С. С. Заливако

ПРИМЕНЕНИЕ КОЛЬЦЕВЫХ ГЕНЕРАТОРОВ ДЛЯ ПОЛУЧЕНИЯ ДЕЙСТВИТЕЛЬНО СЛУЧАЙНЫХ ЧИСЛОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Рассмотрена возможность применения физически неклонируемой функции (ФНФ) типа кольцевой генератор для получения действительно случайных числовых последовательностей (ГДСЧП). Произведена схемная реализация генератора на базе FPGA. Проведен эксперимент по генерированию последовательности трехбайтных случайных чисел. Полученная последовательность протестирована с помощью пакета NIST.

Последовательность случайных чисел является одним из ключевых элементов целого ряда прикладных задач из различных предметных областей: криптография, моделирование, игровая индустрия, случайная выборка, искусство. Поскольку охват сфер использования ДСЧП велик, актуальность создания цифровых устройств для их генерирования не вызывает сомнений.

Генератор представляет собой набор регистров, каждый из которых является выходом схемы, реализующей ФНФ, которая может работать в двух режимах: ФНФ на основе статистического ОЗУ (SRAM-PUF) и ФНФ на основе кольцевых генераторов (RO-PUF). Схемная реализация ячейки регистра приведена на рис.1.

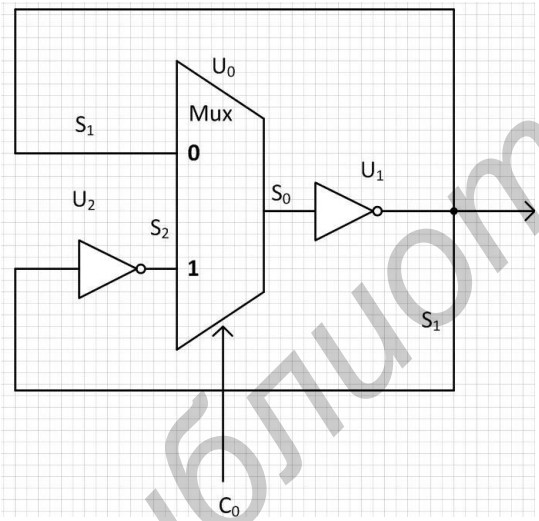

Рис. 1 – Схема ячейки генератора

На вход мультиплексора U_0 поступает управляющий сигнал C_0. Если значение сигнала $C_0 = 0$, то ячейка представляет собой ФНФ типа кольцевой генератор и ФНФ типа статическое ОЗУ [1] в противном случае. В режиме RO-PUF начинается выработка действительно случайного бита, причем каждый из выходов кольцевых генераторов является входом другого кольцевого генератора (см. рис. 2). За счет такого взаимодействия происходит накопление энтропии.

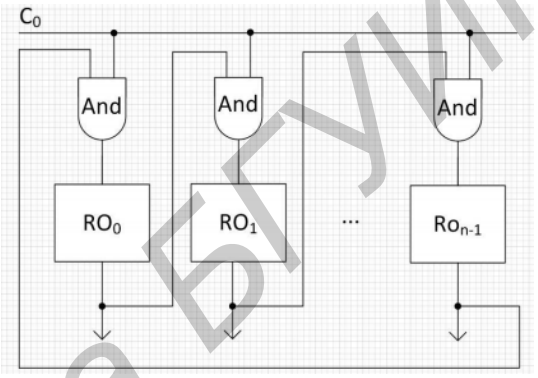

Рис. 2 – Схема генератора

В режиме SRAM на выходе генератора присутствует стабильное значение, что позволяет зафиксировать некое случайное число, полученное в режиме RO-PUF, и выдать его пользователю.

Тестирование последовательности случайных чисел, вырабатываемых предлагаемым генератором, было произведено с помощью пакета статистических тестов NIST. Тестирование показало, что последовательность бит имеет признаки действительно случайной числовой последовательности, но не является таковой в силу того, что отсутствует равномерность распределения случайных чисел в последовательности. Данный недостаток возможно исправить, например, используя LFSR (Linear feedback shift register) в качестве средства сжатия последовательности.

Предлагаемая схема может быть использована не только для генерирования ДСЧП, но и для решения задачи идентификации ПЛИС. Например, если по значениям, которые фиксируются в режиме SRAM-PUF вычислить сигнатуру и использовать ее как идентификатор.

1. Иванюк, А. А. Проектирование встраиваемых цифровых устройств и систем / А. А. Иванюк. – Минск: Бестпринт, 2012. – 338 с.

Заливако Сергей Сергеевич, магистрант кафедры интеллектуальных информационных технологий БГУИР, zalivako@bsuir.by.

Научный руководитель: Иванюк Александр Александрович, заведующий кафедрой вычислительных методов и программирования БГУИР, доктор технических наук, доцент, ivaniuk@bsuir.by.