УДК 004.312

ИССЛЕДОВАНИЕ ПОВЕДЕНИЯ БИСТАБИЛЬНЫХ ЭЛЕМЕНТОВ, РЕАЛИЗОВАННЫХ НА ПЛИС

Кайкы М.Н., Иванюк А.А.

Белорусский государственный университет информатики и радиоэлектроники, Минск, Республика Беларусь, kaikymykhailo@gmail.com

Аннотация: исследуется возможность использования бистабильного элемента на базе LUT6 в качестве физического источника энтропии для генераторов истинно случайных чисел (ГИСЧ), реализуемых на ПЛИС. На аппаратной платформе ПЛИС Xilinx Zynq-7000 из 1024 бистабильных элементов, синтезированных на примитивах LUT6, выполнена серия экспериментов со всеми возможными конфигурациями обратной связи с целью изучения их нестационарного поведения при инициализации. Для количественной оценки равномерности распределения состояний использовалась метрика единообразия. Показано, что значение единообразия зависит от конфигурации обратной связи и от физического размещения ячеек на кристалле ПЛИС: в большинстве конфигураций более 95 % ячеек обладают нулевым значением единообразия, число ячеек с ненулевым значением единообразия варьируется от 7 до 125 из 1024, а максимальное среднее единообразие не превышает 0,0374. Полученные результаты формируют основу для целенаправленного проектирования ячеек с управляемой степенью рассогласования плеч обратной связи.

Ключевые слова: бистабильный элемент; метастабильность; физически неклонируемая функция; генератор истинно случайных чисел; ПЛИС; LUT6; начальное состояние; единообразие.

I. ВВЕДЕНИЕ

Реализация генераторов истинно случайных чисел (ГИСЧ) на базе ПЛИС требует использования полностью цифровых источников энтропии, способных функционировать в условиях жестких аппаратных ограничений [1]. Среди перспективных источников выделяются бистабильные элементы памяти, поведение которых при нарушении временных характеристик становится недетерминированным [2]. В работе [3] была предложена аналитическая модель управляемого бистабильного элемента, доказывающая возможность перехода в режим автоколебаний для генерации случайных данных, однако при реализации подобных решений на базе ПЛИС критическую роль начинают играть факторы, не учитываемые в программных моделях – задержки в цепях межсоединений. Архитектура ПЛИС характеризуется наличием разветвленной сети коммутационных ресурсов, вносящих технологически зависимые задержки распространения сигналов [4]. Автоматизированная трассировка приводит к различию задержек в плечах обратной связи бистабильных элементов, кроме того, временные характеристики нарастания и спада сигналов, проходящих через коммутационные матрицы, могут существенно различаться, что влияет на условия возникновения метастабильности [5].

II. СТРУКТУРА АППАРАТНОЙ ПЛАТФОРМЫ ДЛЯ ПРОВЕДЕНИЯ ЭКСПЕРИМЕНТА

Рассмотрим структуру разработанного аппаратного блока для проведения исследований на платформе ПЛИС (рисунок 1).

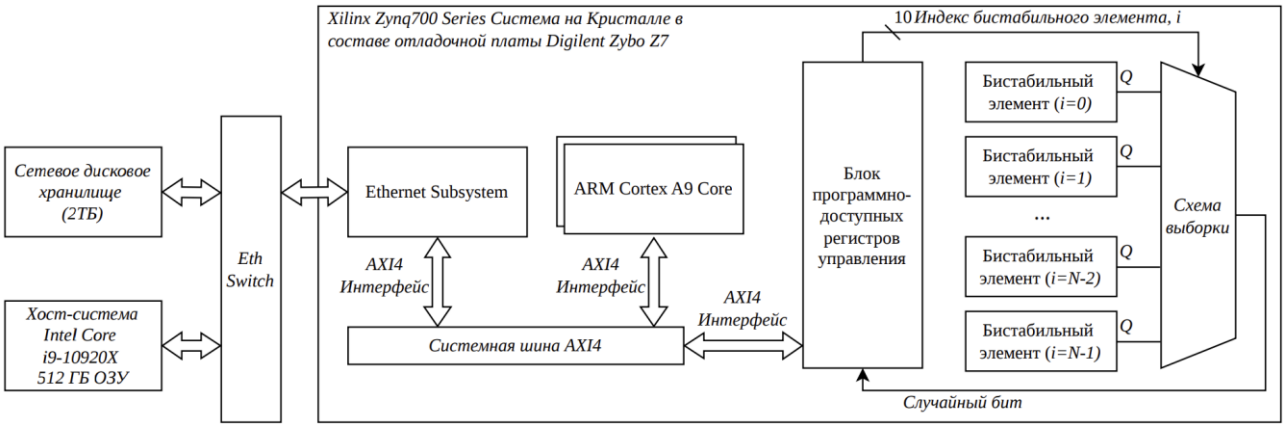


Рисунок 1. Аппаратная платформа для проведения экспериментов

Исследуемыми объектами являются бистабильные элементы, реализованные на примитивах LUT6 ПЛИС семейства Zynq7000 (Xilinx), где каждый из которых состоит из двух шестивходовых элементов переключательной функции LUT6, настроенных на выполнение операции "НЕ" (INV) и охваченных обратной связью, образуя комбинационную петлю (рисунок 2). Оба LUT6 функционально идентичны, а общее количество элементов в системе составляет $N = 1024$.

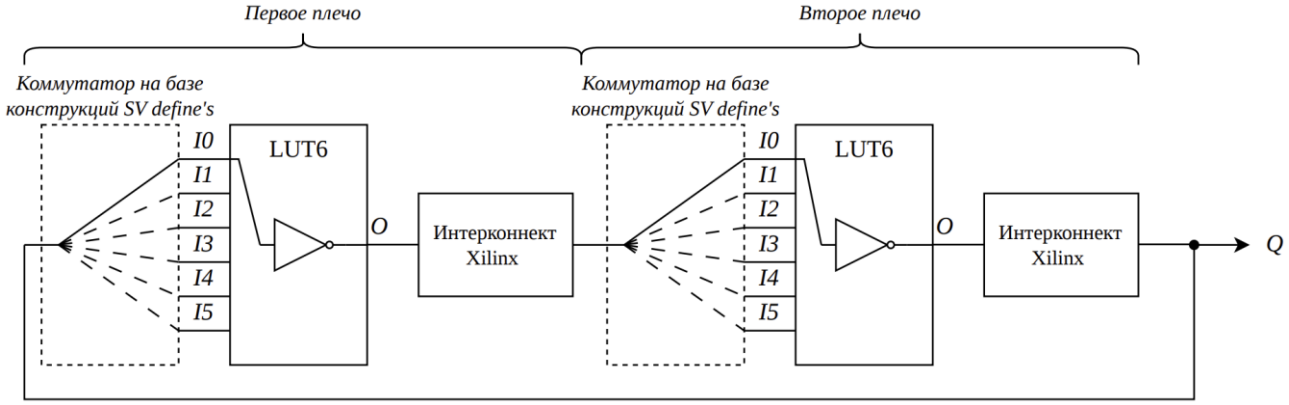


Рисунок 2. Бистабильный элемент на базе примитивов LUT6

Для исследования влияния сетей маршрутизации в экземплярах ПЛИС на качество генерируемых последовательностей начальных состояний элементов были сформированы все возможные 36 конфигураций обратных связей при помощи конструкции *define* препроцессора языка описания аппаратуры SystemVerilog. Для ограничения работы синтезатора также были подготовлены 36 файлов с указанием местоположения каждого из $2 \cdot N = 2048$ элементов LUT6 на кристалле ПЛИС. Разработанное аппаратное обеспечение и файлы ограничений позволили провести эксперимент для выявления зависимости качества начальных состояний бистабильных элементов при инициализации ПЛИС (включении питания) от конфигурации сети маршрутизации на сетях межсоединений.

III. ПРОВЕДЕНИЕ ЭКСПЕРИМЕНТА НА БАЗЕ ПЛИС

Ход эксперимента заключается в последовательном синтезе дизайна с одной из 36 комбинаций петли обратной связи, различающихся индексом используемого информационного входа LUT6 в первом и втором плечах защёлки. После загрузки конфигурации производится адресный опрос состояния каждой ячейки через общий мультиплексор: выбранный бистабильный элемент подключается к выходному регистру, и его логический уровень на выходе Q фиксируется хост-системой на базе процессорных ядер ARM Cortex A9. Для сбора статистики по всем 1024 элементам опрос повторяется для каждой конфигурации, после чего выполняется серия принудительных перезапусков с полным сбросом программируемой логики. В момент снятия сброса каждый бистабильный элемент под действием обратной связи самопроизвольно переходит в одно из двух устойчивых состояний. Процесс перезагрузки повторяется заданное число раз $K = 1000$, что даёт независимые выборки начальных состояний для всего массива из $N = 1024$ элементов. В результате формируется матрица данных размером $N \times K$, каждая строка которой представляет собой значения начальных состояний всех элементов, а каждый столбец - временной ряд инициализационных значений для отдельной ячейки. Обозначим такие столбцы как V_i.

IV. АНАЛИЗ ПОЛУЧЕННЫХ ДАННЫХ

Для анализа полученных данных используем метрику единообразия, которая отображает степень равномерности распределения нулевых и единичных состояний в полученном векторе инициализаций для каждой из ячеек:

$$U_i = 1 - 2 \times \left| \frac{WH(V_i)}{K} - 0{,}5 \right|,$$

где K – количество циклов перезапуска ПЛИС, $WH(V_i)$ – вес Хэмминга вектора V_i, V_i – вектор инициализационных значений для ячейки бистабильного элемента с индексом i.

Метрика единообразия принимает значения в диапазоне [0;1]: значение $U_i = 1$ соответствует идеально сбалансированному элементу, для которой вероятность единичного состояния $P(1) = 0{,}5$, а значение $U_i = 0$ – полностью детерминированному элементу, у которого $P(1) = 0$ или $P(1) = 1$ при всех K перезагрузок. Бистабильный элемент будем называть шумящим, если выполняется неравенство

$0 < WH(V_i) < K$. Для таких элементов метрика единообразия строго положительна: $U_i > 0$. Элементы, у которых $WH(V_i) = 0$ или $WH(V_i) = K$, будем называть детерминированными: их начальное состояние воспроизводится от перезапуска к перезапуску без изменений, а $U_i = 0$. На рисунке 3 приведены столбчатые диаграммы распределения значения единообразия по индексам элементов для двух конфигураций – конфигурации № 0 и конфигурации № 28. Верхний график соответствует конфигурации с наибольшим числом шумящих элементов (125 из 1024), нижний – конфигурации с наименьшим числом таких элементов (7 из 1024). В обоих случаях подавляющее большинство элементов имеет $U_i = 0$, то есть ведёт себя полностью детерминированно, тогда как шумящие элементы распределены по индексам неравномерно. Наблюдаемая картина указывает на то, что начальное состояние бистабильного элемента определяется систематической составляющей, воспроизводимой от перезапуска к перезапуску, а доля случайной компоненты в разрешении состояния крайне мала. На рисунке 4 приведена сводная гистограмма нормированного числа ненулевых ячеек по всем 36 конфигурациям. Каждый столбец соответствует одной конфигурации петли обратной связи, высота графика пропорциональна числу ячеек с $U_i > 0$, нормированному по максимальному значению U_i (конфигурация № 0, 125 ячеек).

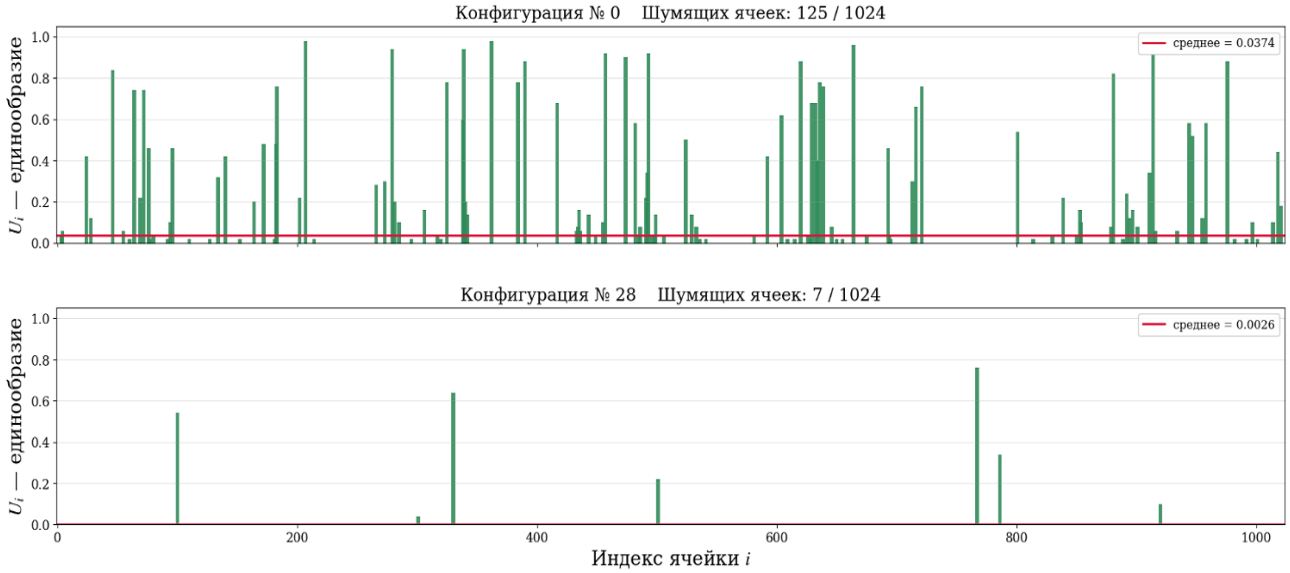


Рисунок 3. Распределение единообразия по ячейкам в разных конфигурациях сетей межсоединений

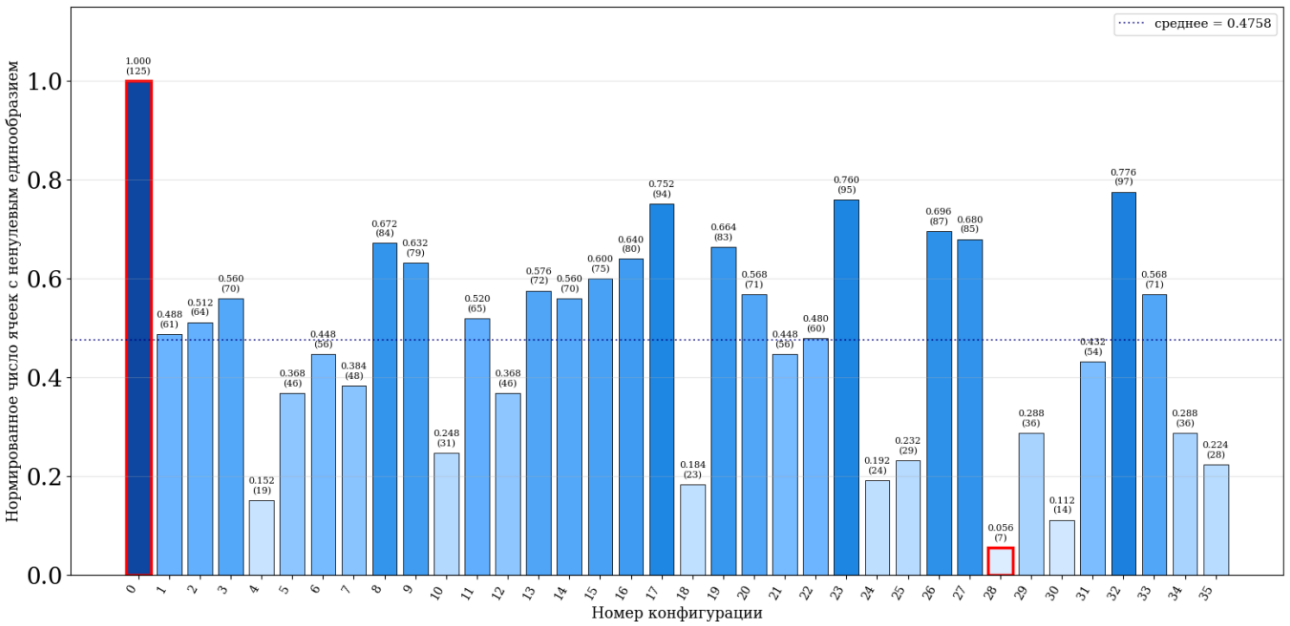


Рисунок 4. Диаграмма распределения нестабильных ячеек по номеру конфигурации

Видно, что распределение конфигураций по числу шумящих ячеек крайне неравномерно: наряду с конфигурациями, дающими 50 – 100 активных ячеек, присутствуют конфигурации с единичными шумящими ячейками (например, № 4 с 12 ячейками, № 25 с 7 ячейками). Среднее нормированное число ненулевых ячеек составляет 0,476, что указывает на значительную вариативность между конфигурациями. Полученные данные показывают, что выбор пары активных входов LUT6 существенно влияет на итоговый уровень случайности при инициализации ПЛИС.

V. ЗАКЛЮЧЕНИЕ

В работе исследовано влияние сети межсоединений бистабильных элементов на базе LUT6 в ПЛИС на качество генерируемых случайных последовательностей их начальных состояний. На аппаратной платформе из 1024 бистабильных элементов с 36 возможными вариантами подключения цепей обратной связи выполнена серия экспериментов с многократными перезапусками программируемой логики. Полученные результаты формируют экспериментальную основу для последующего проектирования ячеек с управляемой степенью рассогласования плеч обратной связи и создания на их основе источников энтропии на базе физически неклонируемых функций в ПЛИС.

БЛАГОДАРНОСТЬ

Авторы выражают искреннюю благодарность резиденту ПВТ компании «Инженерный Центр Ядро», которая является одним из центров разработки YADRO, за предоставленное оборудование для проведения экспериментов в рамках работы совместной учебной лаборатории с Белорусским государственным университетом информатики и радиоэлектроники.

ЛИТЕРАТУРА

[1] Gassend B., Clarke D., Van Dijk M., Devadas S. Silicon Physical Random Functions. Proc. of the 9th ACM conference on Computer and communications security, CCS ’02. 2002:148–160.

[2] Technical specification Physical random number generators for use in cryptographic information protection tools that do not contain information constituting a state secret: TS 26.4.001-2019: valid from 18.04.2019 / Technical Committee for Standardization "Cryptographic Information Protection". – Moscow 2019. – 20 p.

[3] Кайкы М.Н., Иванюк А.А. Управление метастабильным состоянием элемента памяти с целью генерации случайных данных. Доклады БГУИР. 2025;23(5):75–82.

[4] Иванюк, А. А. Физически неклонируемая функция типа абитр с нелинейными парами путей = Physically non-cloneable arbiter -type function with non-linear path pairs / А. А. Иванюк, А. Ю. Шамына // Системный анализ и прикладная информатика. – 2023. – № 1. – С. 54–62.

[5] Skoric, B. Robust key extraction from physical uncloneable functions / B. Skoric, P. Tuyls, W. Ophey // Int. Conf. on Appl. Cryptogr. and Network Secur. (ACNS’05). – New York, USA, 2005. – P. 407–422.

RESEARCH ON THE BEHAVIOR OF BISTABLE ELEMENTS IMPLEMENTED ON AN FPGA

M. Kaiky, A. Ivaniuk

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus,
kaikymykhailo@gmail.com

Abstract: the paper investigates the feasibility of using a LUT6-based bistable element as a physical entropy source for True Random Number Generators (TRNGs) implemented on FPGAs. On an experimental platform based on a Xilinx Zynq-7000 FPGA comprising 1024 bistable elements synthesized on LUT6 primitives, a series of experiments was performed with 36 feedback-loop configurations in order to study their non-stationary behavior during initialization. To quantitatively assess the uniformity of the distribution of states, a uniformity metric was used. The uniformity value is shown to depend on the feedback-loop configuration and on the physical placement of cells on the FPGA die: in most configurations more than 95 % of cells have a zero-uniformity value, the number of cells with a non-zero uniformity value varies from 7 to 125 out of 1024, and the maximum average uniformity does not exceed 0.0374. The results obtained provide a basis for the targeted design of cells with a controlled degree of feedback-branch asymmetry.

Keywords: bistable element; metastability; entropy source; physically unclonable function; true random number generator; FPGA; LUT6; initial state; uniformity.