РАЗРАБОТКА ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ПРИМЕНЕНИЕМ ПРОГРАММИРУЕМЫХ ЛОГИЧЕСКИХ ИНТЕГРАЛЬНЫХ СХЕМ (ПЛИС)

Пирогов А.А.[1], Пирогова Ю.А.[1], Гвозденко С.А.[1],
Шардаков Д.В.[1], Макаров О.Ю.[1]
[1)] Воронежский государственный технический университет, г. Воронеж, Россия
E-mail: pirogov.alx@gmail.com

DEVELOPMENT OF PSEUDORANDOM SEQUENCE GENERATORS USING PROGRAMMABLE LOGIC INTEGRATED CIRCUITS (FPGAS)

Pirogov A.A.[1], Pirogova Y.A.[1], Gvozdenko S.A.[1],
Shardakov D.V.[1], Makarov O.Y.[1]
[1)] Voronezh State Technical University, Voronezh, Russia

This study examines the circuits of digital automata, as well as generators of pseudo-random sequences, which are used in cryptography problems, where the properties of the programmable FPGA structure are quite relevant.

Целью работы является разработка сложно-функционального блока устройства генерирования псевдослучайных кодовых комбинаций на основе регистров с линейной обратной связью. Работа включает построение RTL описания и проведение верификации.

Генератор псевдослучайной последовательности Фибоначчи трехразрядного двоичного кода, выполненный на основе регистра сдвига, с использованием JK-триггеров с асинхронными входами сброса и установки представлен на рисунке ниже.

Основываясь на выражении обратной связи и таблице кодовых комбинаций последовательности Фибоначчи получаем, что внутреннее состояние на седьмом шаге вернулось к исходному при условии, что начальное состояние регистра сдвига равно единице. Поэтому начиная со следующего шага, будет идти повтор бит кодов. На рисунке также представлена временная диаграмма модели генератора псевдослучайной последовательности Фибоначчи. Из диаграммы видно, что переключение генератора происходит по фронту синхроимпульса (Clk), а полученный код на выходе (Y) модели соответствует исходной таблице кодовых комбинаций последовательности Фибоначчи.

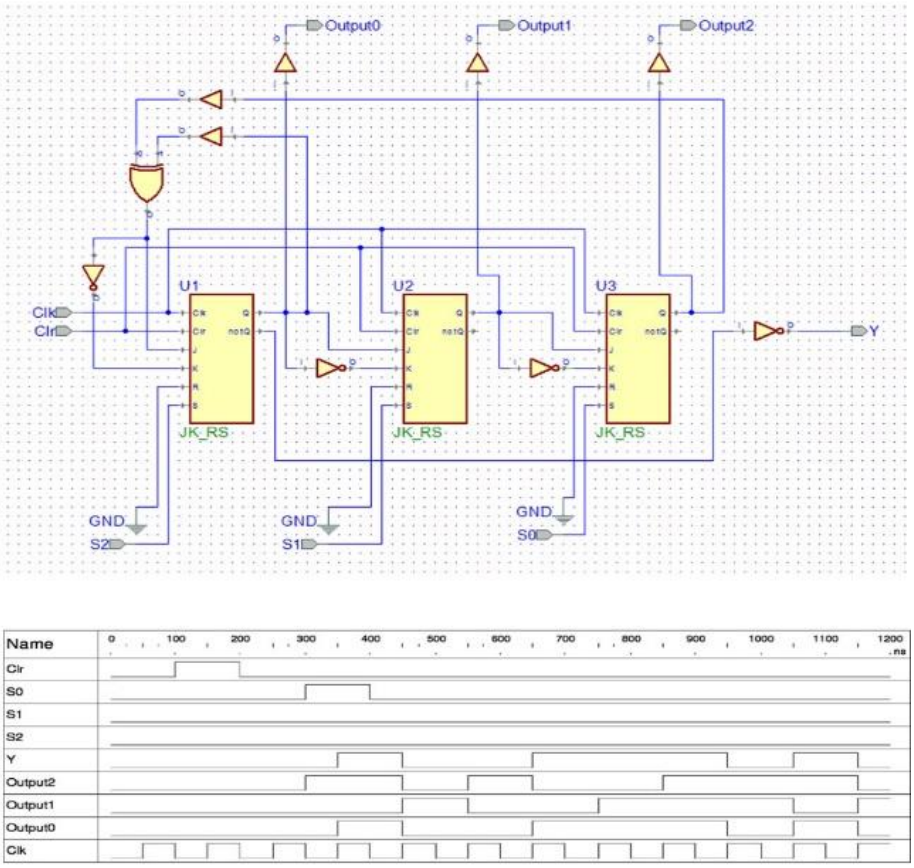

Рис. 1. Генератор псевдослучайной последовательности Фибоначчи

Генератор псевдослучайной последовательности Галуа аналогично построен на основе регистра сдвига. При анализе его работы видно, что внутреннее состояние регистра на седьмом шаге вернулось к исходному, следовательно, его период также как и в прошлом случае равен 7. В отличие от конфигурации Фибоначчи, внутренние состояния регистра получились другие, но генерируемая последовательность совпадает с кодом Фибоначчи, только сдвинута на 4 такта.

1. Башкиров А.В., Свиридова И.В., Муратов А.В. Эффективное многопороговое декодирование недвоичных кодов с предварительной оценкой ошибочности проверок. Вестник воронежского государственного технического университета. 2015. Т.11. №3. с. 99-101.
2. Пирогов А.А. Методы повышения помехозащищенности и эффективности кодирования сетей связи абонентского доступа Вестник воронежского государственного технического университета. 2011. Т.7. №1. С. 162-163.
3. Пирогов А.А., Бочаров Е.А., Сёмка Э.В., Макаров О.Ю. Методика проектирования синтезатора частот прямого цифрового синтеза на базе ПЛИС. Вестник воронежского государственного технического университета. 2018. Т.14. № 6. С. 108-116.