ВРЕМЕННАЯ МОДЕЛЬ RS-ЗАЩЁЛКИ, РЕАЛИЗОВАННОЙ КАК ИСТОЧНИК СЛУЧАЙНОСТИ НА ПЛИС ТИПА FPGA

Кайкы М. Н., Иванюк А. А.
Кафедра информатики, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: kaikymykhailo@gmail.com, ivaniuk@bsuir.by

Исследуется метастабильность RS-защёлок с различными значениями технологических задержек на ПЛИС типа FPGA как источник энтропии для генераторов случайных чисел. Показывается зависимость вероятности перехода RS-защёлки в метастабильное состояние от введенного коэффициента симметрии.

Введение

Разработка генераторов истинно случайных чисел (ГИСЧ) остается актуальной задачей в области криптографии и защиты информации. Одним из перспективных физических источников энтропии для ГИСЧ является метастабильное состояние цифровых элементов, в частности, RS-защелок, где бистабильная система хаотическим образом сходится к одному из двух устойчивых состояний [1]. Однако использование данного явления сопряжено с фундаментальной проблемой: метастабильность изначально рассматривалась в цифровой схемотехнике как нежелательное и аномальное явление, что обусловило недостаточность существующих функциональных и временных моделей для ее точного прогнозирования и анализа. Стандартные детерминистические модели на языках описания аппаратуры (HDL) не способны адекватно описать вероятностную природу и временные параметры метастабильных процессов. В связи с этим, необходимость разработки комплексной методики функционального моделирования метастабильности в RS-защелках становится важной.

I. Реализация RS-защёлки на технологии FPGA

На рисунке 1 изображена структурная схема разработанного аппаратного обеспечения для проведения исследования. Для реализации структур типа RS-защёлка на базе примитивов FPGA от компании Xilinx семейства Zynq7000 используется два блока типа 6-ти входовой таблицы истинности (генераторов переключательной функции), связанных друг с другом при помощи обратной связи с образованием комбинационной петли и выполняющих функцию "И-НЕ"(*NAND2*). При этом два LUT6 абсолютно идентичны друг другу функционально, количество защёлок равнялось $N = 1024$. Для формирования управляющих сигналов на входы Set/Reset защёлок был разработан управляющий автомат, при этом стоит отметить, что управляющих регистров в схеме всего два – один для формирования сигнала Set, второй для формирования сигнала Reset, что позволяет сформировать 2048 технологически уникальных задержек распространения управляющих сигналов до каждого из экземпляров RS-защёлок (δ_{13}, δ_{23}).

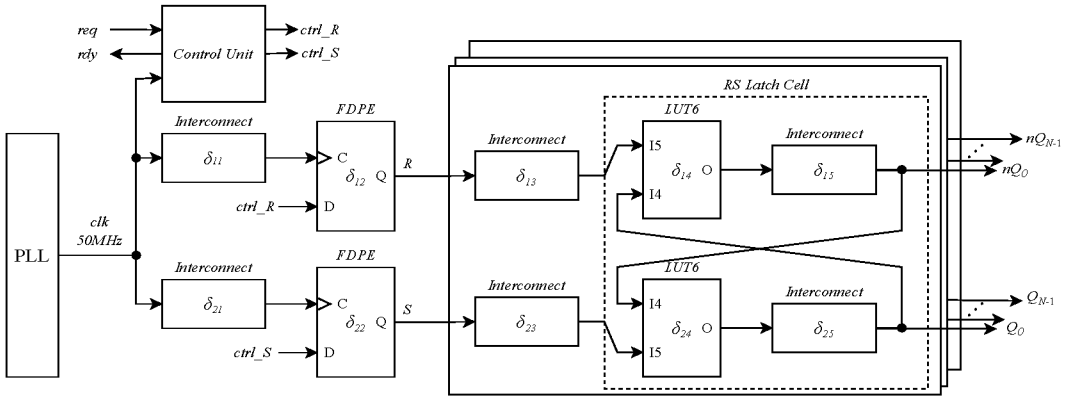

Рис. 1 – Структура стенда для исследования RS-защёлок с задержками на кристалле ПЛИС

Работа выполнена в совместной учебной лаборатории БГУИР-YADRO
https://www.bsuir.by/ru/kaf-informatiki/yadro

II. Временное моделирование RS-защёлок

В ходе проведения моделирования разрабатываемой схемы после процесса имплементации на кристалле FPGA в среде моделирования QuestaSim были получены значения уникальных задержек компонентов схемы ($\delta_{11}, \delta_{12}, \delta_{13}, \delta_{14}, \delta_{15}, \delta_{21}, \delta_{22}, \delta_{32}, \delta_{24}, \delta_{25}$). В процессе моделирования на все 1024 защёлки подавалась последовательность входных воздействий, которая приводила защёлки в последовательность состояний (*Reset*, *Store*, *Forbidden*, *Store*), которое способно привести RS-защёлку в метастабильное состояние. В результате моделирования было получено 1024 различных и уникальных значения счётчиков C, которые фиксировали количество нарастающих и спадающих фронтов на выходе Q для всех 1024 защёлок и были реализованы в тестовом окружении, обладая нулевыми задержками переключения. При $C = \{0, 2\}$ – мы считаем что RS-защёлка стабильно перешла из состояния *Forbidden* в состояние *Store* и сохранила состояние 0 или 1, а при $C > 2$ наблюдается осцилляция на выходе защёлки Q. Всего было зафиксировано 76,85% стабильных защёлок и 23,15% нестабильных. При этом стоит отметить, что при фиксированном времени моделирования, не все значения C были идентичны друг другу, что говорит о разном периоде осцилляции на выходах RS-защёлок. Также было обнаружено что некоторые нестабильные RS-защёлки переходили в устойчивое состояние через некоторое время моделирования, соответственно осцилляция на выходе являлась затухающей, такое же поведение защёлок приведено при КМОП реализации в работе [2].

III. Влияние симметрии в RS-защёлке на её стабильность

Введем коэффициент симметрии (K), который будем рассчитывать по формуле 1.

$$K = \frac{\delta_{upper} - \delta_{lower}}{max(\delta_{upper}, \delta_{lower})}, \quad (1)$$

где $\delta_{upper} = \delta_{11} + \delta_{12} + \delta_{13} + \delta_{14} + \delta_{15}$,
$\delta_{lower} = \delta_{21} + \delta_{22} + \delta_{23} + \delta_{24} + \delta_{25}$.

Результат рассчёта коэффициентов K для всех 1024 RS-защёлок изображен на рисунке 2, при этом синим цветом отображены защёлки, ответы которых были стабильны, а красным – нестабильные защёлки с осцилляцией на выходе Q. Как видно из риснука 2, при коэффициенте K стремящемся к 0 количество осциллирующих (нестабильных) RS-защёлок увеличивается, при этом нестабильные защёлки фиксировались на промежутке $K = [0,121; -0,151]$, полученная зависимость позволяет сделать вывод: способность RS-защёлки переходить в состояние осцилляции на выходах Q, nQ – зависит от степени симметрии при построении RS-защёлки и схемы её управления.

IV. Заключение

В ходе исследования был введен коэффициент симметрии в RS-защёлках, разработанных по технологии FPGA, было обнаружено что при коэффициенте симметрии стремящегося к 0 – вероятность перехода в состояние метастабильности RS-защёлки повышается. Дальнейшие работы направлены на исследование изменения коэффициента симметрии от технологических вариаций и эмпирическое доказательство полученных результатов на реальных экземплярах FPGA.

V. Список литературы

1. Sunar, B. A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks / B. Sunar, W. Martin, D. Stinson // Computers, IEEE Transactions on. – 2007. – Vol. 56. – P. 109–119.
2. Kacprzak, T. Analysis of Oscillatory Metastable Operation of an RS Flip-Flop / T. Kacprzak // Solid-State Circuits, IEEE Journal of. – 1988. – Vol. 23. – P. 260–266.

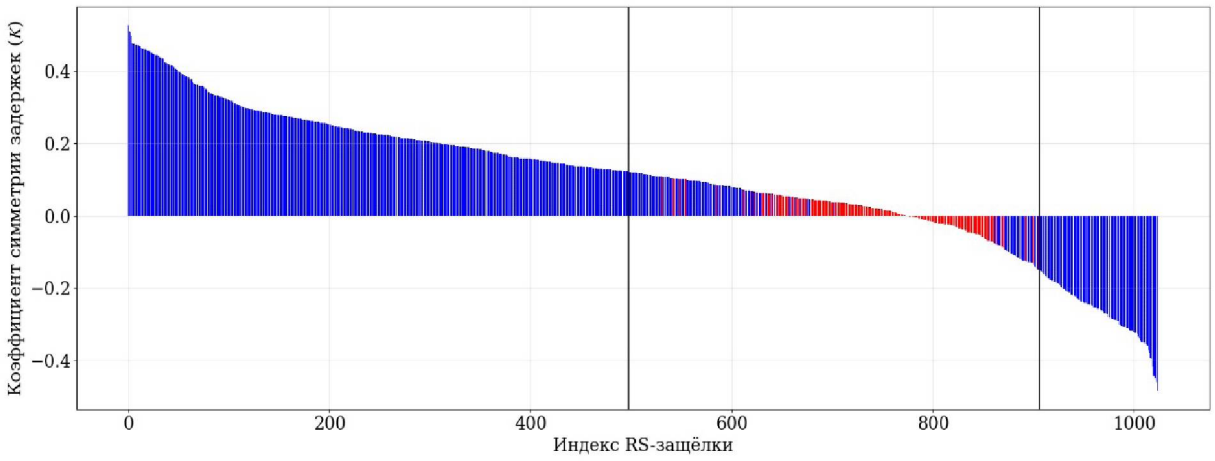

Рис. 2 – Зависимость стабильности RS-защёлок от коэффицинта симметрии