

Генерация случайных чисел на основе кольцевых осцилляторов: реальность и модель

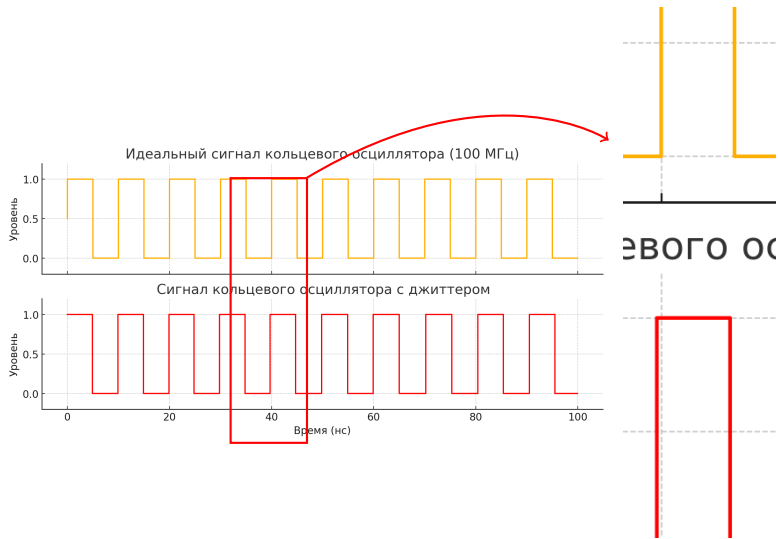
Дмитрий Бобровский, Илья Недомолкин

Код Безопасности

CTCrypt Ramp session, 2025

- Современные IoT-устройства, защищённые микроконтроллеры и смарт-карты требуют компактных и энергоэффективных ФДСЧ.
- Кольцевой осциллятор (КО) — генератор на нечётном числе инверторов, генерирующий прямоугольные импульсы.
- ФДСЧ на КО — перспективный источник энтропии, реализуемый в ПЛИС, ASIC и смарт-картах.
- Основная проблема — мало исследований и отсутствие практических рекомендаций по надёжной реализации.

Ожидание vs Реальность



Идеальный сигнал и реальный сигнал с джиттером.

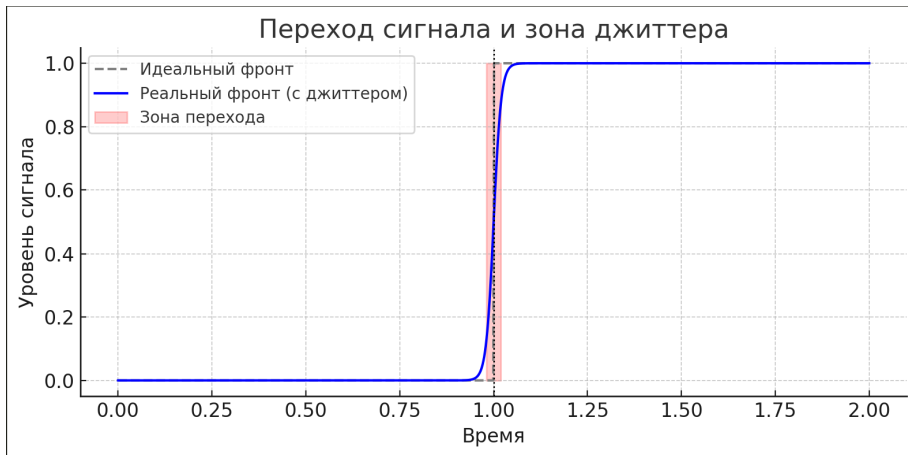
Источник энтропии — джиттер

- Джиттер — случайные временные отклонения фронтов и спадов сигнала.
- Причины: шум питания, нестабильность порогов, электромагнитные помехи.
- Джиттер всегда есть и может служить полезным источником случайности.

“It is important to understand that jitter can never be zero, but it can be mitigated and reduced.” — Microchip Technology Inc.

AN5823 Understanding and Managing Jitter in an Application

Зона перехода сигнала с джиттером



Джиттер расширяет зону перехода сигнала во времени.

Sunar B., Martin W. J., Stinson D. R. *A provably secure true random number generator with built-in tolerance to active attacks*. IEEE Trans. Comput., 2006, 56(1), 109–119.

- Постулируется, что моменты времени, когда сигнал меняет своё значение в зоне перехода, имеют нормальное распределение.
- Гипотетически можно построить ФДСЧ с использованием одного кольца, если дискретизация попадает в зону перехода сигнала.
- Реальность: невозможно синхронизировать сигнал кольца и источника дискретизации; малые размеры зон перехода.

Основная идея: Объединённый сигнал содержит зоны перехода всех колец, что повышает вероятность попадания сигнала дискретизации в зону перехода с высокой энтропией.

- Определён порог между 0 и 1 в зоне перехода — значение при дискретизации в промежутке неопределённо (*Digital Design* M. Mano).
- Зоны перехода колец равномерно распределены по фазе — не учитывается phase interlock (Yoo et al., 2010).
- Параметры колец и джиттера считаются одинаковыми и неизменными для всех колец — из-за размещения и задержек они могут различаться. (Wold K., Tan C. H. 2009).
- Период кольца считается стабильным во времени (*Principles of CMOS VLSI Design* Neil H.E. Weste).

- Классические модели генерации случайных чисел на кольцевых осцилляторах требуют пересмотра с учётом реальных факторов: фазовых сдвигов, асимметрии и неустойчивости.
- Мы открыты к обсуждениям и готовы к научному сотрудничеству!

Спасибо за внимание!

Почему джиттер возникает в ПЛИС

- В идеале: ПЛИС — детерминированная система с фиксированными задержками.
- На практике — аналоговые эффекты и шумы влияют на задержки.
- Время задержки прохождения сигнала:

$$t_{pd} = t_{nom} + \Delta t_{env} + \Delta t_{noise}$$

где Δt_{env} — влияние среды, Δt_{noise} — случайные шумы.