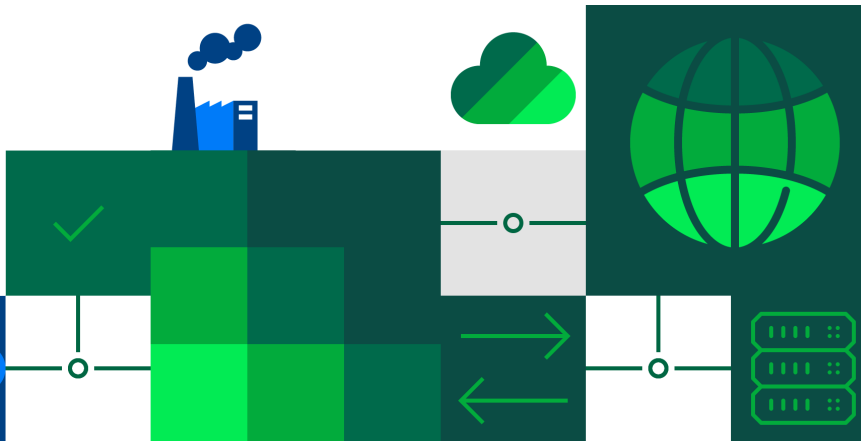




Построение теоретико-вероятностной модели для физического датчика случайных чисел на базе кольцевых осцилляторов

Недомолкин И.Э.
Бобровский Д.А.
Задорожный Д.И.



Физический датчик случайных чисел (ФДСЧ)¹ – датчик, вырабатывающий случайную последовательность путём преобразования сигнала случайного процесса, генерируемого недетерминированной физической системой, устойчивой по отношению к реально возможным изменениям внешних условий и своих параметров.

Программируемая логическая интегральная схема (ПЛИС) – электронный компонент, используемый для создания цифровых интегральных схем, логика работы которого не определяется при изготовлении, а задаётся посредством программирования (проектирования).

¹Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Кольцевой осциллятор – это последовательность из нечетного числа инверторов, где выход последнего соединён со входом первого.

Инвертор – это логический элемент, реализующий операцию логического отрицания.

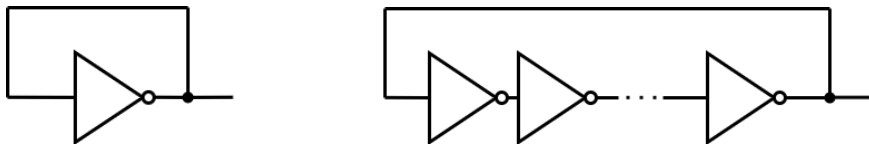


Рисунок 1 – Кольцевой осциллятор состоящий из одного инвертора (слева) и множества инверторов (справа).

Таблица поиска – это структура данных, в которой хранятся результаты вычисления функции по дискретному набору её значений.

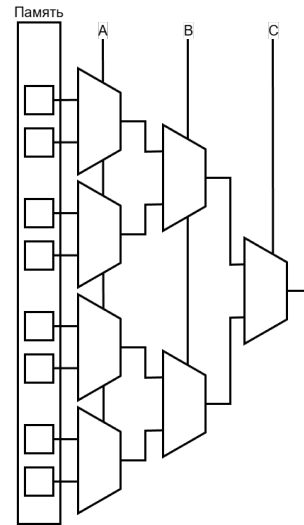
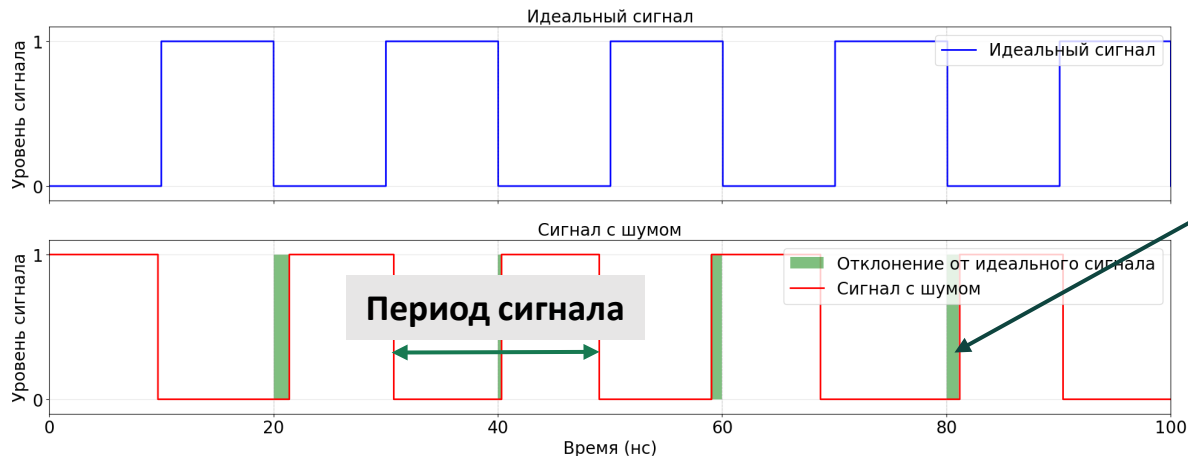


Рисунок 2 – Таблица поиска с тремя входами.



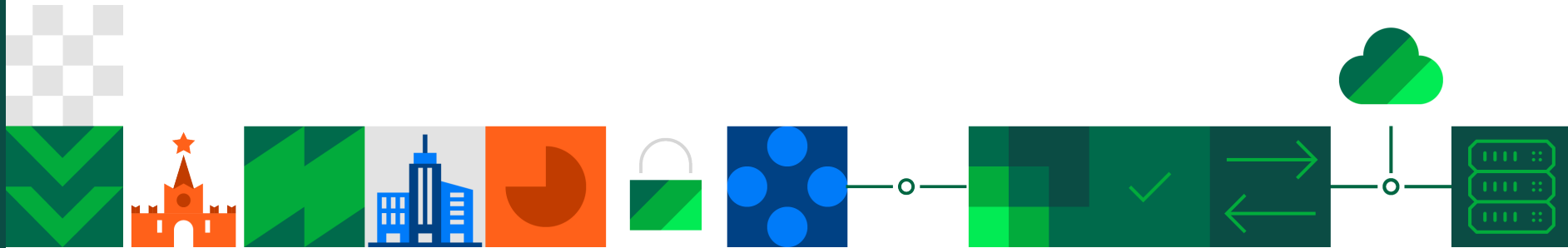
Из-за случайных задержек элементов физической цепи, сигнал на входе кольцевого осциллятора будет отличаться от идеального.

Фронт сигнала – переход цифрового сигнала из состояния «ноль» в состояние «единица».

Период сигнала – время между двумя соседними фронтами.

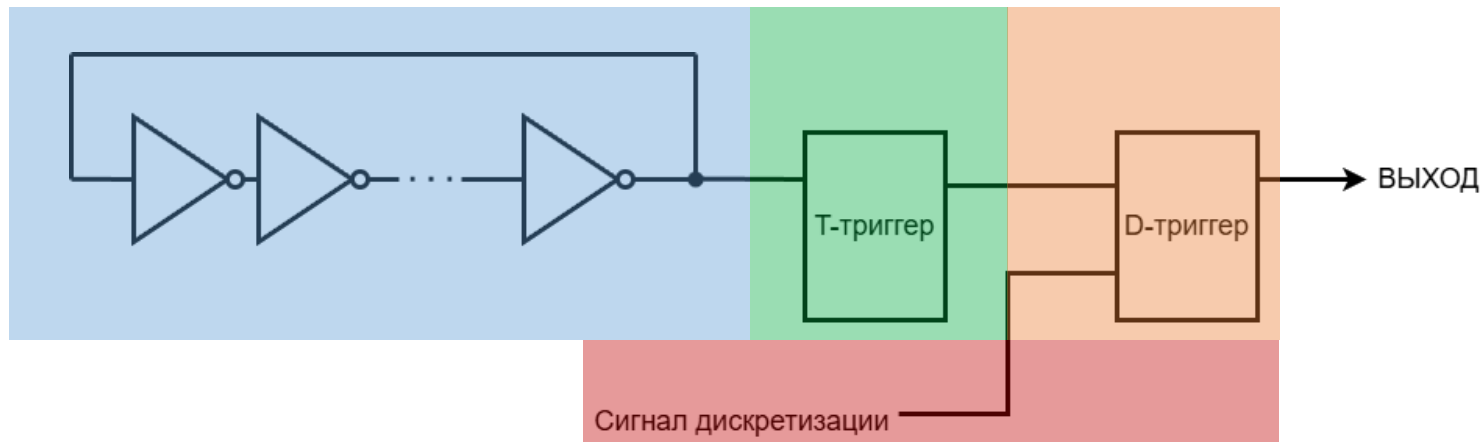


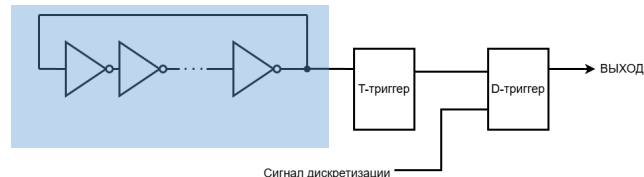
Устройство датчика



Состав датчика:

- ❖ Кольцевой осциллятор (источник случайности)
- ❖ Т-триггер (счетчик фронтов по модулю 2)
- ❖ D-триггер (считывает текущее значение Т-триггера)
- ❖ Источник сигнала дискретизации (задаёт частоту считывания значений с Т-триггера)





Пусть

$$T_1, T_2, T_3, \dots$$

- независимые одинаково распределенные случайные величины имеющие нормальное распределение

$$T_i \sim N(\mu, \sigma^2),$$

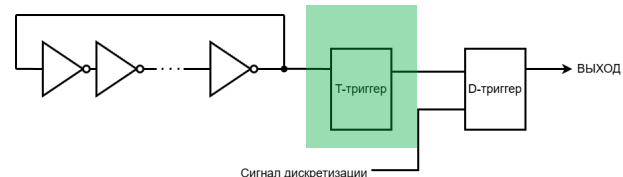
где T_i время между $i - 1$ и i фронтом сигнала кольцевого осциллятора.

Обозначим как $S_n = \sum_{i=1}^n T_n$ время возникновения n -ого фронта. Последовательность $\{S_n\}$ является процессом восстановления, в котором момент восстановления это регистрация фронта сигнала.

Также обозначим число моментов восстановления за время t как N_t . При больших t величина N_t имеет приближенно нормально распределение¹:

$$N_t \sim N(t\mu^{-1}, t\sigma^2\mu^{-3})$$

¹Феллер В. Введение в теорию вероятностей и её приложения. – Рипол Классик, 2013

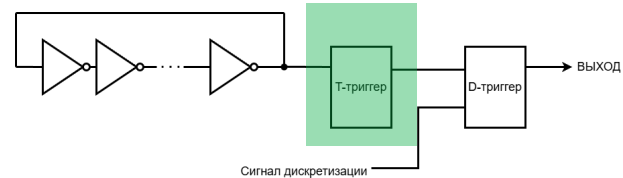


T-триггер можно моделировать как счетчик числа фронтов по модулю 2.

Зная распределение числа фронтов и частоту сигнала дискретизации можно вычислить параметры распределения значений выхода схемы, а также отклонение этих значений от равномерного распределения.

Пусть ξ случайная величина имеет нормальное распределение $\xi \sim N(m, d^2)$

- ❖ $P([\xi] \bmod 2 = 0)$ вероятность считать 0 с выхода схемы
- ❖ $|P([\xi] \bmod 2 = 0) - 0,5|$ отклонение распределения выхода схемы от равномерного распределения



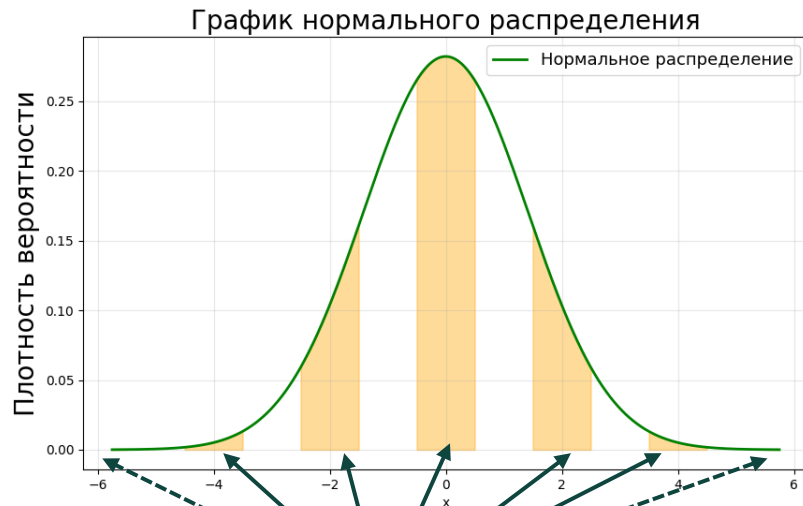
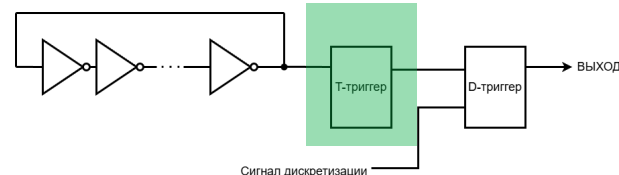
Отклонение значений выхода Т-триггера от равномерного распределение может быть вычислена как

$$|P([\xi] \bmod 2 = 0) - 0,5|$$

где $\xi \sim N(m, d^2)$ случайная величина имеющая нормально распределение.



Вероятность $P([\xi] \bmod 2 = 0)$ представляет из себя сумму площадей в отмеченных **оранжевым** областях.

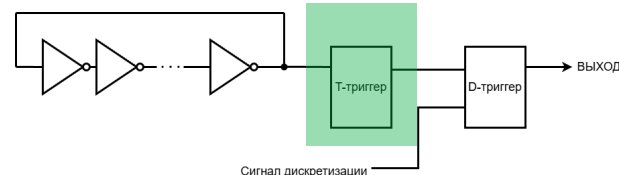


Вычисляем сумму значений плотности вероятности в этих областях и вычитаем 0,5

$$\begin{aligned} & \sum_{n=-\infty}^{+\infty} \left(\Phi \left(\frac{2n + 0,5 - m}{d} \right) - \Phi \left(\frac{2n - 0,5 - m}{d} \right) \right) \\ &= \frac{1}{2} \sum_{n=-\infty}^{+\infty} \left(\operatorname{erf} \left(\frac{2n + 0,5 - m}{\sqrt{2}d^2} \right) - \operatorname{erf} \left(\frac{2n - 0,5 - m}{\sqrt{2}d^2} \right) \right) \\ &= \frac{1}{2} \sum_{n=-\infty}^{\infty} \frac{2}{\sqrt{\pi}} \int_{\frac{2n-m}{\sqrt{2}d^2} - \frac{0,5}{\sqrt{2}d^2}}^{\frac{2n-m}{\sqrt{2}d^2} + \frac{0,5}{\sqrt{2}d^2}} e^{-t^2} dt \end{aligned}$$

$\Phi \left(\frac{x-\mu}{\sigma} \right) = \frac{1}{2} \left(1 + \operatorname{erf} \left(\frac{x-\mu}{\sqrt{2}\sigma^2} \right) \right)$ – функция нормального распределения

$\operatorname{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt$ – функция ошибки



Отклонение было оценено как

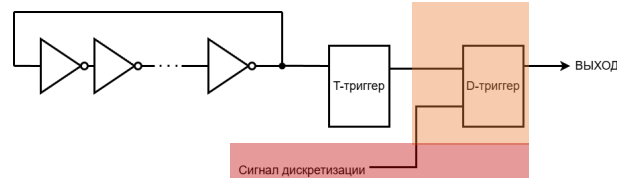
$$|P([\xi] \bmod 2 = 0) - 0,5| \leq e^{-\frac{\pi^2 d^2}{2}} \cdot \frac{2 \cos(\pi t)}{\pi}$$

где $\xi \sim N(t, d^2)$ случайная величина имеющая нормально распределение.

Пример:

Если $\xi \sim N(0, 2)$ то отклонения от равномерного распределения составим

$$|P([\xi] \bmod 2 = 0) - 0,5| \leq e^{-\frac{\pi^2 2}{2}} \cdot \frac{2 \cos(\pi \cdot 0)}{\pi} = \frac{2}{\pi} e^{-\pi^2} \approx 3,2928 \cdot 10^{-5}$$



$$\varepsilon = |P([\xi] \bmod 2 = 0) - 0,5|$$

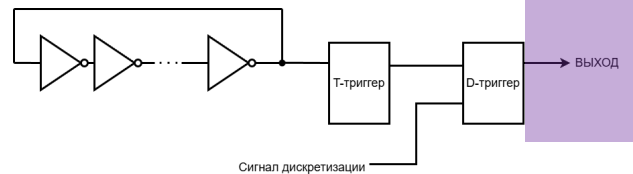
Из работы¹ известно, что если отклонение от равномерного распределения $\varepsilon = 10^{-3}$ то практическая секретность ключа длины 256 бит равна $4,34 \cdot 10^{76}$ (для абсолютно случайного ключа она равна $5,79 \cdot 10^{76}$)

Факторы влияющие на величину отклонения от равномерного распределения:

- ❖ Математическое ожидание периода кольцевого осциллятора
- ❖ Дисперсия кольцевого осциллятора
- ❖ Частота сигнала дискретизации

$$N_t \sim N(t\mu^{-1}, t\sigma^2\mu^{-3})$$

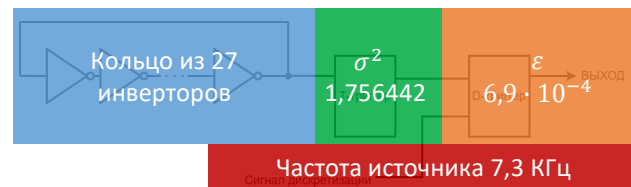
¹Логачев А. С., МIRONKIN В. О. О влиянии вероятностных характеристик дискретных источников, формирующих криптографические ключи, на практическую секретность ключа //Прикладная дискретная математика. – 2024. – №. 65. – С. 66-83.



Параметры разработанной схемы:

- ❖ Кольцо из 27 инверторов
- ❖ Частота опроса выхода Т-триггера $\approx 7,3$ КГц
- ❖ Отклонение выходных бит от равновероятного распределения $\varepsilon = 6,9 \cdot 10^{-4}$
- ❖ Скорость генерации бит $\approx 7,1$ Кбит/с





Параметры разработанной схемы:

Кольцо из 27 инверторов:

- ❖ $\mu = 34,984 \cdot 10^{-9} \text{ с}$
- ❖ $\sigma = 742,6 \cdot 10^{-12}$ (т.е. $\sigma \approx 0,02\mu$)¹
- ❖ Дисперсия распределения фронтов 1,756442

Вывод: ФДСЧ на КО потенциально применим для КИ низших классов.

Отклонение выходных бит от равновероятного распределения:

- ❖ $\varepsilon = 6,9 \cdot 10^{-4}$
- ❖ Теоретическое отклонение $1,1 \cdot 10^{-4}$
- ❖ Успешно проходит статистические тесты NIST

¹Sunar B., Martin W. J., Stinson D. R. A provably secure true random number generator with built-in tolerance to active attacks //IEEE Transactions on computers. – 2007. – Т. 56. – №. 1. – С. 109-119.



Спасибо за внимание!

