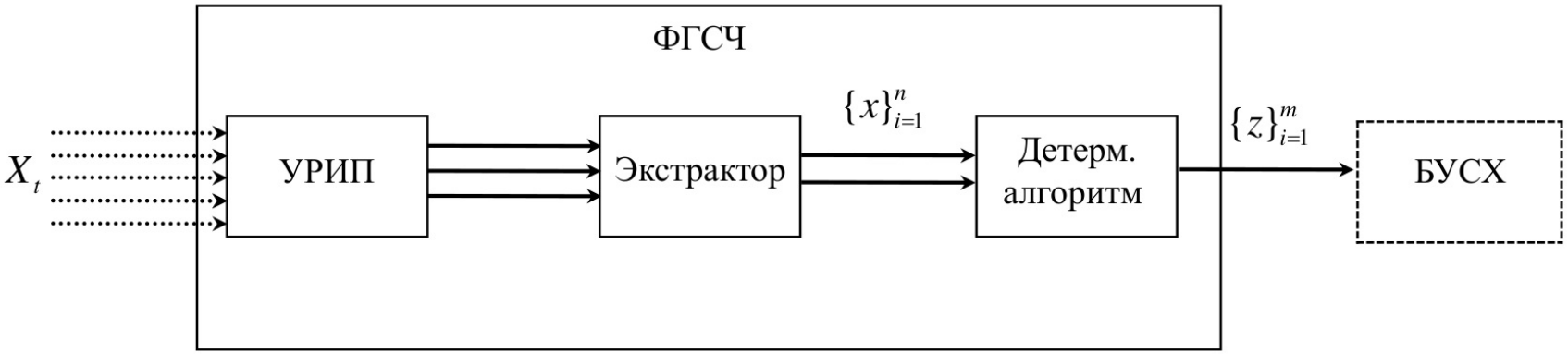


Рис.: Составные элементы ФГСЧ. УРИП - устройство регистрации исходного процесса. БУСХ - блок улучшения статистических характеристик

Способы экстракции случайности из физического процесса

Три способа экстракции

- Схема мгновенных значений
- Схема интервалов
- Схема выбросов

Схема мгновенных значений

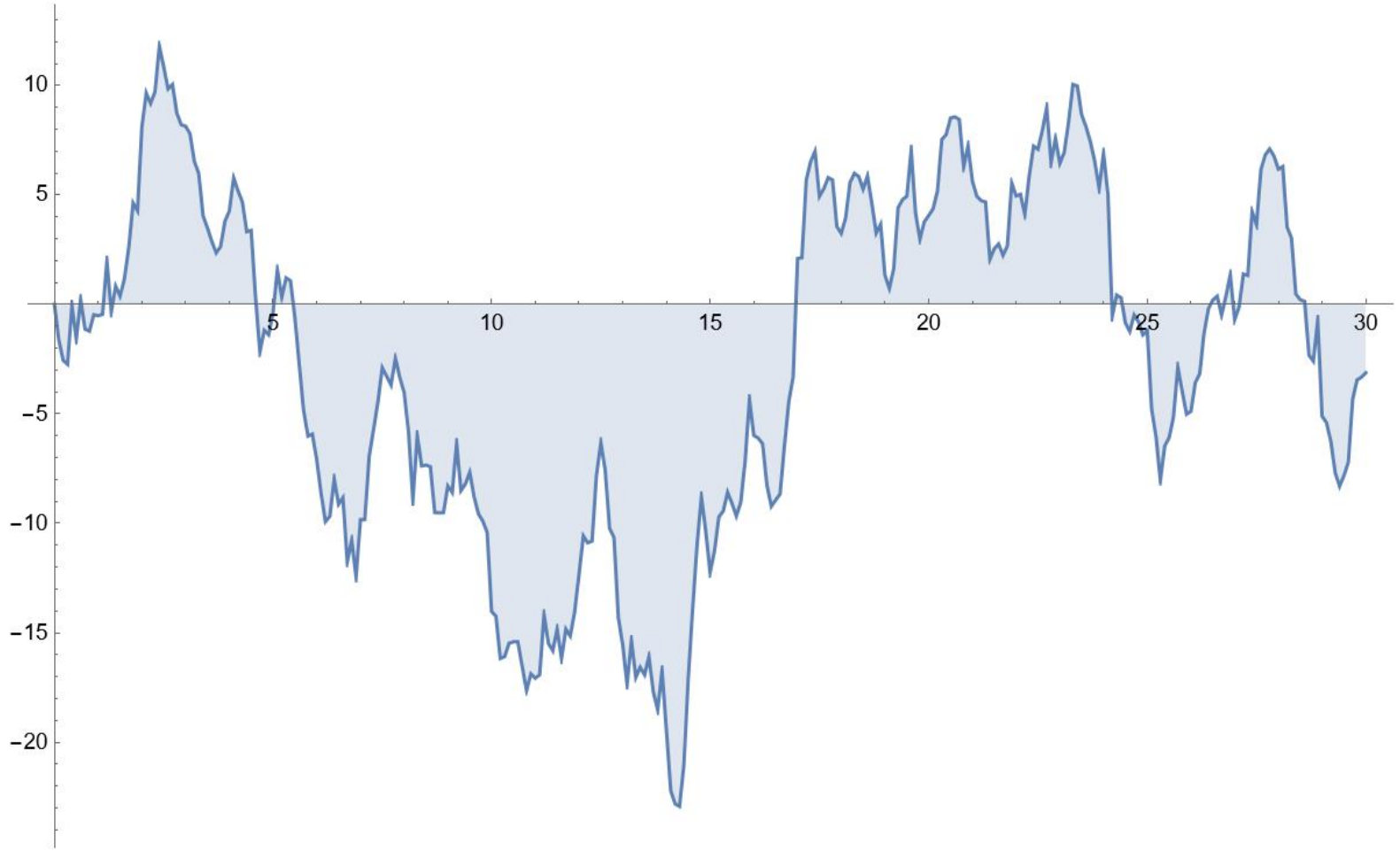
Определение

Пусть X_t, $t \in \mathbb{R}_+$, – случайный процесс, а $f > 0$ – частота его регистрации. Тогда последовательность случайных величин

$$x_1 = X_{\frac{1}{f}}, \; x_2 = X_{\frac{2}{f}}, \; \ldots, \; x_N = X_{\frac{N}{f}}, \ldots$$

называется сырой последовательностью, полученной по схеме мгновенных значений с частотой f регистрации сигнала.

Схема мгновенных значений



Пример "Детерминированного преобразования"после экстракции случайности

Пример

Пусть $x_1, x_2, \ldots$ – сырая последовательность, полученная по схеме мгновенных значений. Тогда выходная последовательность $z_1, z_2, \ldots$ формируется по следующему правилу

$$z_i = [x_i] \pmod 2.$$

Схема мгновенных значений

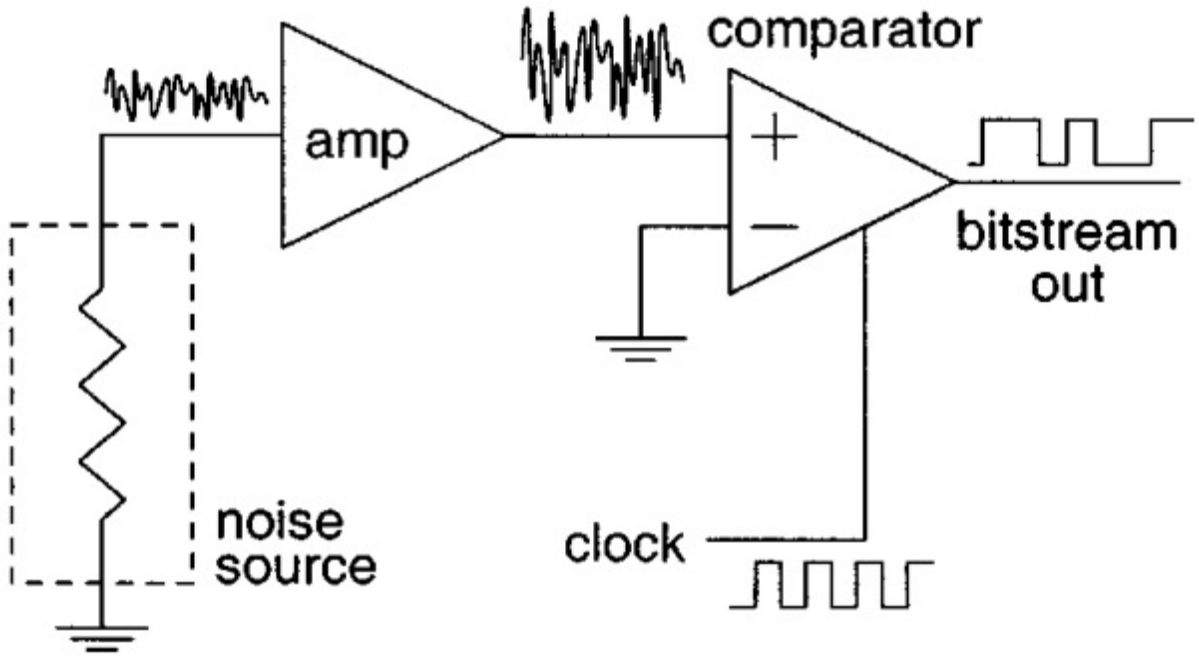


Рис.: Схемотехническое решение ФГСЧ из работы Petrie, Craig S and Connelly, J Alvin "A noise-based IC random number generator for applications in cryptography".

Схема мгновенных значений

Преимущества

- Простота реализации
- Простота описания сырой последовательности

Схема мгновенных значений

Преимущества

- Простота реализации
- Простота описания сырой последовательности

Недостатки

- Статистическая зависимость между членами сырой последовательности

Схема мгновенных значений

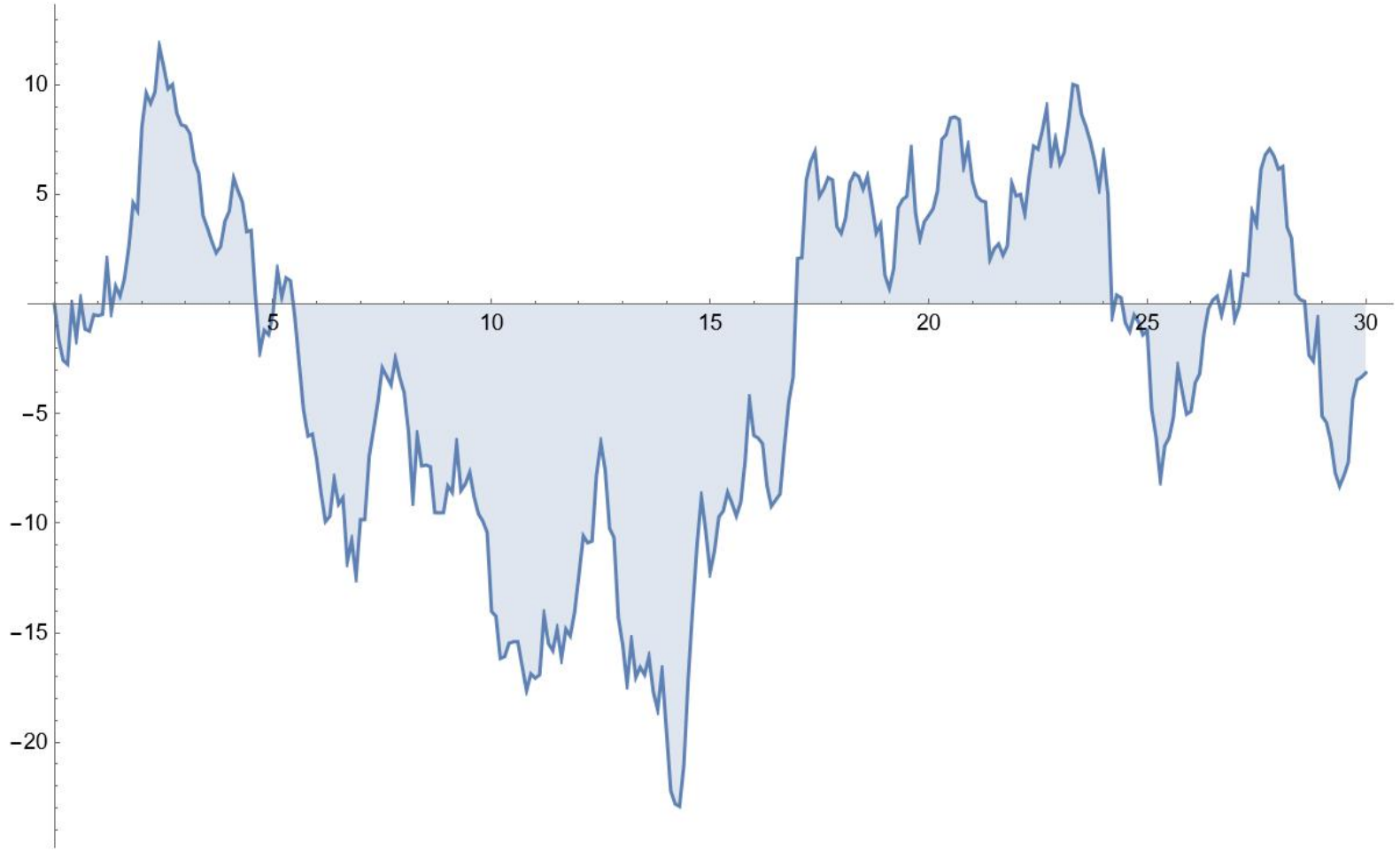


Схема интервалов

Определение

Пусть X_t, $t \in \mathbb{R}_+$, – случайный процесс. Тогда последовательность случайных величин

$$x_1, \; x_2, \; \ldots, \; x_N, \ldots$$

равных **интервалу** времени между регистрациями некоторых случайных событий $A_1, A_2, \ldots$, представляет собой сырую последовательность, полученную по схеме интервалов.

Схема интервалов

Пример

Пусть X_t, $t \in \mathbb{R}_+$, – случайный процесс. Через $\sigma_1 = \inf\{t > 0 : X_t = 0\}$ обозначим первый момент возвращения траектории процесса X_t в ноль, а через $\sigma_i = \inf\{t > \sigma_{i-1} : X_t = 0\}$, $i > 1$, $i \in \mathbb{N}$ – i-тый момент возвращения.

Тогда последовательность

$$x_1 = \sigma_1,\ x_2 = \sigma_2 - \sigma_1,\ \ldots,\ x_i = \sigma_i - \sigma_{i-1}, \ldots$$

редставляет собой сырую последовательность, полученную по "схеме интервалов".

Схема интервалов

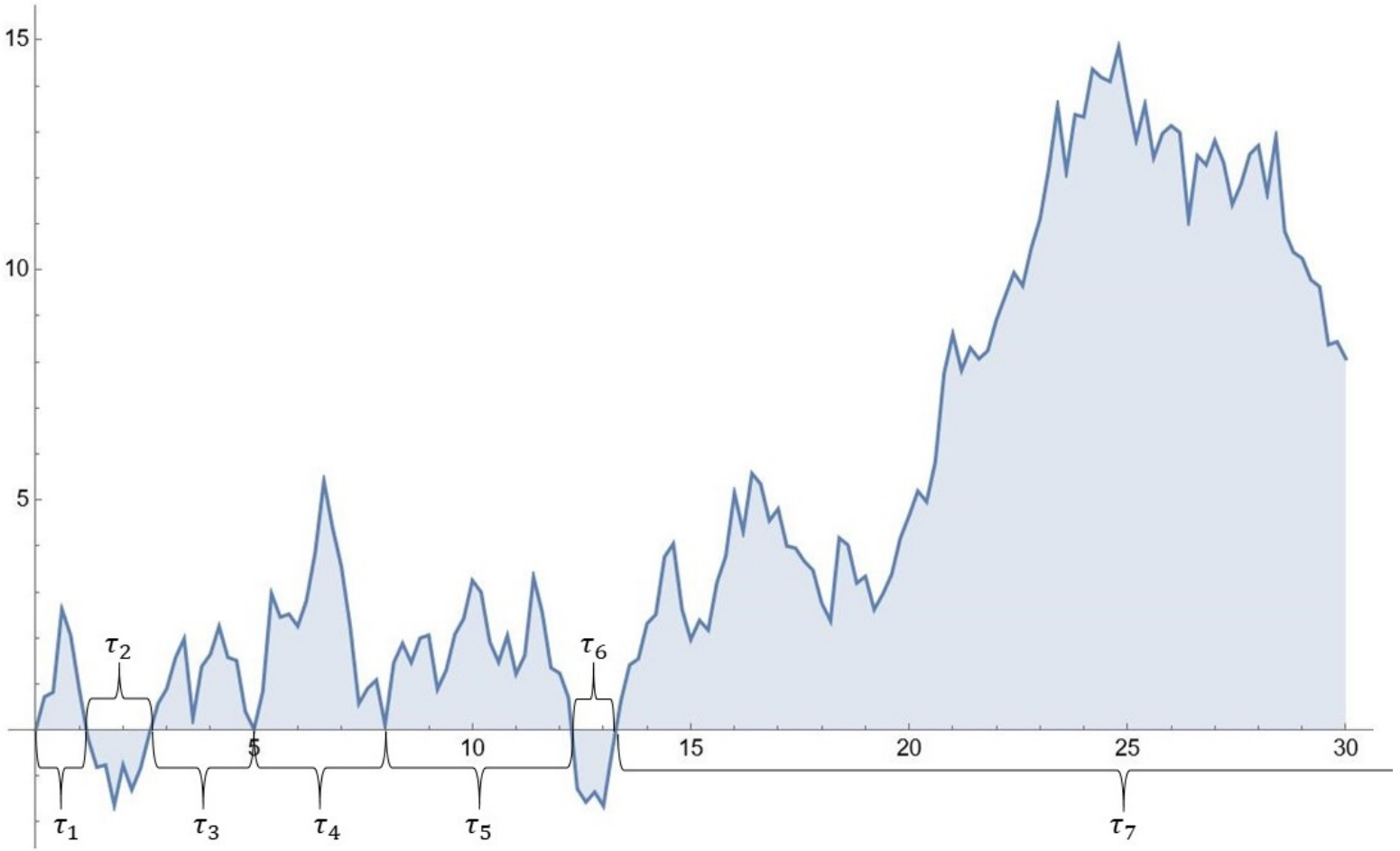


Схема интервалов

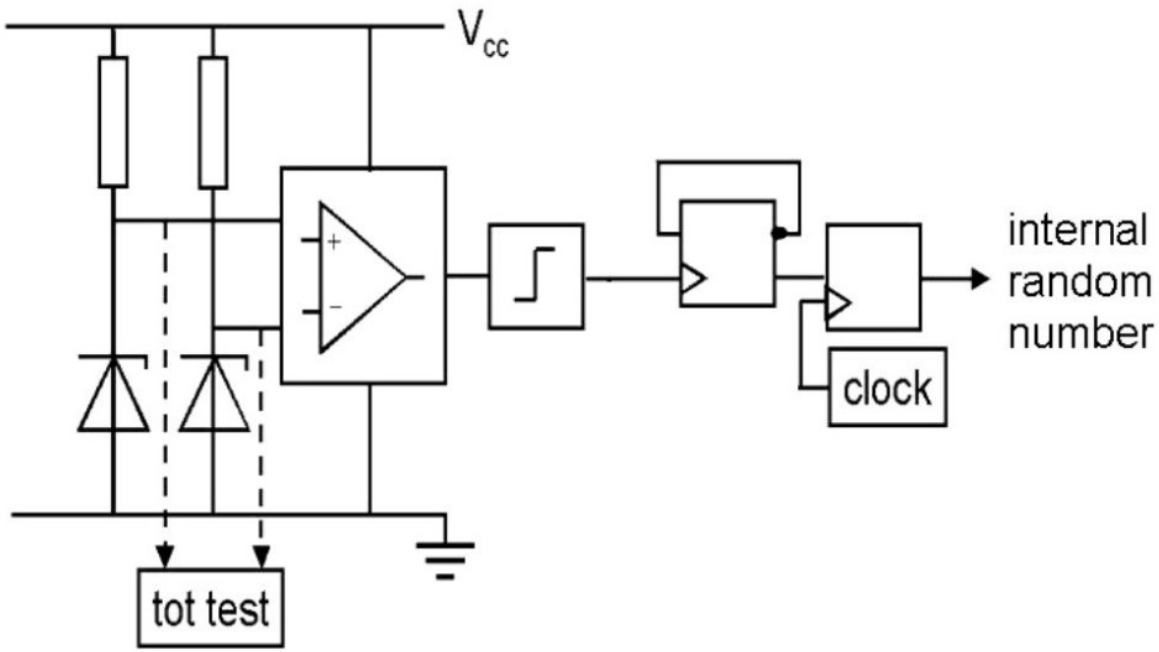


Рис.: Схемотехническое решение ФГСЧ из работы Killmann, W., Schindler, W. "A Design for a Physical RNG with Robust Entropy Estimators".

Схема интервалов

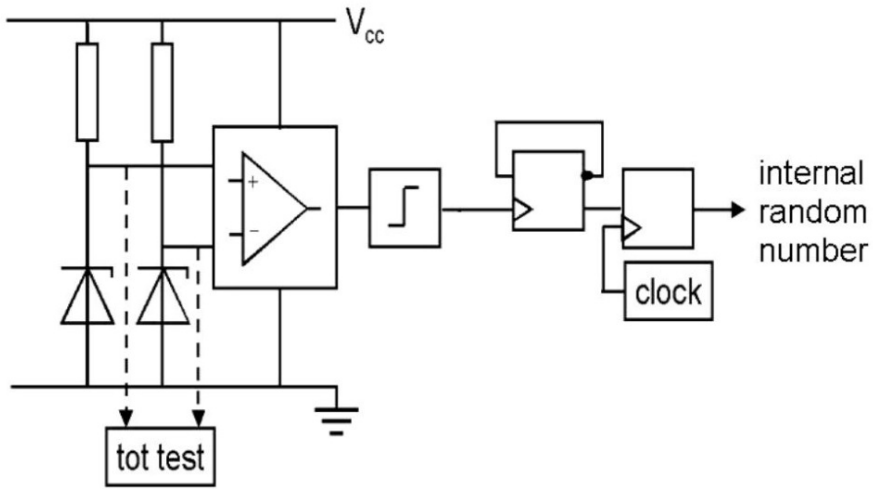


Рис.: На пару диодов подается обратное напряжение, и измеряется разность напряжений на их выходах. За счет лавинного пробоя p-n перехода в случайный момент времени напряжение на одном из диодов падает до нуля. Сырая последовательность – длительность интервала времени в которые разность напряжений на выходах диодов больше нуля.

Схема интервалов

Преимущества

- Можно "удачно"подобрать случайные события

Схема интервалов

Преимущества

- Можно "удачно"подобрать случайные события

Недостатки

- Время формирования очередного элемента сырой последовательности не детерминировано и является случайной величиной

Схема выбросов

Определение

Пусть X_t, $t \in \mathbb{R}_+$, – случайный процесс. Тогда последовательность случайных величин

$$x_1, \; x_2, \; \ldots, \; x_N, \ldots$$

равных **количеству** случайных событий $A_1, A_2, \ldots$, произошедших за фиксированный интервал времени, представляет собой сырую последовательность, полученную по схеме выбросов.

Схема выбросов

Пример

Пусть X_t, $t \in \mathbb{R}_+$, – случайный процесс и $\omega_1, \omega_2, \ldots$ последовательность интервалов, на которых $X_t \geq r$, где $r > 0$. Тогда последовательность

$$x_i = \#\left\{\omega_j \in [(i-1)\,T; iT]\right\},$$

где $T > 0$, представляет собой сырую последовательность, полученную по "схеме выбросов".

Схема выбросов

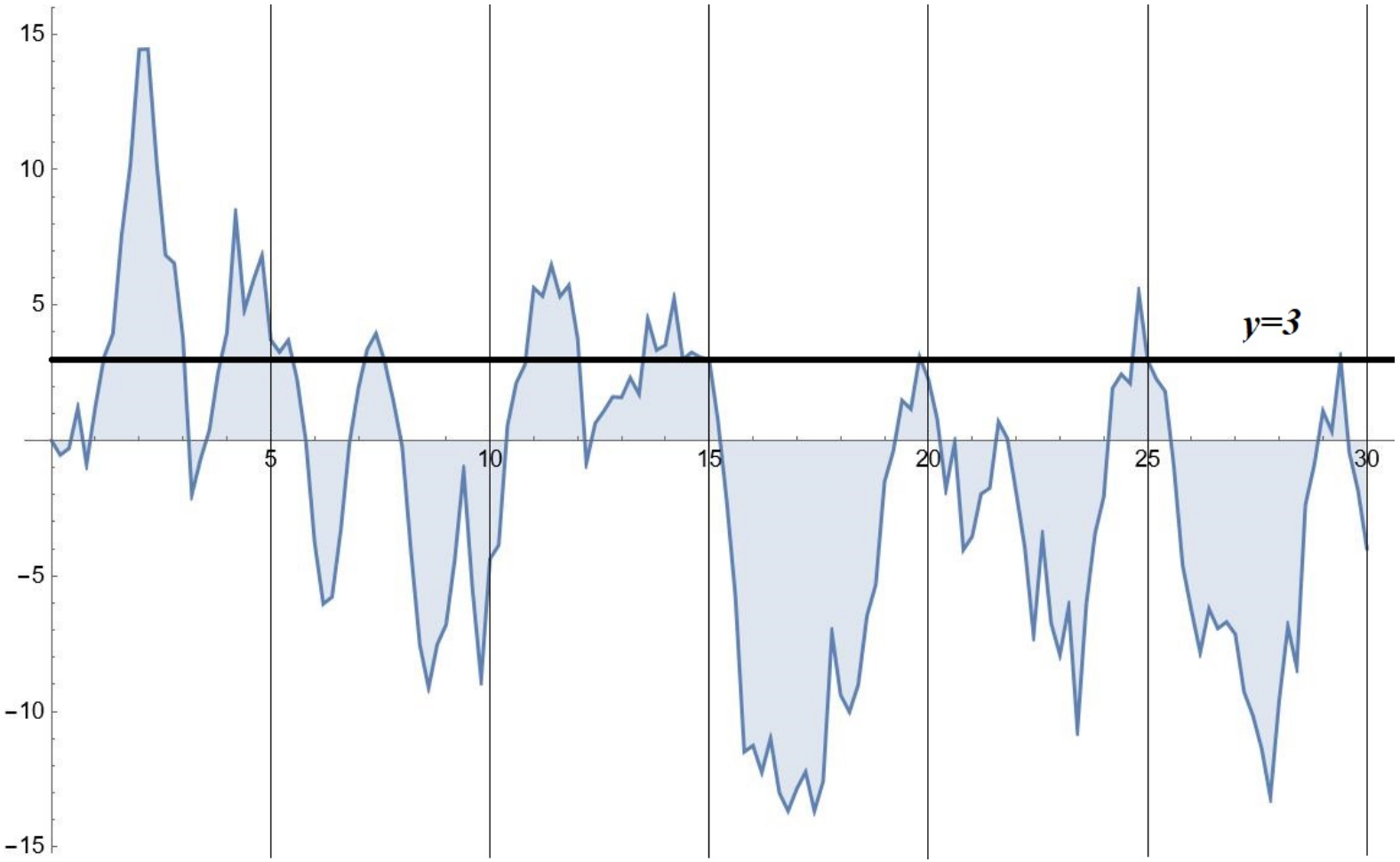


Схема выбросов

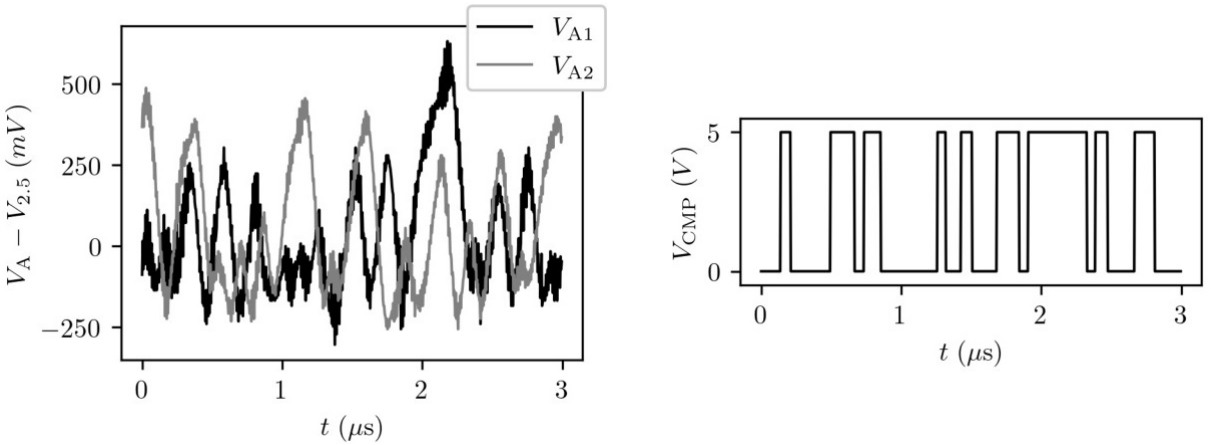


Рис.: Напряжение на выходах диодов и разность напряжений в ФГСЧ из работы Guerrer, G. "RAVA: An Open Hardware True Random Number Generator Based on Avalanche Noise".

Схема выбросов

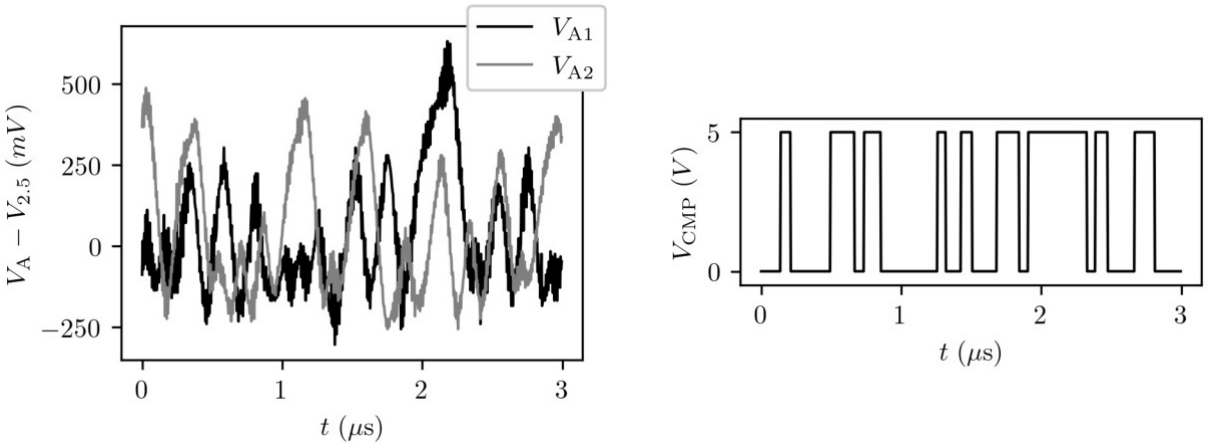


Рис.: На пару диодов подается обратное напряжение и измеряется разность напряжений на их выходах. Далее подсчитывается количество переходов через ноль значений разности напряжений за фиксированный интервал времени $T > 0$. Полученные значения образуют сырую последовательность.

Схема выбросов

Преимущества

- Фиксированное время генерации очередного элемента

Схема выбросов

Преимущества

- Фиксированное время генерации очередного элемента

Недостатки

- Сравнительное сложное теоретико-вероятностное обоснование

БУСХ

Примеры БУСХ

- Алгоритм фон Неймана
- Алгоритм Бабкина (Элайеса)
- Сложение по модулю

БУСХ

Примеры БУСХ

- Алгоритм фон Неймана
- Алгоритм Бабкина (Элайеса)
- Сложение по модулю

Вопрос

Применимы ли они?

Что нужно учитывать при анализе?

- Ограниченностью точности электронных компонент ФГСЧ
- Зависимостью характеристик ФГСЧ от внешних факторов (температуры, влажности, давления и т. д.)
- Анализ совместного распределения случайных величин $z_1, z_2, \ldots$

Идеала не достичь...

... но это и не страшно!

- Арбеков, И.М. "Нижние оценки для практической секретности ключа"
- Логачев А. С., Миронкин В. О. "О влиянии вероятностных характеристик дискретных источников, формирующих криптографические ключи, на практическую секретность ключа"