ИСПОЛЬЗОВАНИЕ КОНФИГУРИРУЕМЫХ КОЛЬЦЕВЫХ ГЕНЕРАТОРОВ ДЛЯ ИДЕНТИФИКАЦИИ ЦИФРОВЫХ УСТРОЙСТВ ПРОГРАММИРУЕМОЙ ЛОГИКИ

П. А. Сечко, А. А. Иванюк
Кафедра инженерной психологии и эргономики, кафедра информатики, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: paul.setchko@icloud.com, ivaniuk@bsuir.by

В данной работе рассмотрен способ идентификация цифровых устройств при помощи конфигурируемого кольцевого генератора (RO, ring oscillator) в качестве схемной реализации физически неклонируемой функции (PUF, physically unclonable function). Методика идентификации основана на сравнении частот импульсов, вырабатываемых функционально и структурно идентичными схемами RO PUF. В ходе работы была проведена симуляция работы генераторов, реализованных на семействе FPGA Artix-7, а также получены и проанализированы частотные характеристики их выходных сигналов.

Введение

Идентификация цифровых устройств решает вопросы защиты программно-аппаратных решений, разработанных на базе этих цифровых устройств, от клонирования (несанкционированного повторения и использования) [1] или внедрения аппаратных троянов, изменяющих функционирование, нарушающих или снижающих работоспособность или передающих секретную информацию из устройства. Также возможно определение легальности компонент сложной системы для защиты от несанкционированной замены компонент на аналогичные с точки зрения интерфейсов и логики взаимодействия с внешним миром, но нарушающих структуру и функционирование устройства.

Для решения задачи идентификации в проектное описание часто внедряют идентификаторы, наличие которых позволяет использовать их для адресации FPGA в сложных системах, в качестве ключей в системах шифрования и в реализации алгоритмов защиты от несанкционированного использования [1]. Также для усложнения нелегального копирования может использоваться лексическая обфускация описания устройства. Однако популярным вектором атаки является клонирование bit-образа и обратное проектирование описания устройства с целью модификации и изучения его функционирования. Таким образом, необходимо решение, идентифицирующее устройство, но не привязанное к значениям, задаваемым при производстве. Таким решением могут являться физически неклонируемые функции (PUFs, physically unclonable functions).

I. Физически неклонируемые функции

Физически неклонируемая функция – это функция, реализованная с помощью физической системы, обладающая следующими свойствами [2]:

- по воздействию на физическую систему легко получить ответ – результат работы функции (реакцию физической системы);
- функцию сложно воспроизвести, вычислительно сложно математически смоделировать или скопировать (свойство неклонируемости);
- на уникальный запрос функция должна возвращать уникальный ответ.

Физически неклонируемые функции являются однонаправленными: по ответу практически невозможно восстановить запрос.

Результат работы физически неклонируемых функций, реализованных на FPGA, зависит от физического расположения логических вентилей, соответствующих функции на устройстве, а также от связей между вентилями и задержек распространения сигналов внутри интегральной схемы, связанных с непредсказуемыми и невоспроизводимыми отклонениями в физической структуре схемы. Важным пунктом является неуправляемость перечисленных выше отклонений относительно действий разработчика.

На рис. 1 и рис. 2 представлены соответственно функциональная модель и структурная схема кольцевого генератора, реализованного в ходе эксперимента по идентификации.

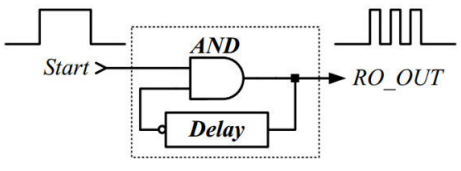

Рис. 1 – Обобщённая функциональная модель кольцевого генератора

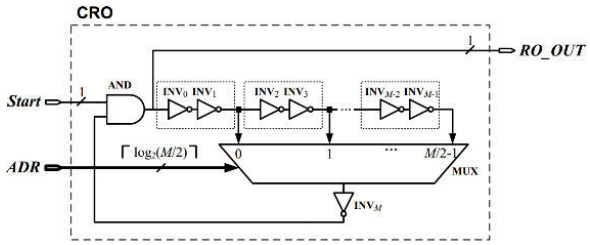

Рис. 2 – Структурная схема конфигурируемого кольцевого генератора

II. Эксперимент по идентификации

В реализованной в эксперименте схеме число M равняется 32, и цепь обратной связи содержит 16 пар инверторов, выход каждой из которых подключён к соответствующему входу мультиплексора MUX. Коммутация выхода мультиплексора с его 16 входами определяется битом, установленным в соответствующем разряде входного 16-битного сигнала, поступающего по шине ADR. Выход мультиплексора соединен с инверсным входом логического вентиля AND, выход которого является выходным портом генератора RO_OUT.

Зависимость частоты выходного сигнала (в МГц) от длины линии задержки, сформированной из пар инверторов, продемонстрирована на рисунке 3.

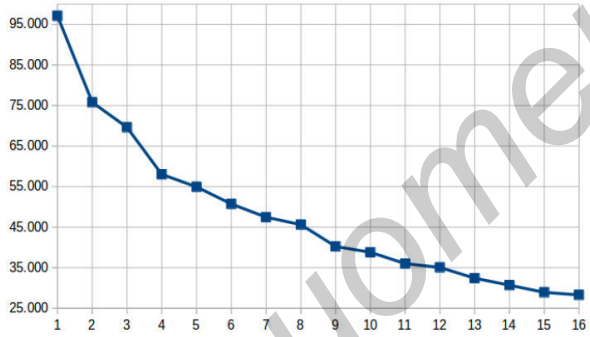

Рис. 3 – Зависимость частоты выходного сигнала кольцевого генератора от количества пар инверторов в линии задержки

Как видно, с ростом длины линии задержки частота выходного сигнала падает.

В случае, когда изменяется описание устройства, изменяется также и геометрическое расположение кольцевого генератора на кристалле, что, в свою очередь, приводит к изменению частоты выходного сигнала. Это особенность можно использовать для защиты от несанкционированного изменения реализации устройства.

В таблице 1 представлена разница между минимальным и максимальным значениями кольцевых генераторов, работающих одновременно на FPGA Artix-7 и обладающих одинаковым количеством блоков инверторов в линии задержки, но разнесённых на кристалле геометрически в результате синтеза устройства из описания.

Таблица 1 – Разница между значениями геометрически разнесённых кольцевых генераторов с линией задержки одинаковой длины

блоки инверторов	1	2	3	4
разница, MHz	41.295	27.735	25.301	17.895
	5	6	7	8
	14.671	8.173	7.819	8.941
	9	10	11	12
	7.921	6.086	7.112	6.721
	13	14	15	16
	5.457	4.397	4.038	4.564

График данной разницы представлен на рисунке 4.

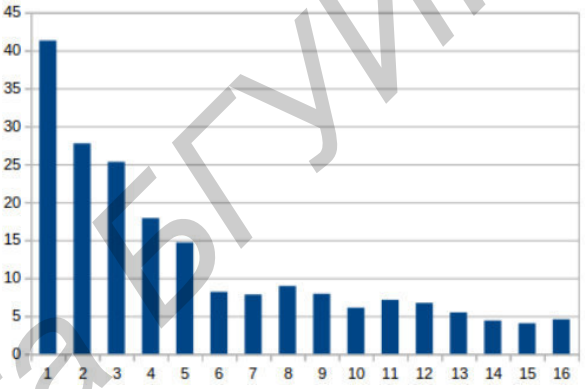

Рис. 4 – График разницы между значениями выходной частоты идентичных разнесённых геометрически кольцевых генераторов

Для подсчёта частоты используются бинарные счётчики. Очевидно, что при большой амплитуде частоты выходного сигнала задача идентификации цифрового устройства решается проще, т.к. существует больший интервал, в пределах которого частота считается неизменной. Однако при высоких частотах значения на выходе бинарного счётчика будут отличаться от реальных ввиду «проскакивания» значений. Данный эффект обусловлен переходными процессами.

III. Вывод

Проведённый эксперимент подтверждает возможность использования кольцевых генераторов для идентификации проектов для ПЛИС. Для решения задачи идентификации необходимо определить длину линии задержки, которая будет как обеспечивать максимальную точность показаний бинарного счётчика, так и позволять однозначно определить, было ли подвержено изменениям начальное описание компоненты.

Список литературы

1. Иванюк, А. А. Проектирование встраиваемых цифровых устройств и систем : монография / А. А. Иванюк – Минск : Бестпринт, 2012. – 337 с.
2. Физически неклонируемые функции [Электронный ресурс] / Encyclopedia of Theoretical and Applied Cryptography – Режим доступа: http://cryptowiki.net/. – Дата доступа: 29.08.2016.