УДК 004.312

ИСТОЧНИК ЭНТРОПИИ НА БАЗЕ КОНФИГУРИРУЕМЫХ КОЛЬЦЕВЫХ ОСЦИЛЛЯТОРОВ

М.Н. Кайкы, А.А. Иванюк
Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Беларусь

SOURCE OF ENTROPY BASED ON CONFIGURABLE RING OSCILLATORS

M. Kaiky, A. Ivaniuk
Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus

Аннотация. Данная работа посвящена изучению конфигурируемого кольцевого осциллятора как элемента схем источников энтропии в генераторах истинно случайных чисел (TRNG). В работе рассмотрены генераторы на базе элементов, позволяющие получать последовательности импульсов для введения элемента памяти в метастабильное состояние.

Ключевые слова: случайные числа, источники энтропии, кольцевой генератор, метастабильность.

Annotation. This work is devoted to the study of a configurable ring oscillator as an element of entropy source circuits in true random number generators (TRNG). The work considers generators based on elements that make it possible to obtain sequences of pulses to introduce a memory element into a metastable state.

Keywords: random numbers, entropy sources, ring generator, metastability.

Согласно NIST SP 800-90, представляющих собой группу стандартов-рекомендаций по построению генераторов истинно случайных чисел – источники энтропии должны основываться на физическом шуме, с последующей оцифровкой и обработкой случайного числа. Использование физически неклонируемых функций (ФНФ) ещё на уровне разработки цифровой части заказных микросхем и ПЛИС позволяет снизить затраты на внедрение таких источников в конечное изделие, так как не требует размещения на кристалле сложных и больших структур АЦП. В работе рассматривается применение схемы с двумя конфигурируемыми кольцевыми осцилляторами и D-триггером как источника энтропии в составе генератора истинно случайных чисел (рисунок 1).

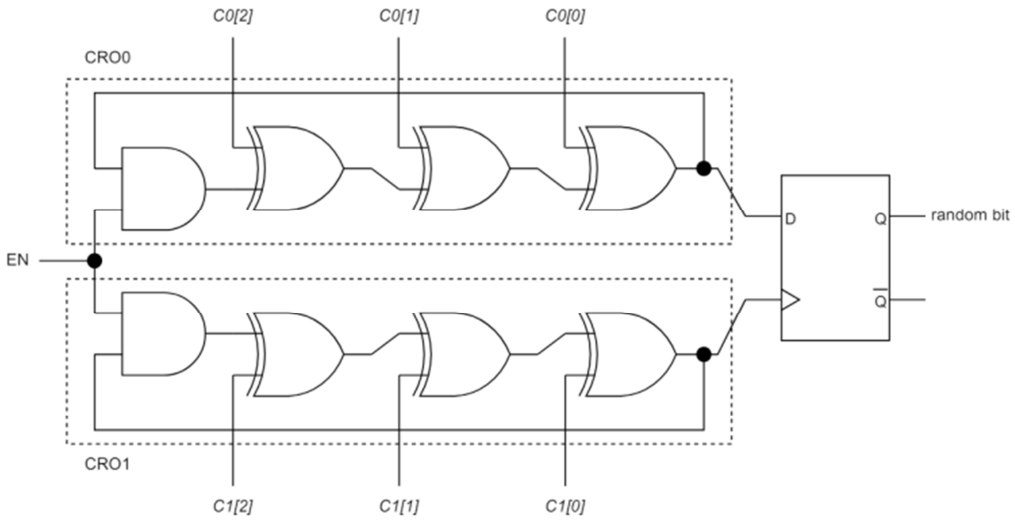

Рисунок 1 – Схема источника энтропии на базе двух конфигурируемых кольцевых осцилляторов

Входы *C0*, *C1* являются конфигурационными входами кольцевых осцилляторов CRO0, CRO1, вход *EN* является управляющим входом, и когда его уровень активен, осциллятор может начать колебаться (в зависимости от конфигурации). Используемые осцилляторы начинают колебаться только тогда, когда вес Хэмминга вектора *C* нечетен, а частота колебаний зависит от количества вентилей и значения конфигурации. На рисунке 2 показана зависимость значения периода колебаний конфигурируемых осцилляторов от заданной конфигурации, всего таких конфигураций 128.

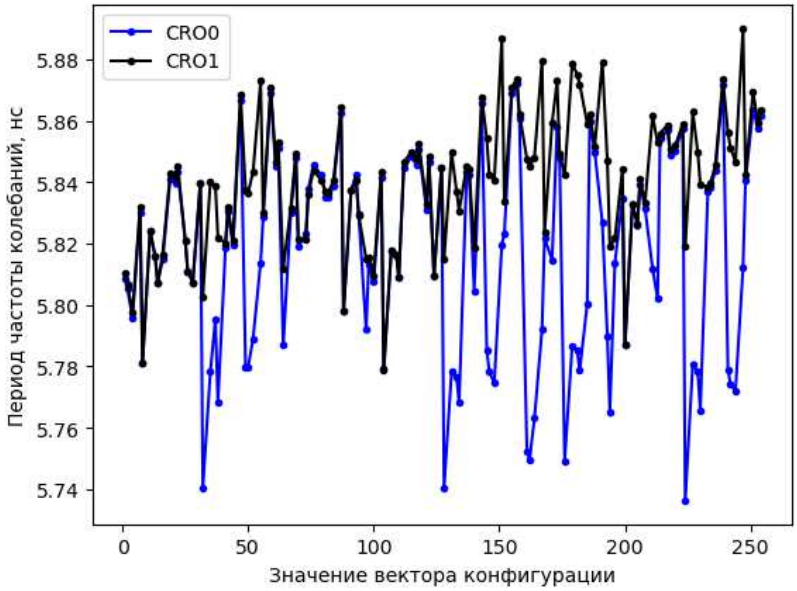

Рисунок 2 – Зависимость периода генерируемого сигнала от подаваемого запроса

С использованием Post-Implementation моделирования и фиксированными задержками для каждого из элементов, разработанной моделью обнаружения разницы между фронтами сигналов CRO0, CRO1 - были получены диаграммы работы осцилляторов (рисунок 3), значение периода повторений минимального и максимального значения разницы между фронтами сигналов синхронизации и данных для D-триггера с нарушениями как по setup-time так и по hold-time, также были получены задающие рабочие диапазоны переключений сигналов синхронизации и данных у триггера. Период повторений для *C0* = 1 (5.79784 нс), *C1* = 8 (5.88768 нс) составил 9.86 микросекунд, минимальное значение разницы фронтов составило – 0.003 пс.

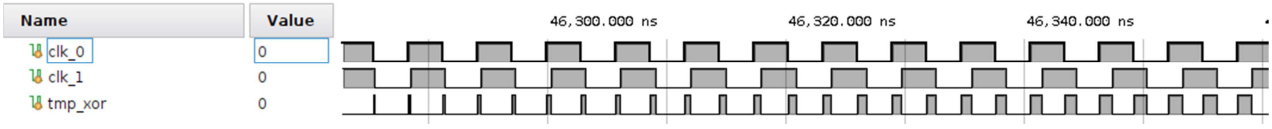

Рисунок 3 – Диаграмма изменения расстояния между фронтами выходов двух CRO

Используемая схема с двумя конфигурируемыми кольцевыми осцилляторами способна генерировать близкие друг к другу частоты, что способствует девиации разницы между фронтами сигналов синхронизации и данных у D-триггера и повышает вероятность попадания триггера в метастабильное состояние. Дальнейшие работы предполагают изучение зоны метастабильности триггера, для проведения подстройки осцилляторов с целью получения постоянного потока случайных бит с D-триггера.

Список цитируемых источников

1. NIST Special Publication, NIST SP 800-90, Recommendation for Random Bit Generation – NIST. [Электронный ресурс] – Режим доступа: https://nvlpubs.nist.gov/nistpubs/Legacy/-SP/nistspecialpublication800-90r.pdf. – Дата доступа: 01.10.2023.