РЕАЛИЗАЦИЯ ФИЗИЧЕСКИ НЕКЛОНИРУЕМОЙ ФУНКЦИИ НА LUT-БЛОКАХ FPGA

Иванюк А. А., Заливако С.С.
Кафедра информатики, Белорусский государственный университет информатики и радиоэлектроники
ООО "СК хайникс мемори солюшнс Восточная Европа"
Минск, Республика Беларусь
E-mail: ivaniuk@bsuir.by, sergey.zalivako@sk.com

В данной работе рассматривается схемотехническая реализация физически неклонируемой функции (ФНФ) на LUT-блоках кристаллов FPGA. Новый тип ФНФ может быть использован для построения схем уникальной идентификации цифровых устройств, реализованных на FPGA, и для схем источника цифрового шума для задач генерирования случайных чисел. Предложенная схема ФНФ отличается от существующих решений малыми аппаратурными затратами, легко масштабируется под произвольную разрядность и может быть реализована на различных типах FPGA.

Введение

Физически неклонируемые функции (ФНФ) являются базовыми примитивами для физической криптографии, которая основана на использовании случайных, уникальных, неповторимых, непредсказуемых физических характеристик интегральных схем. Основными областями применения ФНФ является уникальная неклонируемая идентификация и генерирование истино случайных числовых последовательностей. На основе этих двух направлений ведутся работы по реализации безопасной аутентификации цифровых устройств, реализации аппаратных водяных знаков и отпечатков пальцев, защите от нелегального использования и клонирования цифровых интегральных схем [1,2].

В данной работе предлагается новая компактная схема ФНФ, сочетающая в себе поведение двух известных типов ФНФ: ФНФ статического ОЗУ и ФНФ кольцевого генератора. Схемотехнически предложенная ФНФ состоит из одного мультиплексора с конфигурацией 2x1 и одного инвертора. Показано, что для реализации подобной схемы на FPGA необходим один LUT-блок.

В следующих разделах описана схемотехника предложенной ФНФ, режимы ее функционирования, особенности реализации на FPGA. Приведены экспериментальные данные по функционированию реализованной схемы.

I. Схемотехника предлагаемой ФНФ

За основу новой схемы ФНФ была взята схема управляемого кольцевого генератора, вырабатывающая выходной сигнал в форме меандра с уникальной невоспроизводимой частотой [1]. В общем случае подобная схема включает в себя схему кольцевого генератора, состоящую из $2k+1$ ($k \in N_0$) последовательно соединенных инверторов и цепи обратной связи, включающую управляющий вентиль, как правило двухвходовой логический элемент И, ко входам которого подключена линия обратной связи генератора и линия управляющего сигнала EN. Выход Q такой схемы может быть подключен к выходному полюсу одного из инверторов в цепи обратной связи. При значении управляющего сигнала $EN = 1$ схема генерирует импульсы на выходе Q с уникальной частотой F_Q, результат анализа которой может быть использован для генерации случайных чисел либо для построения уникального идентификатора. В случае $EN = 0$ схема прекращает генерацию импульсов и на ее выходе будет сформирован сигнал $Q = 0$.

Заменим управляющий вентиль в данной схеме на схему двухвходового мультиплексора, как это показано на рисунке 1.

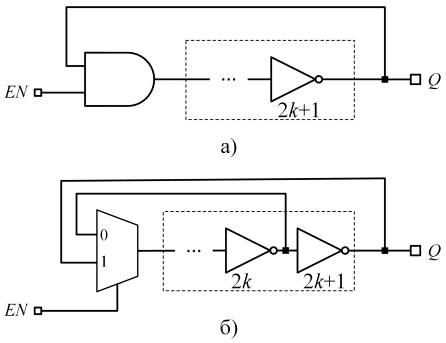

Рис. 1 – Схема управляемого кольцевого генератора (а) и предлагаемая схема ФНФ (б).

Управляющий сигнал EN подается на селективный вход мультиплексора, который обеспечивает две конфигурации цепи обратной связи: конфигурацию кольцевого генератора ($EN = 1$) и конфигурацию бистабильного элемента ($EN = 0$).

Рассмотрим подробнее функционирование предложенной схемы.

1. *Режим инициализации.* В данном режиме, при удержании $EN = 0$, схема в конфигурации бистабильного элемента хранит непредсказуемое значение, которое можно наблюдать на выходе Q. Поведение схемы в этом режиме аналогично ФНФ типа статическое ОЗУ. Генерируемое выход-

ное значение при этом можно использовать для получение уникального неклонируемого идентификатора.

2. *Режим кольцевого генератора.* В данном режиме схема функционирует при удержании $EN = 1$, при этом в цепи обратной связи, соединяющей выход схемы с единичным входом мультиплексора, включено нечетное количество инверторов, а на выходе Q вырабатывается сигнал в виде меандра с уникальной частотой, обусловленной структурными особенностями всех элементов схемы и их проводящих линий.
3. *Режим хранения.* В этот режим схема переходит при переключении управляющего сигнала EN из 1 в 0. При этом в цепи обратной связи конфигурируется четное число инверторов и схема становится эквивалентной схеме бистабильного элемента.

II. Реализация ФНФ на FPGA

Реализация произвольной комбинационной схемы на FPGA осуществляется при помощи LUT-блоков. Предложенная схема ФНФ в минимальной ее конфигурации ($k = 0$) может быть реализована на одном LUT-блоке. При этом, для уменьшения аппаратурных затрат, функция инвертора может быть перенесена в конфигурацию LUT. Современные FPGA, такие как Xilinx Artix-7 имеют в своем составе 6-входовые LUT-блоки, что может быть использовано для расширения реализации предложенной ФНФ. На рисунке 2 приведены схемы упаковки ФНФ в технологические блоки LUT-3 и LUT-6.

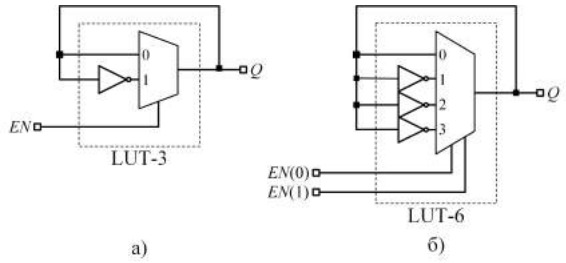

Рис. 2 – Схема упаковки ФНФ на блоках LUT-3 (а) и LUT-6 (б)

В модифицированной схеме ФНФ на LUT-6 вместо сигнала EN используются два селективных сигнала $EN(0)$ и $EN(1)$, определяющие следующие режимы функционирования: $EN = 00$ – режим бистабильного элемента, $EN = \{01, 10, 11\}$ – режимы трех принципиально различных кольцевых генераторов, вырабатывающих сигналы с различными частотами в зависимости от значения EN: $F_Q^{01} \neq F_Q^{10} \neq F_Q^{11}$.

Для реализации данной схемы на LUT-6 была использована FPGA Xilinx Artix-7 XC7A100T, входящая в состав платы быстрого прототипирования Digilent NEXYS 4.

III. Анализ экспериментальных данных

Для проведения экспериментов были собраны 16 схем ФНФ на LUT-6 блоках с общим управлением по входным линиям EN от устройства управления на основе софт-процессора MicroBlaze и UART-компоненты, посредством которой данные передавались для анализа от платы NEXYS 4 на рабочую станцию.

В ходе проведенных экспериментов было установлено, что только две из 16 ФНФ-схем (схемы с индексом 2 и 3) вырабатывают нестабильные значения в режиме инициализации. Вероятности появления единичного символа для этих схем следующие: $P_1^2 = 0,10$ и $P_1^3 = 0,49$, что свидетельствует о возможном применении данной схемы ФНФ для построения неклонируемых идентификаторов цифровых устройств.

На рисунке 2 приведены значения вероятностей появления единичного символа в трех режимах кольцевых генераторов для всех 16 схем.

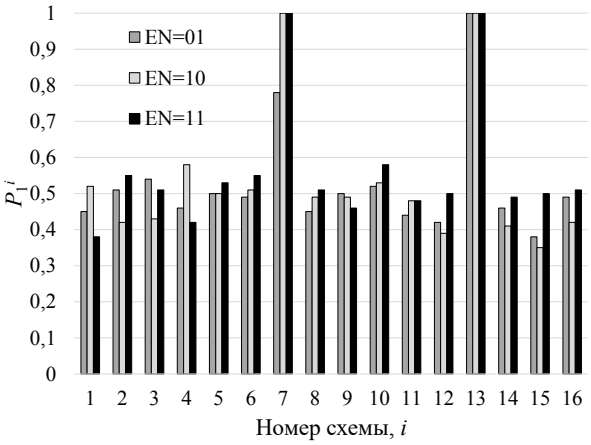

Рис. 3 – Значения вероятностей P_1^i для трех режимов схемы ФНФ

IV. Заключение

В работе предложена компактная схемотехническая реализация ФНФ, использующая ресурсы одного блока LUT-6 кристалла FPGA Xilinx Atrix-7. Планируются дальнейшие исследования характеристик предложенной ФНФ и разработка схем генерирования уникальных идентификаторов и случайных числовых последовательностей на ее основе.

V. Список литературы

1. Suh, G. E. Physical unclonable functions for device authentication and secret key generation / G. E. Suh, S. Devadas // ACM/IEEE Design Automat. Conf. (DAC'2007). – San Diego, USA, 2007. – P. 9–14.
2. The bistable ring PUF: A new architecture for strong physical unclonable functions / Q. Chen [et al.] // Proc. IEEE Int. Sympos. on Hardw. Orient. Secur. and Trust (HOST'11). – San Diego, USA, 2011. –P. 134–141.