ЛОГИЧЕСКОЕ ПРОЕКТИРОВАНИЕ

УДК 681.325

А.А. Иванюк

ПРИМЕНЕНИЕ КОНФИГУРИРУЕМЫХ ГЕНЕРАТОРОВ ИМПУЛЬСОВ ДЛЯ ИДЕНТИФИКАЦИИ ПЛИС

Рассматривается возможность применения конфигурируемых генераторов цифровых импульсов в качестве аппаратной реализации физически неклонируемых функций для решения задач идентификации программируемых логических интегральных схем (ПЛИС) типа FPGA. Приводятся и анализируются результаты экспериментальных исследований генераторов импульсов, реализованных для FPGA Xilinx SPARTAN-3E.

Введение

Современные ПЛИС способны реализовывать практически произвольную пользовательскую логику: от простейшего цифрового устройства управления до многоядерной вычислительной системы [1]. Наличие множества САПР цифровых устройств, языков высокого уровня описания цифровой аппаратуры, доступность на рынке и низкая стоимость делают ПЛИС не только технологической платформой для макетирования цифровых интегральных схем, но и реальной альтернативой заказных СБИС. Свойство реконфигурируемости ПЛИС совместно с большим разнообразием встроенных модулей привлекает внимание не только разработчиков специализированного оборудования, но и крупных корпораций [2]. Расширяющийся мировой рынок готовых решений на основе ПЛИС ставит перед разработчиками множество новых задач, в том числе и задачи защиты авторских прав на проектируемые и реализованные компоненты интеллектуальной собственности. Одним из направлений в этой области является исследование и применение так называемых физически неклонируемых функций (ФНФ, или PUF – от англ. Physical Unclonable Function) [3–5], которые основаны на использовании непредсказуемых и невоспроизводимых отклонений в физической структуре интегральной схемы при ее изготовлении. Подобные отклонения в первую очередь сказываются на задержках распространения сигналов внутри интегральной схемы, а методики, способные регистрировать такие отклонения, лежат в основе аппаратных PUF.

В данной статье предлагается методика построения цифровых идентификаторов ПЛИС, основанная на реализации модифицированного метода RO-PUF (Ring Oscillator PUF) [5–8], заключающегося в сравнении числа цифровых импульсов, вырабатываемых двумя функционально идентичными кольцевыми генераторами.

1. Физически неклонируемые функции на основе кольцевых генераторов

Формальные определения и основные методы аппаратных реализаций ФНФ приведены в работе [5]. В данной статье будем основываться на реализации ФНФ на базе кольцевых генераторов импульсов RO-PUF с целью получения уникальных идентификаторов ПЛИС типа FPGA. Основная идея реализация RO-PUF заключается в сравнении числа вырабатываемых импульсов несколькими идентичными генераторами [6]. На рис. 1 представлена схема реализации ФНФ типа RO-PUF, состоящая из n кольцевых генераторов ($RO_0 \ldots RO_{n-1}$), двух мультиплексоров (MUX_0 и MUX_1), двух m-разрядных двоичных счетчиков (CNT_0 и CNT_1) и схемы сравнения двух m-разрядных двоичных чисел (CMP).

Бит ответа R (Response) формируется путем сравнения значений числа зарегистрированных импульсов, вырабатываемых двумя кольцевыми генераторами, посредством счетчиков CNT_0 и CNT_1. Пара сравниваемых генераторов из $\frac{1}{2}(n^2 - n)$ возможных пар выбирается

путем подачи $\left\lceil \log_2(\frac{1}{2}(n^2-n)) \right\rceil$-разрядного двоичного запроса C (Challenge) на адресные входы мультиплексоров MUX_0 и MUX_1. Временной интервал, в течение которого происходит регистрация импульсов, задается продолжительностью удержания сигнала разрешения в состоянии ‘1’ (*Enable* = ’1’).

Таким образом, приведенная схема реализует необратимую функцию $PUF_{RO}(C_j) = R_j$.

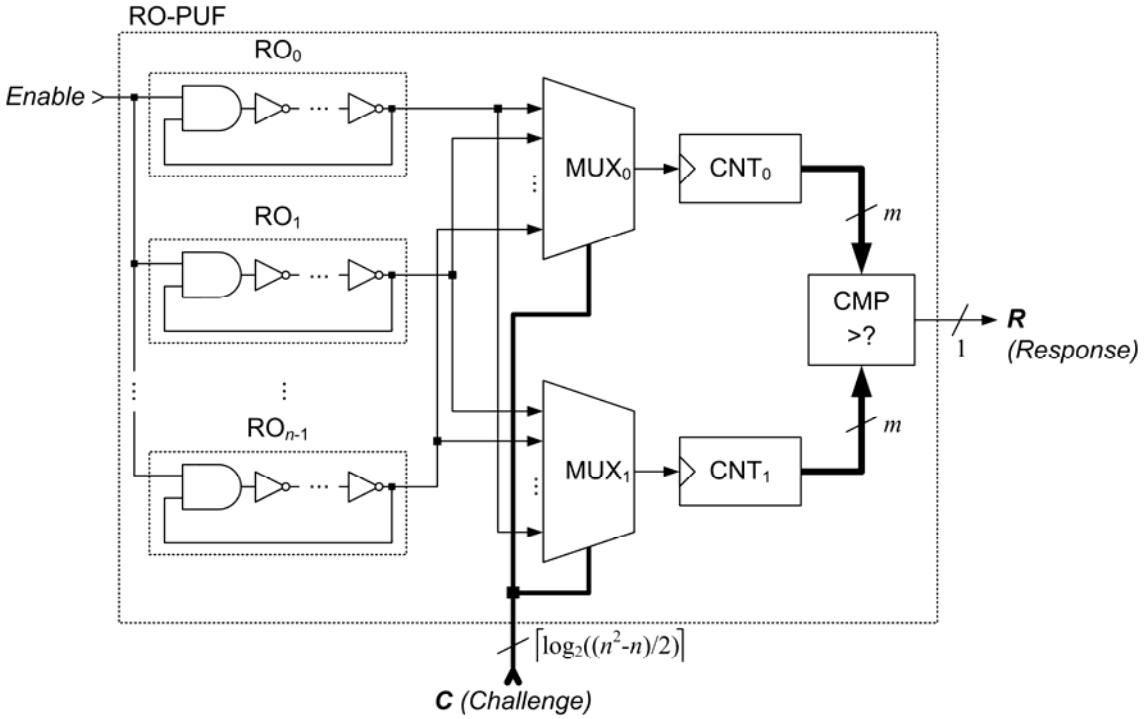


Рис. 1. ФНФ типа RO-PUF

Неповторимость физической реализации каждого генератора RO_i позволяет формировать уникальные фиксированные битовые последовательности на выходе R в зависимости от двоичных запросов C. Как показал ряд экспериментов [7–9], реализация ФНФ типа RO-PUF является наиболее предпочтительной для ПЛИС типа FPGA, так как основывается не на сравнении идеально симметричных путей [5], которые в принципе невозможно реализовать на FPGA [9], а на частотных характеристиках кольцевых генераторов.

Многие производители интегральных схем решают задачу идентификации СБИС путем реализации специальных регистров хранения уникальных идентификаторов (серийных номеров), значения которых, как правило, единожды задаются на этапе производства и в дальнейшем доступны только для чтения. Наличие подобного рода идентификаторов позволяет проектировщикам цифровых систем эффективно решать многие задачи, например, такие как адресация СБИС, подключенных к единой информационной магистрали; использование идентификаторов в качестве открытого ключа при реализации алгоритмов шифрования; реализация методов и алгоритмов защиты от несанкционированного использования и т. д. Однако большинство серийно выпускаемых ПЛИС не содержат регистров уникальных идентификаторов, что затрудняет разработчикам цифровых систем решение вышеперечисленных задач. В свою очередь, пользовательская реализация соответствующих регистров ресурсами ПЛИС не защищена от клонирования (несанкционированного повторения и использования) как во время создания проектных описаний, например исходных HDL-кодов, так и после реализации в аппаратуре.

Наличие заведомо асимметричных путей в ПЛИС затрудняет применение многих физически неклонируемых функций, таких, например, как ФНФ типа Arbiter PUF [10]. В настоящей работе предлагается методика получения уникальных идентификаторов FPGA, основанная на

модифицированной аппаратной реализации ФНФ типа RO-PUF. Теоретически формирование уникального идентификатора на основе схемы, представленной на рис. 1, возможно путем генерирования бинарной последовательности определенной длины на выходе *R* при подаче соответствующих значений на вход *C*. При этом сравнению подлежат не пути прохождения сигналов, а частотные характеристики кольцевых генераторов.

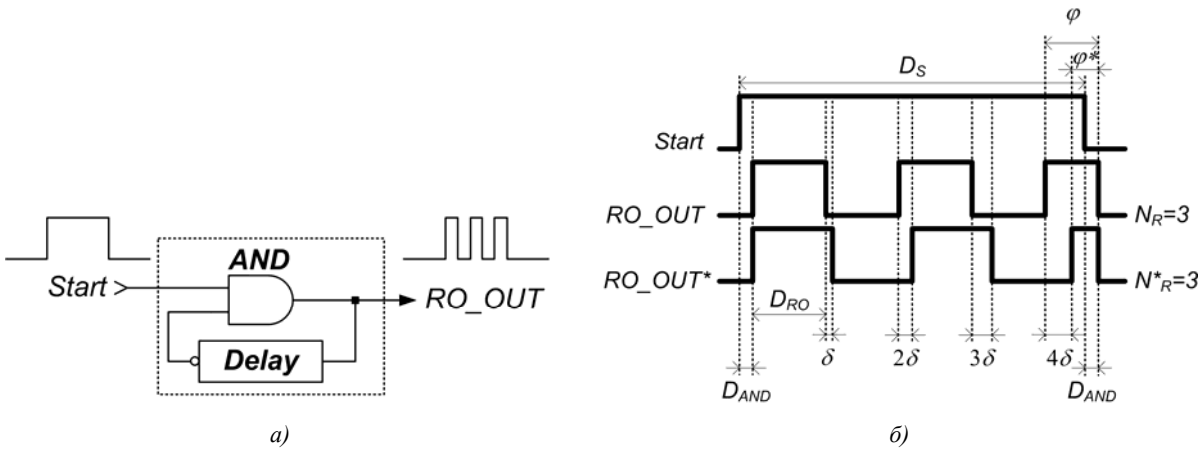
2. Кольцевой генератор цифровых импульсов

Функциональная схема кольцевого генератора представляет собой нечетное число последовательно соединенных инверторов, при этом выход последнего инвертора, являющийся выходом самого генератора, соединен с входом первого, образуя цепь обратной связи (кольцо). Для определения конкретного начального состояния генератора и обеспечения его управляемости можно добавить в цепь обратной связи двухвходовой логический элемент *AND*, первый вход которого является входом разрешения функционирования генератора, а второй вход участвует в формировании кольца (см. рис. 1).

Представленный на рис. 2, *а* генератор имеет входную линию сигнала разрешения функционирования *Start* и выходную линию цифровых импульсов *RO_OUT*. При нулевом значении сигнала *Start* генератор находится в состоянии ожидания, при этом сигнал на выходной линии принимает также нулевое значение. Функционирование генератора начинается при переключении уровня сигнала *Start* из значения ‘0’ в значение ‘1’ и продолжается весь период удержания в значении ‘1’. Количество вырабатываемых импульсов на выходе *RO_OUT* находится в прямой зависимости от продолжительности удержания сигнала на входе *Start* в значении ‘1’ и от задержки распространения выходного сигнала по цепи обратной связи, включающей логический вентиль *AND* и элемент задержки *Delay* (множества инверторов). Обозначим временной интервал удержания сигнала разрешения как D_S, а задержку распространения сигнала в цепи обратной связи генератора как $D_{RO} = D_{AND} + D_{Delay}$. Предположим, что счет вырабатываемых генератором импульсов производится цифровым двоичным счетчиком, стробируемым фронтом выходного сигнала *RO_OUT*. Если $D_{RO} \geq D_S$, генератор будет вырабатывать один единственный импульс продолжительностью D_S. В этом случае регистрируемое значение на счетчике будет равно $N_R = 1$. При условии, что $2D_{RO} < D_S$, счетчик будет регистрировать значение $N_R > 1$. Выразим значение D_S через временные параметры генератора:

$$D_S = D_{AND} + 2D_{RO}(N_R - 1) + \varphi - D_{AND} = 2D_{RO}(N_R - 1) + \varphi, \quad (1)$$

где значение φ удовлетворяет неравенствам $D_{AND} < \varphi < (2D_{RO} - D_{AND})$.



а) *б)*

Рис. 2. Кольцевой генератор импульсов: *а)* обобщенная функциональная модель; *б)* основные временные параметры

Будем рассматривать значение D_S как продолжительность временного окна измерения числа зарегистрированных импульсов N_R. Для двух сравниваемых генераторов, реализован-

ных на различных ПЛИС, временное окно измерений должно быть идентичным и легко масштабируемым.

Предположим, что сигнал *Start* вырабатывается для кольцевого генератора на основе внешнего стабильного и технологически независимого источника синхронизации, которым, например, может служить кварцевый осциллятор. Условимся, что осциллятор генерирует сигнал синхронизации в форме меандра с частотой F_{CLKG}. Тогда минимальное значение D_S времени удержания сигнала *Start* можно принять равным $\frac{1}{F_{CLKG}}$. В этом случае для увеличения значения D_S можно использовать аппаратные делители частоты F_{CLKG}, среди которых наиболее предпочтительными выглядят делители с коэффициентом деления $k = 2^i$, реализованные на двоичных счетчиках. При этом временное окно измерения числа импульсов может быть линейно масштабируемым относительно значения D_S. Например, для увеличения временного окна измерения в четыре раза ($k = 4$) можно использовать двухразрядный двоичный счетчик, на вход синхронизации которого поступает сигнал с частотой $F_{CLKG} = \frac{1}{D_S}$, а на выходе старшего разряда счетчика формируется сигнал *Start* продолжительностью $4D_S$.

Предположим, что измерение числа импульсов производится во временном интервале, кратном значению D_S. В этом случае (1) будет выглядеть следующим образом:

$$kD_S = 2D_{RO}(N_R(k) - 1) + \varphi(k),$$

где k – натуральное число, определяющее коэффициент масштабирования D_S; $N_R(k)$ – число зарегистрированных импульсов; $\varphi(k)$ – временной интервал, измеряемый от фронта последнего импульса и до момента окончания окна измерения. Покажем, что значение k непосредственно влияет не только на число регистрируемых импульсов кольцевых генераторов, но и на достоверность идентификации микросхем ПЛИС.

Выразим число регистрируемых импульсов в окне измерения продолжительностью kD_S:

$$N_R(k) = \left\lfloor \frac{kD_S - \varphi(k)}{2D_{RO}} \right\rfloor + 1. \qquad (2)$$

Предположим, что два генератора цифровых импульсов, реализованных на различных ПЛИС, имеют незначительные отличия, которые можно выразить увеличением задержки распространения сигнала по цепи обратной связи D^*_{RO} на некоторую малую величину $\delta << D_{RO}$, $D^*_{RO} = D_{RO} + \delta$ (рис. 2, *б*). Тогда согласно выражению (2) число регистрируемых импульсов второго генератора определяется как

$$N^*_R(k) = \left\lfloor \frac{kD_S - \varphi^*(k)}{2(D_{RO} + \delta)} \right\rfloor + 1.$$

При этом абсолютное значение разности чисел регистрируемых импульсов двух генераторов оценивается выражением

$$\Delta N_R(k) = \left| N_R(k) - N^*_R(k) \right| = \left\| \left\lfloor \frac{kD_S - \varphi(k)}{2D_{RO}} \right\rfloor - \left\lfloor \frac{kD_S - \varphi^*(k)}{2(D_{RO} + \delta)} \right\rfloor \right\| \approx \left\| \left\lfloor \frac{\varphi^*(k) - \varphi(k)}{2D_{RO}} \right\rfloor \right\| \qquad (3)$$

при условии, что $\delta << D_{RO}$.

Разницу значений $\varphi^*(k) - \varphi(k)$ можно представить в виде $2(N_R(k)-1)\delta$. С учетом, что $N_R(k) \approx \left\lfloor \frac{kD_S}{2D_{RO}} \right\rfloor + 1$, выражение (3) примет вид

$$\Delta N_R(k) \approx \left\| \left\lfloor \frac{\varphi^*(k) - \varphi(k)}{2D_{RO}} \right\rfloor \right\| \approx k \left\lfloor \frac{\delta D_S}{2D_{RO}^2} \right\rfloor. \quad (4)$$

Очевидно, что при малых значениях k разница (4) будет принимать нулевые значения. Установим экспериментальным путем, при каких значениях k (4) будет принимать стабильные ненулевые значения.

3. Структура конфигурируемого генератора импульсов

Для проведения эксперимента были выбраны идентичные цифровые системы Digilent Nexys-2 [11], в состав которых входят ПЛИС Xilinx SPARTAN-3E (XC3s500e-5FG320) [12]. Для возможности реализации генераторов импульсов с различными значениями D_{RO} была предложена функциональная цифровая модель (рис. 3).

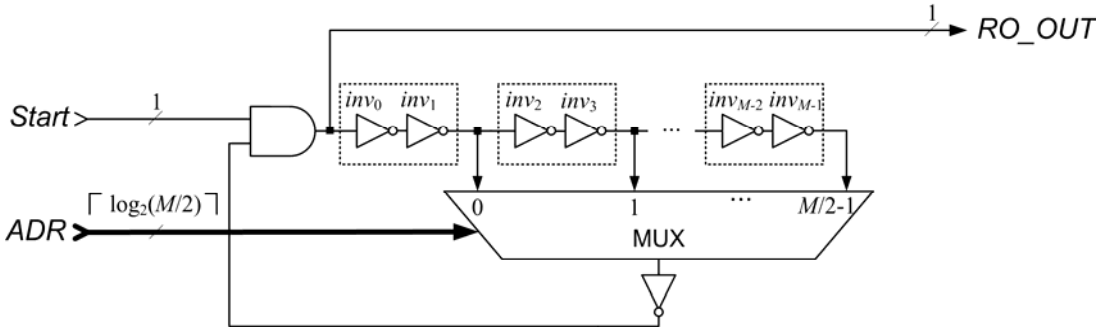


Рис. 3. Структура конфигурируемого цифрового генератора импульсов

Цепь обратной связи генератора содержит M инверторов, которые попарно сгруппированы. Выход каждой пары подключен к соответствующему входу мультиплексора MUX. Коммутация $M/2$ входов мультиплексора с его выходным портом определяется двоичным значением, подаваемым на $\lceil \log_2(M/2) \rceil$-разрядную адресную шину *ADR*. Выход мультиплексора соединен с инверсным входом логического вентиля *AND*, выход которого является выходным портом генератора *RO_OUT*. Таким образом, представленная схема реализует $M/2$ кольцевых генераторов с различными фиксированными значениями D_{RO}.

Предлагается использовать схему конфигурируемого генератора импульсов в качестве схемы, реализующей физически неклонируемую функцию, аргументами которой являются продолжительность импульса на входе *Start* и значение на входной шине *ADR*. Значение физически неклонируемой функции есть число зарегистрированных импульсов на выходном порте *RO_OUT*:

$$PUF_{CRO}(kD_S, ADR) = N_R(k).$$

Для аппаратной реализации представленной структуры конфигурируемого генератора импульсов было спроектировано цифровое устройство, позволяющее устанавливать различные фиксированные значения kD_S и *ADR* с возможностью регистрации вырабатываемых значений $N_R(k)$. Устройство включает в себя следующие основные блоки: генератор стартового импульса SPG, конфигурируемый генератор цифровых импульсов CRO, счетчик импульсов CNT, контроллер светодиодных индикаторов SLC. Устройство, реализуемое на ПЛИС FPGA XC3s500e-5FG320, управляется генератором системных импульсов CLKG (F_{CLKG} = 50 МГц), аппаратными

кнопками BNT1 (источник асинхронного сигнала инициализации) и BTN2 (управление режимом отображения результата) и тремя переключателями SW(2:0), входящими в состав цифровой системы Digilent Nexys-2 (рис. 4).

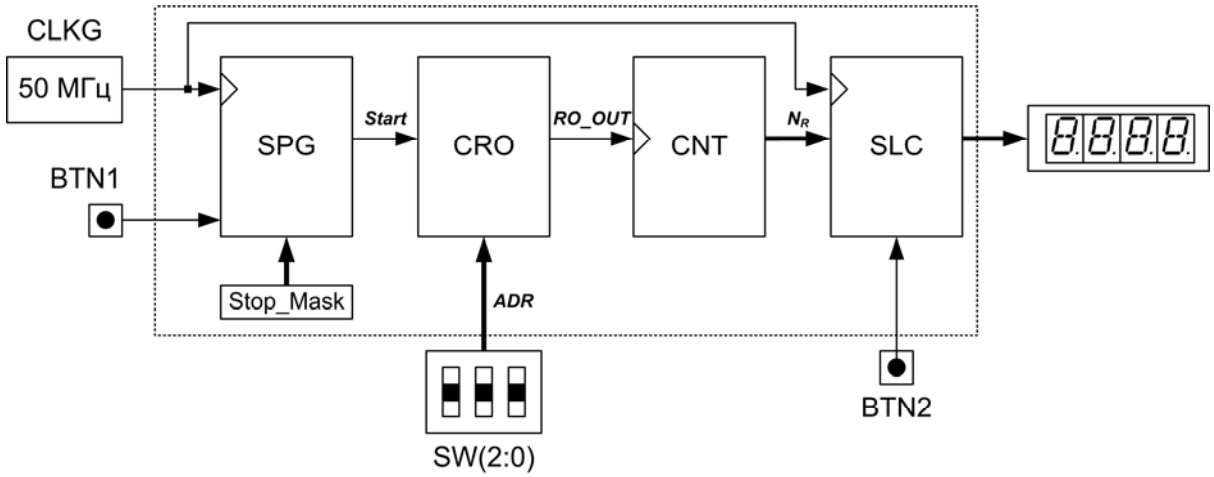


Рис. 4. Структура реализованного цифрового устройства в системе Digilent Nexys-2

Приведенная структура конфигурируемого генератора была спроектирована и описана с помощью САПР Xilinx ISE WebPack 13.1 на языке VHDL с учетом конструктивных особенностей системы Digilent Nexys-2 [13]. Для исключения логической оптимизации конфигурируемого генератора импульсов все его функциональные блоки (в том числе и инверторы) были описаны в качестве отдельных компонент, а в параметрах программной системы синтеза Xilinx ISE был принудительно установлен флаг Keep Hierarchy в положение Yes (закладка Synthesize :: Process Properties : Synthesis Options : Keep Hierarchy) [14]. По результатам синтеза VHDL-описания аппаратура генератора импульсов занимает 97 slice-блоков кристалла Xilinx SPARTAN-3E, что составляет около 2 % от всех ресурсов данной ПЛИС (46 slice-блоков при этом было использовано для реализации контроллера семисегментных индикаторов SLC).

4. Постановка эксперимента и анализ результатов

Для проведения эксперимента были взяты две идентичные системы *B* и *B** (Digilent Nexys-2 с ПЛИС FPGA XC3s500e-5FG320), для которых были определены следующие ограничения:

1. Питание обеих систем (+3,3 В) осуществлялось от одного источника питания системного блока ПЭВМ класса Pentium Dual-Core посредством интерфейсных кабелей USB (+5,0 В) при помощи идентичных регуляторов напряжения LTC1765 [11], входящих в состав систем *B* и *B**.

2. Обе ПЛИС были сконфигурированы одной битовой последовательностью, сгенерированной САПР ISE WebPack на основе общего VHDL-проекта при абсолютно одинаковых параметрах синтеза, размещения, трассировки соединений и конфигурации.

3. Процедура конфигурирования ПЛИС осуществлялась посредством программного обеспечения Digilent Adept 2.5.

4. Выработка системной частоты, на основании которой осуществлялось генерирование сигнала *Start*, производилась идентичными генераторами AGXO 75IL (50 МГц).

5. Процессы инициализации и функционирования конфигурируемых генераторов импульсов осуществлялись одновременно.

Обобщая вышесказанное, можно сделать предположение о равных внешних условиях проведения эксперимента для двух функционально идентичных цифровых систем. Эксперимент проводился в несколько этапов. На первом этапе для выбранных значений $k = 2^i$ ($i = 0, \ldots, 10$) осуществлялся мониторинг числа сгенерированных импульсов $N_R(k)$ двумя конфигурируемыми генераторами.

Из графиков на рис. 5 видно, что первое ненулевое значение разница импульсов принимает для $k = 2^4$ и $ADR = \{2,7\}$. При этом число импульсов для значения $ADR = 2$ составляет $N_R(16) = 23$ и $N_R^*(16) = 22$. С увеличением значения k наблюдается линейное увеличение разницы регистрируемых импульсов для всех значений ADR.

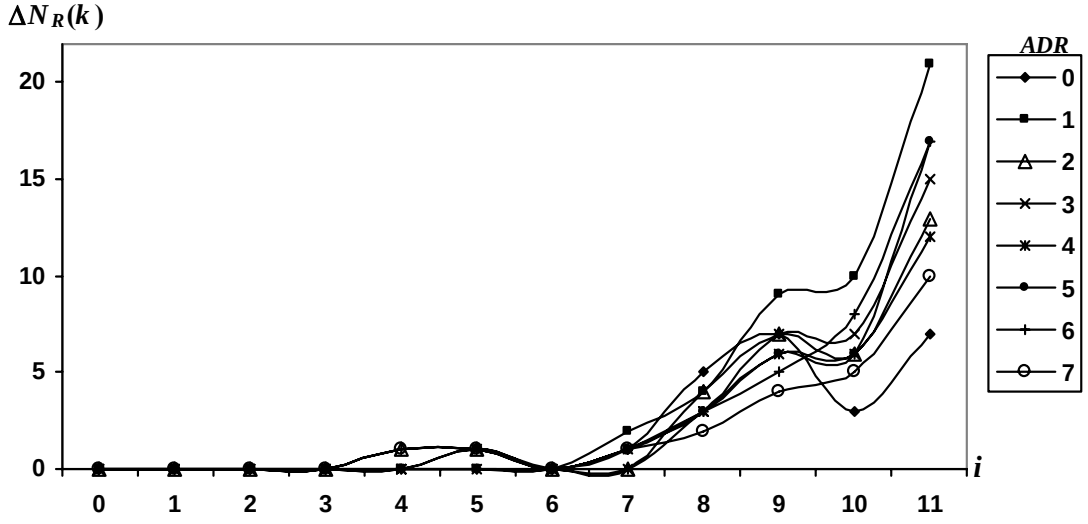


Рис. 5. Значения разницы $\Delta N_R(k)$ для $k = 2^i$ и всех возможных значений ADR

В табл. 1 приведены экспериментальные данные, полученные для значения $k = 2^{10}$ ($kD_S = 2^{10} * 20 = 20\,480$ нс). Здесь и далее по тексту значения чисел регистрируемых импульсов представлены в шестнадцатеричном формате.

Таблица 1

Экспериментальные данные для $kD_S = 20\,480$ нс

Параметры	*ADR*							
	0	1	2	3	4	5	6	7
$N_R(k)$	7fc	671	55d	4bb	40f	396	33d	2f2
$N_R^*(k)$	7f8	666	557	4b3	408	38f	334	2ed
$D_\Delta(k)$	4	11	6	8	7	7	9	5
$H_\Delta(k)$	1	4	2	1	3	3	2	5

Значения чисел зарегистрированных импульсов $N_R(k)$ и $N_R^*(k)$ соответствуют первой B и второй B^* цифровым системам. Значение арифметической разницы импульсов обозначено как $D_\Delta(k)$, а значение расстояния Хэмминга как $H_\Delta(k)$. Для данного эксперимента средние значения арифметической разницы и расстояния Хэмминга равны соответственно $\lfloor \overline{D_\Delta}(k) \rfloor = 7$ и $\lfloor \overline{H_\Delta}(k) \rfloor = 2$.

Далее для каждого значения ADR и выбранного $kD_S = 20\,480$ нс было проведено 100 последовательных экспериментов для выявления отклонений в регистрируемых значениях $N_R(k)$ и $N_R^*(k)$. Отклонения в регистрируемых значениях возможны в силу наличия технологических вариаций и выработки генераторами импульсов с частотой, превосходящей рабочую частоту функционирования ПЛИС [15, 16]. Так, для значений $ADR = 0$ и $k = 2^{10}$ регистрируются порядка 2040 импульсов, что соответствует частоте 100 МГц, вдвое превышающей частоту функционирования XC3s500e-5FG320.

В качестве эталонного регистрируемого значения числа импульсов были выбраны значения, наиболее часто встречаемые в 100 последовательных экспериментах. Следует от-

метить, что для всех возможных значений *ADR* абсолютная величина отклонений не превышала 2 (рис. 6).

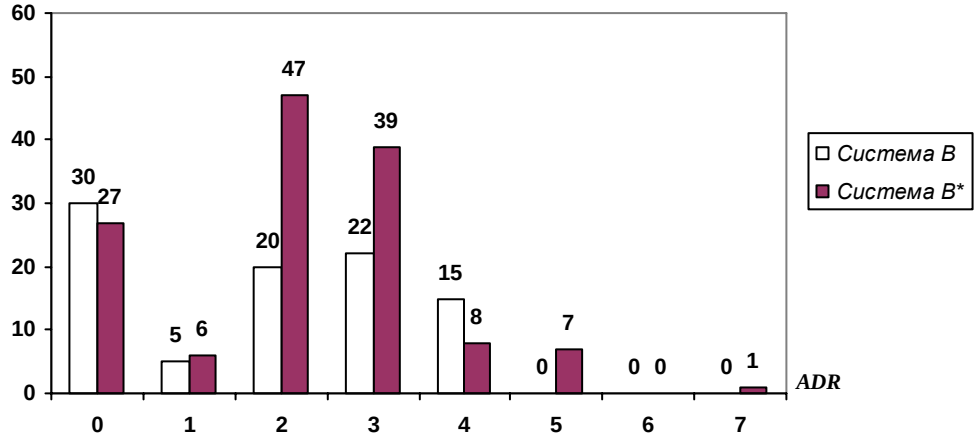


Рис. 6. Распределение числа отклонений от эталонного значения регистрируемых импульсов

Например, для значения *ADR* = 4 генератор импульсов, реализованный на системе *B*, имеет следующее распределение значений по $N_R(k)$: 410 (85 %), 40f (10 %), 411 (5 %), а генератор, реализованный на системе *B**, по $N_R^*(k)$: 409 (92 %), 40a (7 %), 408 (1 %). С учетом полученных данных сформируем карты вероятностей появления символа ‘1’ на 11 значимых разрядах двоичных представлений чисел $N_R(k)$ и $N_R^*(k)$ (табл. 2).

Таблица 2

Карты вероятностей появления символа ‘1’

Параметры	Номер двоичного разряда										
	10	9	8	7	6	5	4	3	2	1	0
$N_R(k)$	1,0	0	0	0	0	0	0,9	0,1	0,1	0,1	0,15
$N_R^*(k)$	1,0	0	0	0	0	0	0	1,0	0	0,07	0,92

Значения зарегистрированных импульсов, в том числе и значения вероятностей появления символа ‘1’ на различных позициях, могут быть использованы для построения уникального идентификатора ПЛИС, реализующего конфигурируемый генератор цифровых импульсов. Например, приведенную карту вероятностей преобразуем в соответствии с мажоритарным принципом, при котором все значения вероятности меньше 0,5 представим символом ‘0’, а остальные – символом ‘1’. При этом карты вероятностей трансформируются в двоичные идентификаторы (табл. 3).

Таблица 3

Двоичные идентификаторы цифровых систем

Параметры	Номер двоичного разряда										
	10	9	8	7	6	5	4	3	2	1	0
ID(*B*)	1	0	0	0	0	0	**1**	**0**	0	0	**0**
ID(*B**)	1	0	0	0	0	0	**0**	**1**	0	0	**1**

Как видно из табл. 3, значения идентификаторов *ID*(*B*) и *ID*(*B**) различимы на трех разрядах, что коррелируется с экспериментальными данными, приведенными в табл. 1. Реализация подобного алгоритма вычисления двоичных идентификаторов не всегда может быть оправдана с точки зрения как аппаратурных, так и временных ресурсов.

В качестве альтернативы предлагается следующий алгоритм, основанный на увеличении значения D_S и разрядности счетчика *CNT* (см. рис. 4), при которых можно выделить фиксиро-

ванные двоичные разряды чисел $N_R(k)$ и $N_R^*(k)$ с единичными значениями вероятности появления символов ‘1’ и ‘0’.

Экспериментальным путем было установлено, что для значения $kD_S = 2^{25} * 20 \cong 0{,}671$ с, 26-разрядного счетчика *CNT* и различных значений *ADR* десять старших двоичных разрядов чисел $N_R(k)$ и $N_R^*(k)$ имеют единичные вероятности появления символов ‘0’ и ‘1’ на фиксированных позициях (табл. 4).

Таблица 4

Экспериментальные данные для $kD_S \cong 0{,}671$ с ($k = 2^{25}$)

Параметры	*ADR*							
	0	1	2	3	4	5	6	7
$N_R(k)$	3d9	34e	2ce	26e	232	1e5	1a9	187
$N_R^*(k)$	3c8	340	2c1	260	224	1d9	19e	17b
$D_\Delta(k)$	17	14	13	14	14	12	11	12
$H_\Delta(k)$	2	3	4	3	3	4	5	6

Для данного эксперимента средние значения арифметической разницы и расстояния Хэмминга равны соответственно $\lfloor \overline{D_\Delta}(k) \rfloor = 13$ и $\lfloor \overline{H_\Delta}(k) \rfloor = 3$.

Проведенные эксперименты наглядно демонстрируют возможность применения конфигурируемых генераторов цифровых импульсов для построения уникальных идентификаторов ПЛИС. Для приближенной оценки степени различия идентификаторов для всех функционально идентичных ПЛИС из класса XC3s500e-5FG320 было осуществлено тестовое моделирование конфигурируемого генератора цифровых импульсов с учетом усредненных технологических параметров в симуляторе ISim, который входит в состав САПР Xilinx ISE. Для этого после успешно проведенного процесса размещения и трассировки (Place and Route) в меню Design была выбрана опция View-Simulate, а в качестве параметра этой опции было указано Post-Route. Симулятор ISim осуществляет параметрическое моделирование цифрового проекта ПЛИС с возможностью наблюдения значений сигналов в основных узлах размещенной схемы.

На рис. 7 представлена гистограмма распределения числа сгенерированных импульсов на реальных цифровых системах *B*/*B** и зарегистрированных в симуляторе ISim при следующих условиях: *ADR* = 7, $k = 2^i$, $i = 0, ..., 10$.

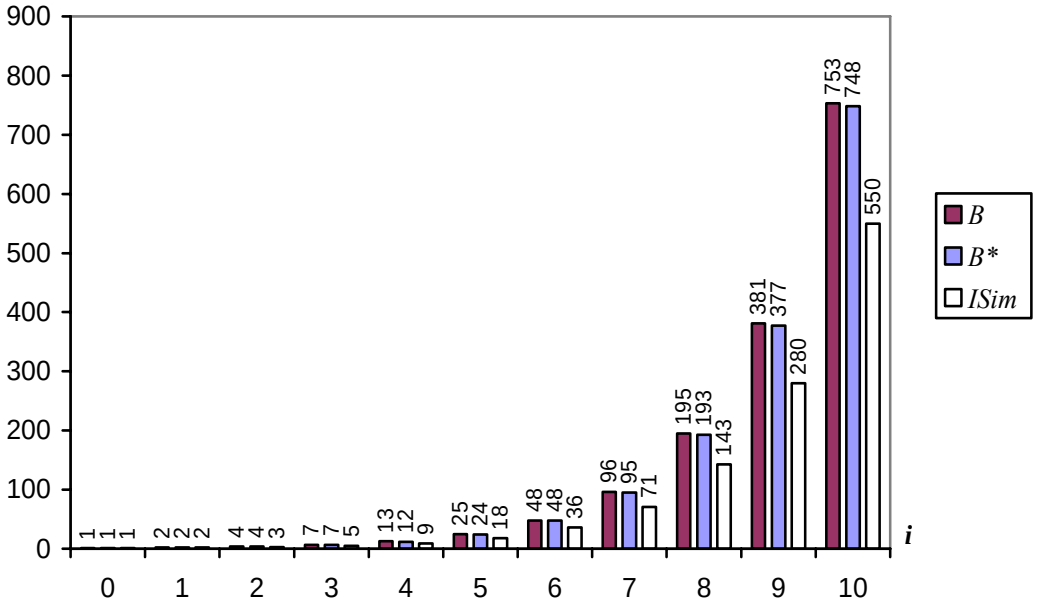


Рис. 7. Распределение числа регистрируемых импульсов

Согласно полученным экспериментальным данным для значений $i \geq 7$ ($i = \lceil \log_2 k \rceil$) наблюдается стабильное увеличение арифметического расстояния $D^*_\Delta(k)$ между числом импульсов, зарегистрированных в процессе моделирования, и числом импульсов, зарегистрированных на реальных цифровых системах. Так, для значения $k = 2^7$ значение разницы $D^*_\Delta(k) = 25$, $D^*_\Delta(2^8) \approx 50$, $D^*_\Delta(2^9) \approx 100$, $D^*_\Delta(2^{10}) \approx 200$ и т. д.

Можно предположить, что с увеличением k значение $D^*_\Delta(k)$ будет изменяться согласно выражению $D^*_\Delta(k) \approx 25 \cdot 2^{\lceil \log_2 k \rceil - 7} = \frac{25}{128} k, \quad \forall k \geq 2^7$. В свою очередь, значение $D^*_\Delta(k)$ определяет число уникальных идентификаторов (число исследуемых микросхем ПЛИС) для выбранного значения k. Например, можно предположить, что для $k = 2^{11}$ около 400 ПЛИС из класса XC3s500e-5FG320 могут быть различимы. Таким образом, увеличение значения k позволяет повышать достоверность идентификации ПЛИС.

Заключение

В статье предложено использовать частотные характеристики конфигурируемых генераторов цифровых импульсов в качестве физически неклонируемых функций с целью идентификации программируемых логических интегральных схем типа FPGA. Показано, что для функционально идентичных ПЛИС Xilinx SPARTAN-3E (XC3s500e-5FG320), входящих в состав идентичных цифровых систем Digilent Nexys-2, при равных внешних условиях эксплуатации регистрируется стабильная разница числа генерируемых импульсов, вызванная физическими вариациями структур кристаллов интегральных схем.

Список литературы

1. FPGA Based Symmetric Multi-core Processors for Optimized Performance of H.264 Encoder / M.E. Krishnan [et al.] // Advances in Recent Technologies in Communication and Computing (ARTCom'10) : Proc. on IEEE Int. Conf. – Kottayam, India, 2010. – P. 235–239.

2. Temple, K. Intel Expands Customer Choice with First Configurable Intel® Atom™-based Processor / K. Temple // Intel Newsroom [Electronic resource]. – 2010. – Mode of access : http://newsroom.intel.com/community/intel_newsroom/blog/2010/11/22/intel-expands-customer-choice-with-first-configurable-intel-atom-based-processor. – Date of access : 13.06.2011.

3. Delay-Based Circuit Authentication and Applications / B. Gassend [et al.] // Applied Computing (SAC'03) : Proc. of the ACM Symp. – Melbourne, FL, USA, 2003. – P. 294–301.

4. Physical Unclonable Functions and Public-Key Crypto for FPGA IP Protection / J. Guajardo [et al.] // Field Programmable Logic and Applications (FPL'07) : Proc. on IEEE Int. Conf. – Amsterdam, Netherlands, 2007. – P. 189–195.

5. Ярмолик, В.Н. Физически неклонируемые функции / В.Н. Ярмолик, Ю.Г. Вашинко // Информатика. – 2011. – № 2 (30). – С. 90–100.

6. Suh, G.E. Physical unclonable functions for device authentication and secret key generation / G.E. Suh, S. Devadas // Design Automation Conference (DAC'07) : Proc. of 44th ACM/IEEE Conf. – San Diego, CA, USA, 2007. – P. 9–14.

7. A Large Scale Characterization of RO-PUF / A. Maiti [et al.] // Hardware-Oriented Security and Trust (HOST'10) : Proc. on IEEE Int. Symp. – Anaheim, CA, USA, 2010. – P. 66–71.

8. Improving the Quality of Ring Oscillator PUFs on FPGAs / D. Merli [et al.] // Embedded Systems Security (WESS'10) : Proc. of the 5th Workshop. – Scottsdale, AZ, USA, 2010. – P. 190–198.

9. Fine-Grained Characterization of Process Variation in FPGAs / H. Yu [et al.] // Field Programmable Technology (FPT'10) : IEEE Int. Conf. – Beijing, China, 2010. – P. 138–145.

10. An FPGA Chip Identification Generator Using Configurable Ring Oscillator / H. Yu [et al.] // Field Programmable Technology (FPT'10) : IEEE Int. Conf. – Beijing, China, 2010. – P. 312–315.

11. Digilent Nexys2 Board Reference Manual [Electronic resource]. – Digilent Inc. – 2008. – Mode of access : http://digilentinc.com/Data/Products/NEXYS2/Nexys2_rm.pdf. – Date of access : 25.03.2011.

12. Spartan-3E FPGA Family Data Sheet (DS312 (v3.8)) [Electronic resource]. – Xilinx Inc. – 2006. – Mode of access : http://www.xilinx.com/support/documentation/data_sheets/ds312.pdf. – Date of access : 25.03.2011.

13. ISE WebPACK Design Software [Electronic resource]. – Mode of access : http://www.xilinx.com/products/design-tools/ise-design-suite/ise-webpack.htm. – Date of access : 14.06.2011.

14. Зотов, В. Измеритель частоты цифровых сигналов, выполненный на основе микропроцессорного ядра семейства PicoBlaze и реализуемый на базе инструментального комплекта Spartan-3E Starter Kit фирмы Xilinx / В. Зотов // Компоненты и технологии. – 2007. – № 12. – С. 54–62.

15. Sedcole, P. Within-die Delay Variability in 90nm FPGAs and Beyond / P. Sedcole, P.Y.K. Cheung // Field Programmable Technology (FPT'06) : IEEE Int. Conf. – Bangkog, 2006. – P. 97–104.

16. Drutarovsky, M. Analysis of Randomness Sources in Transition Effect Ring Oscillator based TRNG / M. Drutarovsky, M. Varchola // Cryptographic Architectures Embedded in Reconfigurable Devices (CryptArchi'10) : Proc. of Int. Workshop, Gif sur Yvette. – France, 2010. – P. 102–107.

Поступила 06.07.11

Белорусский государственный университет
информатики и радиоэлектроники,
Минск, ул. П. Бровки, 6
e-mail: ivaniuk@bsuir.by

A.A. Ivaniuk

APPLICATION OF CONFIGURABLE PULSE GENERATOR FOR FPGA IDENTIFICATION

The application of configurable pulse generator as a hardware implementation of physical unclonable function for FPGA identification is considered. Results of an experimental investigation of configurable pulse generators for FPGA Xilinx SPARTAN-3E are reported and discussed.