УДК 004.312

RS-ЗАЩЕЛКА КАК ИСТОЧНИК СЛУЧАЙНОСТИ В РЕЖИМЕ ИНИЦИАЛИЗАЦИИ

М.Н. Кайкы, А.А. Иванюк
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В работе выполнен анализ значений инициализации RS-защелки, реализованной на базе ПЛИС, в котором показано, что разброс задержек в межсоединениях, обусловленный различиями в маршрутах трассировки, является определяющим фактором в получении случайных последовательностей.
Ключевые слова: RS-защелка; метастабильность; задержка распространения; источник энтропии; физически неклонируемая функция (ФНФ); автоколебания, ПЛИС;

RS-LATCH AS A SOURCE OF RANDOMNESS IN INITIALIZATION MODE

M.N. Kaiky, A.A. Ivaniuk
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The work analyzes the initialization values of an RS latch implemented on an FPGA, which shows that the spread of delays in interconnections, caused by differences in routing paths, is a determining factor in obtaining high randomness characteristics.
Keywords: RS latch; metastability; propagation delay; entropy source; physically unclonable function (PUF); oscillations; FPGA;

Введение

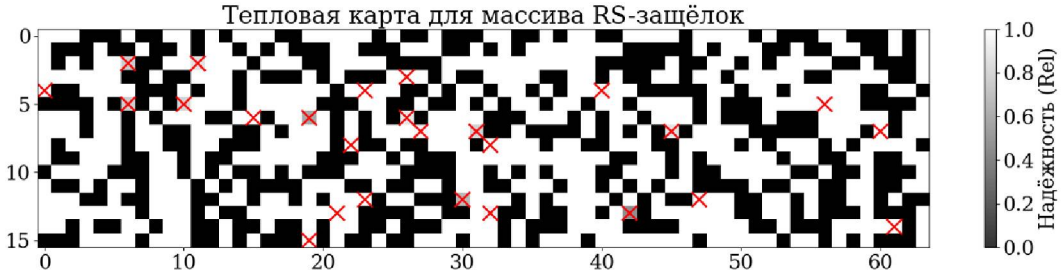
Реализация генераторов истинно случайных чисел (ГИСЧ) на базе программируемых логических интегральных схем (ПЛИС) требует использования полностью цифровых источников энтропии, способных функционировать в условиях жестких аппаратных ограничений [1]. Среди перспективных источников выделяются бистабильные элементы памяти, поведение которых при нарушении временных соотношений становится недетерминированным [2]. Архитектура ПЛИС характеризуется наличием разветвленной сети коммутационных ресурсов, вносящих технологически зависимые задержки распространения сигналов [3]. Автоматизированная трассировка приводит к различию задержек в плечах обратной связи RS-защелки, нарушая симметрию элемента. Цель работы – анализ влияния вариативности задержек в цепях межсоединений ПЛИС на переход RS-защелки в метастабильное состояние для использования в качестве источника энтропии в аппаратных ГИСЧ в режиме инициализации при включении питания.

Эксперимент по инициализации RS-защелки

Проведем эксперимент, в котором покажем зависимость параметра надежности ФНФ на базе RS-защелки. Для проведения эксперимента будем перезагружать экземпляр ПЛИС (Xilinx Zynq-7020 в составе платы быстрого прототипирования PYNQ Z2) K раз, где $K = 500$ и после каждой перезагрузки считывать значения с выхода Q_i из 1024 ячеек RS-защелок, где i – индекс защелки. Тогда надежность для каждой ячейки рассчитывается так:

$$Rel_i = 2\left|\frac{\sum_{k=0}^{K-1} Q_{ik}}{K} - 0{,}5\right|, \quad (1)$$

где K – количество циклов перезагрузки ПЛИС; Q_{ik} - ответ i-той RS-защелки в цикле перезагрузки k.



Тепловая карта надежности массива RS-защелок
RS Latch array reliability heat map

Как видно из рисунка, у большинства ячеек (97,5%) между циклами перезагрузки ответы соответствовали $Rel = 1$ и формировали подобие уникального и стабильного отпечатка экземпляра ПЛИС, однако у оставшихся 2,5% RS-защелок надежность $Rel < 1$.

При помощи инструментов netlist-моделирования системы автоматизированного проектирования Vivado был получен файл, предназначенный для хранения и передачи информации о задержках и временных характеристиках электронных схем – SDF (Standard Delay Format). Анализ временных параметров показал, что задержки на цепях межсоединений значительно превышают задержки на логических элементах (LUT6). В среднем, задержки маршрутизации больше в 9 раз, что свидетельствует о доминирующем вкладе межсоединений в общую асимметрию временных характеристик аппаратной реализации RS-защелки.

Заключение

Полученные результаты позволяют сформулировать ряд выводов, имеющих значение для развития физических методов генерации случайных чисел в полностью цифровых средах. Проведенное исследование подтвердило, что основным источником недетерминированного поведения RS-защелок при включении питания является не только внутренний шум полупроводниковой структуры, а и технологически обусловленная асимметрия задержек в цепях межсоединений. Автоматизированная трассировка, выполняемая системами проектирования, неизбежно вносит различия в длины маршрутов обратной связи. Практическая значимость полученных результатов заключается в возможности создания гибридных архитектур, совмещающих на одном кристалле функции идентификации и генерации случайных чисел. Исследование демонстрирует, что сложность и неоднородность современных ПЛИС, традиционно рассматриваемые как недостаток, могут быть обращены в преимущество при создании физических источников энтропии. Технологический разброс, неизбежный при производстве и автоматизированном проектировании, становится не препятствием, а основой для реализации криптографических примитивов, опирающихся на неконтролируемые физические процессы.

Список использованных источников

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. Ivanyuk, A. A. Physically non-cloneable Arbiter-type function with non-linear path pairs / A. A. Ivanyuk, A. Yu. Shamina // Systems Analysis and Applied Informatics. - 2023. - No. 1. - P. 54-62.

References

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. Ivanyuk, A. A. Physically non-cloneable Arbiter-type function with non-linear path pairs / A. A. Ivanyuk, A. Yu. Shamina // Systems Analysis and Applied Informatics. - 2023. - No. 1. - P. 54-62.

Сведения об авторах

Кайкы М.Н., магистр техн. наук, учреждение обраования «Белорусский государственный университет информатики и радиоэлектроники», kaikymykhailo@gmail.com

Иванюк А.А., д-р техн. наук, проф., проф. каф. информатики, «Белорусский государственный университет информатики и радиоэлектроники», ivaniuk@bsuir.by

Information about the authors

Kaiky M. N., M. Sci. (Tech.), Educational Institution "Belarusian State University of Informatics and Radioelectronics", kaikymykhailo@gmail.com

Ivaniuk A. A., Dr. Sci. (Tech.), Professor, Professor at the Department of Computer Science, Educational Institution "Belarusian State University of Informatics and Radioelectronics", ivaniuk@bsuir.by