ИНФОРМАТИКА

2011 **апрель-июнь** **№ 2**

ЗАЩИТА ИНФОРМАЦИИ

УДК 681.324

В.Н. Ярмолик, Ю.Г. Вашинко

ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫЕ ФУНКЦИИ

Анализируются методы построения физически неклонируемых функций, являющихся основой физической криптографии. Показываются ограничения при реализации подобных функций для цифровых устройств, в особенности с программируемой архитектурой. Предлагаются комбинированные физически неклонируемые функции. Экспериментально подтверждается их эффективность для случая программируемых логических матриц.

Введение

Физическая криптография (Physical Cryptography), которая основана на структурной сложности оптических и электронных физических систем, является одним из наиболее современных достижений в области криптографии и защиты информации [1–4]. Наряду с квантовой криптографией (Quantum Cryptography) [5, 6] и криптографией, основанной на применении хаотических динамических систем (Chaos-base Cryptography) [7], физическая криптография использует шумоподобное поведение физических объектов и систем [1]. Это позволяет в большей мере обеспечить высокие требования (по сравнению с классической алгебраической криптографией) к таким параметрам криптографических систем, как диффузия и конфузия. Эти параметры определены К. Шенноном в его фундаментальной работе, посвященной защите информации [8].

Доминирующей категорией физической криптографии являются физически неклонируемые функции (Physical Unclonable Functions, PUF), которые изначально назывались физическими однонаправленными функциями (Physical One-Way Functions, POWF) или физическими случайными функциями (Physical Random Functions, PRF) [1–4]. Несмотря на то что последние два определения были сформулированы исторически раньше, в настоящее время в основном употребляется понятие «физически неклонируемые функции» (ФНФ). Изначально идея ФНФ была сформулирована Р. Паппу в его пионерских работах [1, 2], и ему, безусловно, принадлежит заслуга как первому, кто сделал попытку сформулировать основные понятия и определения в данной области. Одно из наиболее широко используемых на сегодняшний день определений ФНФ было предложено П. Туилсом [9]. ФНФ, по его определению, – это физические системы (устройства), неотъемлемым свойством которых является неклонируемость (неповторяемость) некоторых их функций, свойств, характеристик либо параметров. ФНФ наследуют это свойство из того факта, что состоят из множества компонент, параметры которых в процессе создания подобных физических систем принимают случайные значения. Величинами параметров компонент в процессе создания систем в силу их физической сущности принципиально невозможно управлять, задавая им конкретные значения. Результатом всегда будет случайное значение параметра компоненты конкретной физической системы. Наличие случайных элементов, а также невозможность контролировать эти элементы во время производства делают ФНФ уникальными и физически неклонируемыми. При подаче некоторого сигнала на вход подобная система формирует выходной сигнал – ответ в виде фиксированного значения случайного параметра компоненты, которое для разных систем будет различным.

ФНФ описываются значениями пар входных и соответствующих им выходных параметров (сигналов). Подобная пара, состоящая из входного физического параметра (запроса) и выходного параметра (ответа), называется парой запрос – ответ (Challenge-Response Pair, CRP). В простейшем случае ФНФ можно рассматривать как функцию, которая преобразует запросы C в ответы R [9].

Более общее определение ФНФ как системы со сверхбольшим объемом информации (Super High Information Content, SHIC) было предложено У. Рухрмаиром [10].

Физически неклонируемые функции – это сложные неупорядоченные физические системы с чрезвычайно большим объемом структурной информации, которые удовлетворяют следующим свойствам:

1. Структурная информация подобных систем может быть извлечена надежно и неоднократно путем проведения измерений для различных запросов C_i и получения ответов R_i.

2. Количество возможных запросов C_i должно быть настолько велико, что значения всех соответствующих ответов R_i не могут быть получены путем перебора всех возможных запросов C_i за реальный временной промежуток.

3. Ввиду наличия в системе чрезвычайно большого объема структурной информации должно быть невозможным смоделировать, рассчитать, или каким-либо другим математическим способом предсказать пару запрос – ответ (C_j, R_j), зная другую пару (C_i, R_i) или некоторое множество таких пар.

4. Для физической системы с чрезвычайно большим объемом структурной информации должно быть чрезвычайно сложным ее физическое воспроизведение или клонирование как аналогичной физической системы, описываемой идентичным множеством пар запрос – ответ.

Для случая интегральных цифровых схем фундаментальной идеей большинства реализованных ФНФ является создание цифрового устройства, выходное значение которого определяется случайными значениями временных параметров (задержек) кремниевой подложки. Благодаря технологическим вариациям во время изготовления цифровых устройств время задержки сигналов по определенному пути цифрового устройства будет незначительно изменяться от цифрового устройства к цифровому устройству и от кристалла к кристаллу несмотря на идентичность их топологии и функциональности [11].

1. Физически неклонируемые функции, реализуемые в цифровых устройствах

Первые подходы для построения ФНФ, которые были предложены и реально применены в цифровых устройствах, базируются на измерении задержек распространения сигнала в реконфигурируемых путях цифрового устройства. Под понятием «путь цифрового устройства» понимают последовательно подключенные друг к другу логические элементы, каждый из которых характеризуется таким параметром, как задержка d распространения сигнала через элемент. Величина задержки определяется двумя составляющими, т. е. $d = d_S + d_R$, где d_S – статическая задержка элемента либо минимальное значение d, а d_R – случайная динамическая компонента, зависящая от изменений параметров технологического процесса производства элемента и свойств материалов (кремниевой подложки) для его изготовления. Любой путь цифрового устройства характеризуется длиной, т. е. количеством последовательно подключенных элементов, а также имеет вход и выход.

В силу физической неоднородности кремниевой подложки, на которой реализуется цифровое устройство, а также вариаций технологического процесса его изготовления один и тот же путь на двух цифровых устройствах или в двух различных местах подложки одного устройства принципиально не может иметь одинаковую задержку распространения сигнала между его входом и выходом. Одним из наиболее известных методов, который основан на измерении случайных вариаций задержек сигналов в цифровых устройствах, является ФНФ типа арбитр (Arbiter PUF) [12, 13].

1.1. Физически неклонируемые функции типа арбитр

Для реализации ФНФ типа арбитр на цифровом устройстве либо нескольких устройствах изготавливаются два топологически и функционально идентичных пути. Очевидно, что оба пути будут иметь близкие значения величин распространения по ним сигналов, однако они будут принципиально разными. Процесс измерения времени распространения сигнала будет заключаться в одновременной подаче на входы обоих путей сигнала и определении, который из сигналов появится на выходе быстрее. По сути, схема ФНФ типа арбитр определяет, какой из путей является более быстрым. Симметричные пути задержки изготавливаются таким образом, что одновременно из большого множества пар путей выбирается одна пара за счет формирова-

ния конкретного запроса. Далее для выбранной пары путей определяется, какой из них является более быстрым.

Наиболее распространена схема ФНФ типа арбитр (рис. 1) [12]. Эта схема строится с использованием n последовательно подключенных пар двухвходовых мультиплексоров. Адресные входы обоих мультиплексоров каждой пары объединяются и используются в качестве одного из входов для задания значения запроса. В качестве запроса в данном случае используется n-разрядный вектор $C_i = c_0\, c_1\, c_2 \ldots c_{n-1}$, где $c_j \in \{0, 1\}, j \in \{0, 1, 2, \ldots, n-1\}$. Запрос C_i в схеме ФНФ типа арбитр формирует два пути таким образом, что если $c_j = 0$, то для построения первого пути используется верхний мультиплексор MUX_j, а для второго – нижний MUX_j, а при $c_j = 1$ наоборот. Каждая пара путей имеет общий вход, а выходы первого и второго пути соответственно подключены к входу D D-триггера и к его синхронизирующему входу Clk. Очевидно, что количество пар путей с увеличением n растет экспоненциально и равняется 2^n. Для конкретного запроса C_i генерируется ответ $R_i \in \{0, 1\}$ как результат эксперимента по определению, какой из путей выбранной запросом C_i пары – первый или второй – быстрее. Например, если первый, то принимается $R_i = 1$, а если второй – $R_i = 0$.

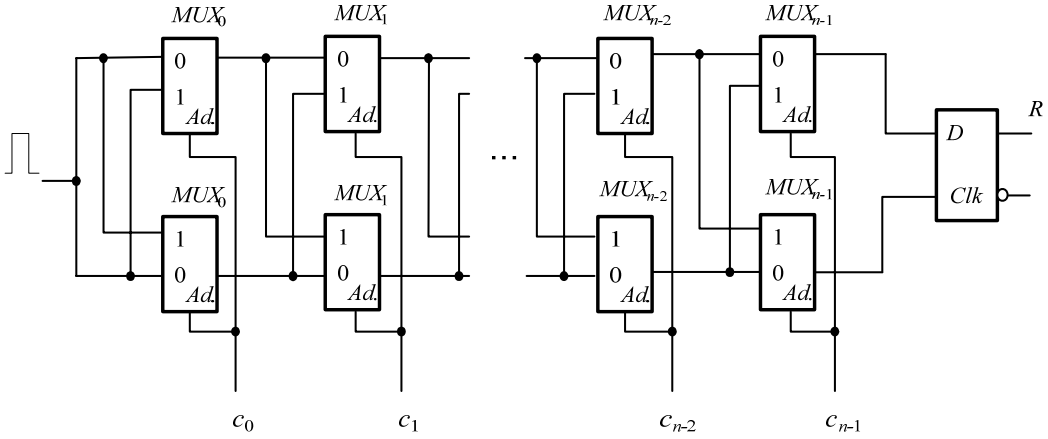

Рис. 1. ФНФ типа арбитр на основе мультиплексоров

Как показано на рис. 1, для получения ответа R_i на конкретный запрос C_i на входы обоих путей одновременно подается высокий уровень сигнала (импульс). Импульс последовательно проходит по двум путям, каждый из которых состоит из n мультиплексоров, а арбитр, в данном случае это D-триггер, определяет, какой из путей является более быстрым (имеет меньшую задержку). Значение ответа R_i равняется 1, если импульсный сигнал по первому пути приходит на вход D D-триггера раньше, чем на синхронизирующий вход Clk по второму пути. В противном случае $R_i = 0$. Отметим, что перед проведением сравнения задержек двух путей D-триггер устанавливается в нулевое состояние. Очевидно, что в силу симметрии путей каждой пары на этапе изготовления невозможно предсказать и запрограммировать, какой из путей конкретной пары имеет меньшую задержку. Таким образом, ФНФ типа арбитр позволяет получить однобитный ответ R_i на n-битный запрос C_i.

Существует два способа для получения m-битного ответа R_i на базе схемы однобитной ФНФ типа арбитр, представленной на рис. 1. Одним из самых простых решений является использование запроса C_i в качестве начального значения для генератора псевдослучайных чисел той же разрядности n. Затем m последовательных значений, формируемых генератором, используются как m запросов C_i, на каждый из которых ФНФ типа арбитр генерирует ответ R_i. В случае реальных значений m и n данное решение является очень затратным по времени. Второй способ основывается на дублировании m раз схемы ФНФ типа арбитр, что не увеличивает время получения m-битного ответа R_i по сравнению с однобитным вариантом. Однако в данном случае аппаратная сложность ФНФ типа арбитр увеличивается в m раз и во столько же раз увеличивается площадь кристалла на реализацию данной ФНФ, а также потребляемая ею мощность.

При использовании ФНФ типа арбитр на базе мультиплексоров для конкретного запроса C_i один и тот же нижний либо верхний мультиплексор равновероятно может быть использован как для первого, так и для второго путей [12], т. е. для построения двух путей используются одни и те же элементы. Как альтернатива ФНФ типа арбитр в [13] было предложено и изучено использование двух раздельных множеств путей, когда первый путь пары строится из первого множества элементов, а второй – из второго. Предложенная схема использует вариации задержек буфера с тремя состояниями и строится путем последовательного подключения пар буферов [13]. Результаты моделирования, представленные в [13], показывают, что ФНФ типа арбитр, основанная на буферах с тремя состояниями, потребляет меньше энергии и к тому же требует для своей реализации значительно меньше места на кристалле по сравнению с аналогичной схемой на мультиплексорах.

Для всех разновидностей ФНФ типа арбитр весьма важной является стабильность (надежность и повторяемость) их функционирования, которая характеризуется повторяемостью значения ответа R_i на один и тот же запрос C_i. Отметим, что в случае ФНФ типа арбитр значение R_i зависит от соотношения задержек двух путей, а задержки элементов в большой степени зависят от таких внешних факторов, как температура, вариации напряжения питания и др.

Экспериментальные исследования для однобитовой ФНФ типа арбитр на базе мультиплексоров, изготовленной по технологии TSMC 0,18 μm., показали, что вероятность изменения ответа R_i в процентном исчислении при повторяющемся запросе C_i составила 0,7 % [13]. В то же время изменение температуры в пределах от −20 °С до +70 °С, а также питающего напряжения в пределах ±2 % увеличивает значение данной вероятности до 4,8 %. Вторым весьма важным свойством ФНФ, наряду со стабильностью, является неклонируемость, которая может быть оценена вероятностью различия ответов для двух ФНФ, изготовленных на одном либо разных кристаллах, на входы которых подается один и тот же запрос. Очевидно, что в идеале, когда обе ФНФ представляют абсолютно симметричные схемы, данная вероятность равняется 50 %. Однако в силу зависимости технологических процессов изготовления ФНФ в результате эксперимента было получено только 23 % различных значений R_i. Изменение температуры и питающего напряжения в тех же пределах приводит к вариации вероятности различия в пределах 3,7 % [13].

Основным недостатком ФНФ типа арбитр является невысокая их надежность в силу того, что изготовленная схема ФНФ имеет систематическую асимметрию в своей топологии в результате ее автоматизированного синтеза и производства. При автоматизированном проектировании и изготовлении достаточно сложно соблюдать симметрию таких топологических элементов ФНФ, как длины проводников соединений, идентичность полупроводниковых элементов и их геометрических размеров, равенство задержек и др.

1.2. Физически неклонируемые функции на базе кольцевых генераторов

Существенно большей стабильностью характеризуются ФНФ на базе кольцевых генераторов (КГ) [12, 14]. Данный тип ФНФ основан на применении КГ, которые представляют собой последовательно включенные инверторы, охваченные отрицательной обратной связью. Количество инверторов должно быть нечетным, что является условием формирования на выходе кольцевого генератора импульсной последовательности, частота которой определяется величиной задержки на элементах генератора, охваченных обратной связью. В силу вариаций задержек сигнала на элементах генератора два идентичных по топологии и функциональности КГ имеют отличающиеся частоты выходных импульсных сигналов. Различие частот сигналов, формируемых КГ, и является основой для формирования однобитного ответа. Действительно, две пары КГ на одном либо разных кристаллах будут иметь произвольное соотношение частот и уникально характеризовать данную пару либо соответственно кристалл.

Для того чтобы сгенерировать фиксированное число бит ответа R_i, ФНФ, основанная на КГ, включает n кольцевых генераторов (рис. 2). Тогда один бит ответа формируется путем сравнения частот двух КГ, которые выбираются с использованием двух мультиплексоров *MUX*. Каждый из мультиплексоров на основании запроса *C* выбирает один из n КГ. Выходы мультиплексоров подключены к входам двух суммирующих двоичных счетчиков *COUNTER*, которые суммируют поступающие на их входы импульсы. Отметим, что частоты поступления импуль-

сов от двух КГ будут отличаться. Это приводит к тому, что за фиксированный промежуток времени содержимое счетчиков будет различным. При этом чем больше временной интервал, на котором проводится измерение, тем больше различие состояний двух счетчиков, что, по сути, гарантирует существенно большую стабильность ФНФ, использующих КГ, по сравнению с ФНФ, основанными на применении мультиплексоров. Затем состояния двух счетчиков *COUNTER* сравниваются на схеме сравнения *COMPARATER*, на выходе которой формируется однобитный ответ *R*. Временной интервал, в течение которого осуществляется измерение, задается путем одновременной подачи на входы двухвходовых элементов 2И-НЕ всех КГ единичного сигнала.

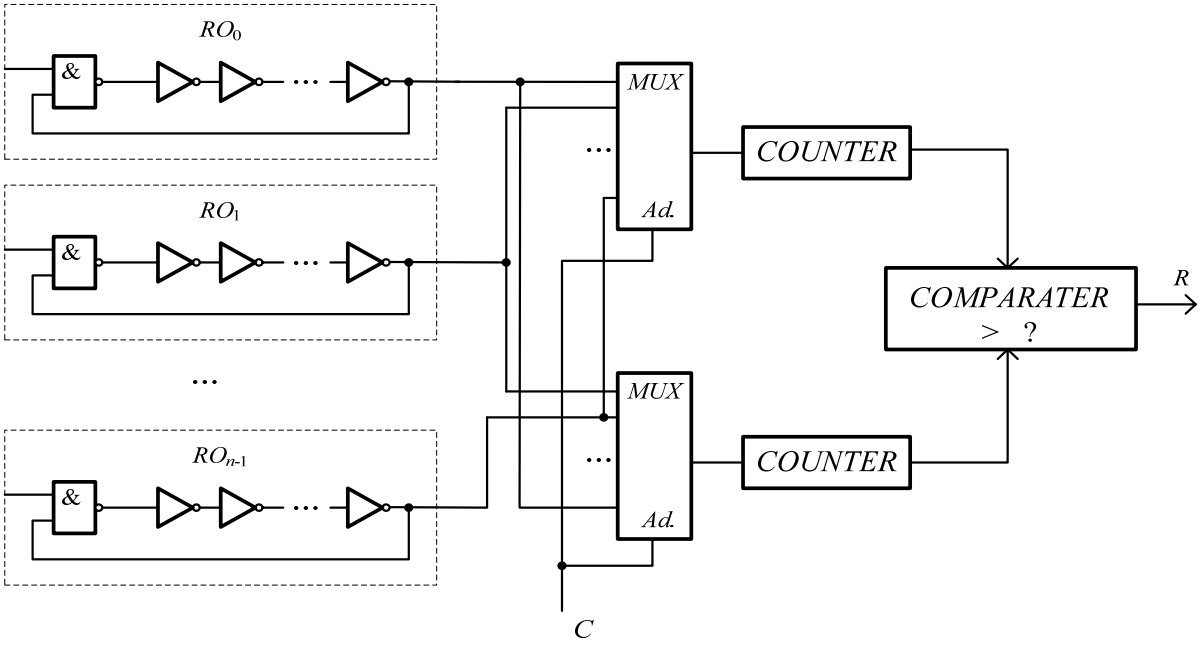

Рис. 2. ФНФ на базе КГ

По сравнению с ФНФ типа арбитр в случае с ФНФ на основе КГ не требуются тщательная топологическая симметрия и идентичность трассировки. К примеру, длины проводников от выходов КГ к входам счетчиков не обязательно должны быть одинаковыми, так как при подсчете импульсных сигналов разница между состояниями двух счетчиков будет возрастать и превышать погрешность, которую могут внести задержки в соединительных проводниках.

Таким образом, ФНФ на базе КГ в результате сравнения частот импульсных сигналов пары КГ генерирует один бит ответа *R* (рис. 2). Для *n* генераторов существует $n(n-1)/2$ различных пар КГ, причем один и тот же генератор может входить в несколько пар КГ. Это обстоятельство вносит корреляцию в формируемые ответы *R* [12]. Например, если генератор $КГ_i$ имеет большую частоту, чем генератор $КГ_j$, и в результате сравнения формируется ответ $R = 1$, а генератор $КГ_j$ является более высокочастотным по сравнении с $КГ_r$, то очевидно, что результатом сравнения частот $КГ_i$ и $КГ_r$ также будет $R = 1$. Данное обстоятельство регламентирует выборку независимых пар КГ, что заметно увеличивает сложность ФНФ на базе КГ [12, 14].

По сравнению с ФНФ типа арбитр схема ФНФ на основе КГ проще в реализации и, что важнее всего, имеет достаточно высокую степень надежности [14]. В то же время ФНФ на базе КГ имеют меньшее быстродействие и потребляют больше энергии для генерирования ответов, чем ФНФ типа арбитр [12, 14].

1.3. Физически неклонируемые функции на базе статического оперативного запоминающего устройства

Статические оперативные запоминающие устройства (СОЗУ) широко используются в вычислительной технике для хранения данных. Непосредственно запоминающий элемент

СОЗУ (ячейка) состоит из четырех транзисторов, реализующих два инвертора с перекрестными обратными связями [13]. Подобная ячейка всегда находится в одном из двух состояний, что, в свою очередь, позволяет использовать ее для хранения одного бита информации. Примером такой ячейки может служить *RS*-триггер, реализованный на двух логических элементах 2И-НЕ (рис. 3).

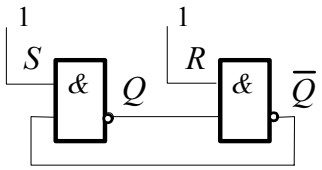

Рис. 3. ФНФ на базе ячейки СОЗУ, реализованной в виде *RS*-триггера

Высокий уровень сигнала, соответствующий логической единице (1) и подаваемый одновременно на входы *S* и *R RS*-триггера, позволяет сохранять предыдущее состояние 0 либо 1, определяемое последней операцией записи в данную запоминающую ячейку. При включении питающего напряжения все ячейки СОЗУ устанавливаются в одно из двух возможных состояний – 0 или 1; причем в силу симметрии *RS*-триггера априори неизвестно, какое конечное состояние примет ячейка – 0 или 1. Это состояние является случайным и определяется множеством факторов [15]. Экспериментально подтверждено, что большинство ячеек СОЗУ при включении питающего напряжения преимущественно переходят в одно из двух состояний. Причиной этого является то, что каждая ячейка СОЗУ, представляющая собой *RS*-триггер, в силу особенностей технологии изготовления имеет множество несимметричных элементов. К таким элементам можно отнести длины соединительных проводников, их геометрические размеры, неоднородность физических и химических свойств кремния, девиацию задержек сигналов и др. В работе [16] было показано, что только для части ячеек СОЗУ их состояние после включения питающего напряжения является действительно случайным и зачастую приближается к равномерному распределению. Остальные ячейки устойчиво принимают значение состояния 0 или 1.

Факт того, что количество случайных значений состояний ячеек СОЗУ при включении питания является ограниченным, был экспериментально подтвержден в работе [17]. Для исследований были выбраны три различные программируемые матрицы Virtex-II Pro. В этих матрицах анализировалось состояние 4 096 ячеек СОЗУ после включения питающего напряжения. Каждое СОЗУ представляет собой матрицу запоминающих ячеек, состоящую из 32 столбцов и 128 строк. Результат показал, что более 90 % исследуемых ячеек СОЗУ всегда устанавливались в состояние 0, менее 10 % ячеек – исключительно в состояние 1 и только менее 1 % ячеек устанавливались равновероятно в состояние 0 или 1 [17]. Эти результаты позволяют сделать вывод, что ФНФ на базе СОЗУ являются весьма ненадежными, особенно применительно к программируемым матрицам (FPGA). Это объясняется тем, что в силу регулярности топологии FPGA в любом симметричном элементе (например, *RS*-триггере), реализованном на FPGA, практически всегда присутствует прогнозируемая асимметрия. Для того чтобы обойти эту проблему, была предложена концепция ФНФ типа бабочка (Butterfly PUF), поведение которой аналогично симметричной ячейке СОЗУ при включении питающего напряжения [18].

1.4. Физически неклонируемые функции типа бабочка

ФНФ типа бабочка, предложенная С. Кумаром и др. в [18], – это технический прием, направленный на эмуляцию работы ФНФ на базе запоминающей ячейки СОЗУ [16]. Данный прием основывается на формировании перекрестных обратных связей с использованием стандартных триггеров, применяемых в программируемых логических матрицах. В результате структура запоминающей ячейки ФНФ типа бабочка оказывается настолько симметричной, насколько это возможно. Подобная ячейка строится как схема с перекрестными обратными связями, кото-

рые используются в ФНФ на базе запоминающих ячеек СОЗУ. Однако в данном случае логические элементы 2И-НЕ заменяются на *D*-триггеры (рис. 4).

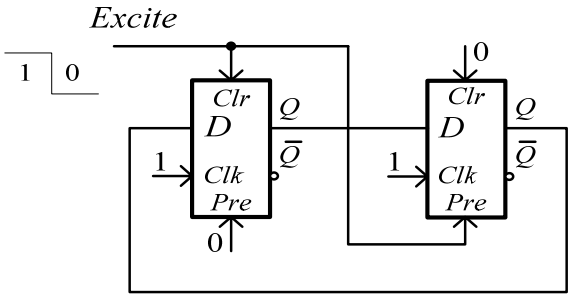

Рис. 4. ФНФ типа бабочка

ФНФ типа бабочка состоит и двух *D*-триггеров, каждый из которых имеет асинхронные входы установки в единичное состояние *Pre* и сброса в нулевое состояние *Clr*. На вход *Pre* первого триггера и на вход *Clr* второго триггера постоянно подается значение логического 0. Отметим, что активным уровнем входного сигнала по входу синхронизации (*Clk*) и по входам асинхронного управления *Pre* и *Clr* является единичный сигнал. Наличие нулевого сигнала на указанных входах сохраняет предыдущее состояние. Как показано на рис. 4, вход *Excite* ФНФ типа бабочка соединен с входом *Clr* первого триггера и входом *Pre* второго триггера. На входы синхронизации *Clk* обоих триггеров подается единичный сигнал. Первоначально на вход *Excite* подается единичный сигнал, что приводит схему ФНФ типа бабочка в нестабильное состояние. Для первого *D*-триггера единичный сигнал по входу *Clk* устанавливает его в нулевое состояние, а по *D*-входу – в единичное, так как второй триггер по входу *Pre* устанавливается в единичное состояние. Такие же взаимоисключающие входные сигналы подаются на входы второго триггера. Таким образом, на выходах обоих триггеров устанавливается неустойчивое промежуточное значение. Затем через некоторое время на вход *Excite* подается сигнал низкого уровня, что инициирует процесс перехода схемы ФНФ в одно из двух стабильных состояний, когда на выходе второго триггера будет сформировано значение 0 или 1. Конечное состояние обусловливается случайной разностью задержек в паре линии обратной связи и линии сигнала *Excite*, что является следствием изменений параметров технологического процесса изготовления FPGA.

2. Анализ физически неклонируемых функций

Основой реализации рассмотренных в предыдущем разделе ФНФ является использование различия в задержках сигналов $d = d_S + d_R$ по двум симметричным путям. Очевидно, что максимальная эффективность ФНФ будет достигнута в случае сравнения только случайных составляющих d_R общей задержки d обоих путей. Это объясняется тем фактом, что случайная динамическая компонента d_R зависит от изменений параметров технологического процесса производства и свойств материалов для изготовления ФНФ и поэтому является уникальной и непредсказуемой.

Эффективность ФНФ зависит от того, какая максимальная симметричность может быть достигнута между определенными парами путей (элементов) для того, чтобы снизить эффект влияния статической задержки d_S на результат сравнения. В идеале для пары анализируемых путей необходимо, чтобы их статические задержки были равными. Их отличие приводит к нарушению симметрии для пары сравниваемых путей и соответственно прогнозируемости результата сравнения, а как следствие – и к клонируемости ФНФ. Требование к симметричности различно по своей природе для каждого типа ФНФ и определяется схемотехническими решениями и сложностью реализации ФНФ. Известны три основные типа ФНФ, использующие девиацию задержек сигналов: ФНФ типа арбитр, ФНФ на основе КГ и ФНФ типа бабочка [12−18].

В случае ФНФ типа арбитр необходимо соблюдение симметрии для всех компонент, используемых для их построения. Весьма существенной является симметрия соединительных проводников не только в части их длин, но и места их расположения на кристалле. Такие же

требования предъявляются и к ФНФ типа бабочка, где требования симметрии необходимо соблюдать и для двух *D*-триггеров. Менее жесткие требования к симметрии соединительных проводников выдвигаются к ФНФ на основе КГ. В данном случае требования симметрии необходимо соблюдать для главных элементов ФНФ.

3. Комбинированные физически неклонируемые функции

Как было показано в подразд. 1.3, главным составным элементом ФНФ на базе СОЗУ является стандартный *RS*-триггер (см. рис. 3). Схема *RS*-триггера построена таким образом, что позволяет комбинационной схеме с положительной обратной связью хранить требуемое значение 0 или 1. Функционирование подобной схемы может быть описано с помощью таблицы переходов, однозначно определяющей функционирование *RS*-триггера. Входные значения *S* и *R* могут принимать любую из четырех возможных комбинаций значений 00, 01, 10 и 11. Для обозначения безразличного значения входных сигналов *S* и *R* используется $XX \in \{00, 01, 10, 11\}$, а для выходных значений – $Q\overline{Q} \in \{01, 10, 11\}$. Отметим, что для *RS*-триггера, показанного на рис. 3, на его выходах Q и $\overline{Q}$ невозможно получение комбинации $Q = 0$ и $\overline{Q} = 0$.

Таблица переходов *RS*-триггера

Текущие значения на входах *S* и *R*	Следующие значения на входах *S* и *R*	Текущее состояние $Q\overline{Q}$	Следующее состояние $Q\overline{Q}$
$SR = XX$	0 0	$Q\overline{Q}$	1 1
$SR = XX$	0 1	$Q\overline{Q}$	1 0
$SR = XX$	1 0	$Q\overline{Q}$	0 1
$SR \neq 0\,0$	1 1	$Q\overline{Q}$	$Q\overline{Q}$
$SR = 0\,0$	1 1	$Q\overline{Q}$	Случайное значение $Q\overline{Q} = 1\,0$ или $0\,1$

Для случая стандартного применения *RS*-триггера, когда на его выходе необходимо формировать предсказуемые значения, запрещается использование на входах *S* и *R* перехода от комбинации 00 к 11. В данном случае *RS*-триггер примет одно из двух стабильных состояний, а именно единичное ($Q\overline{Q} = 1\,0$) или нулевое ($Q\overline{Q} = 0\,1$). Это может произойти с определенным предпочтением, в зависимости от внесенной асимметрии при производстве *RS*-триггера между двумя его частями, состоящими из двух логических элементов 2И-НЕ и соединительных проводников.

Данный запрещенный переход может быть рассмотрен как эмуляция подключения питающего напряжения на ячейку СОЗУ и соответственно может быть использован в качестве ФНФ на основе *RS*-триггера (рис. 5). Отличие схемы на рис. 5 от ФНФ на базе ячейки СОЗУ, реализованной в виде *RS*-триггера (см. рис. 3), заключается в объединении входов *S* и *R*, которое исключает возможность использования такого устройства в качестве запоминающего элемента. После последовательной подачи на вход данной схемы значений 0 и 1 стабильное выходное состояние сигналов $Q\overline{Q}$ будет случайным и непредсказуемым, причем непредсказуемость так же, как и в предыдущих случаях, объясняется вариациями технологического процесса изготовления ФНФ с использованием *RS*-триггера и может интерпретироваться как неклонируемость.

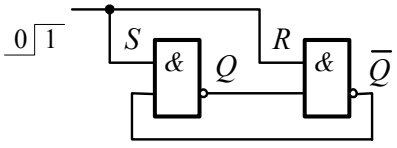

Рис. 5. ФНФ на основе *RS*-триггера

В общем случае величина задержки *d* логического элемента 2И-НЕ – это функция, зависящая от его сопротивления и выходной паразитной емкости. Известно, что сопротивление элемента и его выходная емкость в сильной степени зависят от геометрических размеров транзисторов (транзистора), используемых при его изготовлении, которые в процессе производства элемента могут незначительно и неуправляемо изменяться. Соответственно небольшие геометрические изменения приводят к увеличению или уменьшению задержки сигнала *d*. Как и в случае ФНФ на базе ячейки СОЗУ, реализованной в виде *RS*-триггера, в данном случае асимметрия, внесенная на этапе производства, будет снижать качество ФНФ.

Для увеличения диапазона изменения случайных значений задержек и соответственно стабильности и надежности ФНФ может быть предложена комбинированная реализация ФНФ. Одним из вариантов подобных ФНФ является объединение ФНФ типа арбитр и ФНФ на основе RS-триггера. В результате функциональная схема ФНФ на основе арбитра и RS-триггера принимает следующий вид (рис. 6).

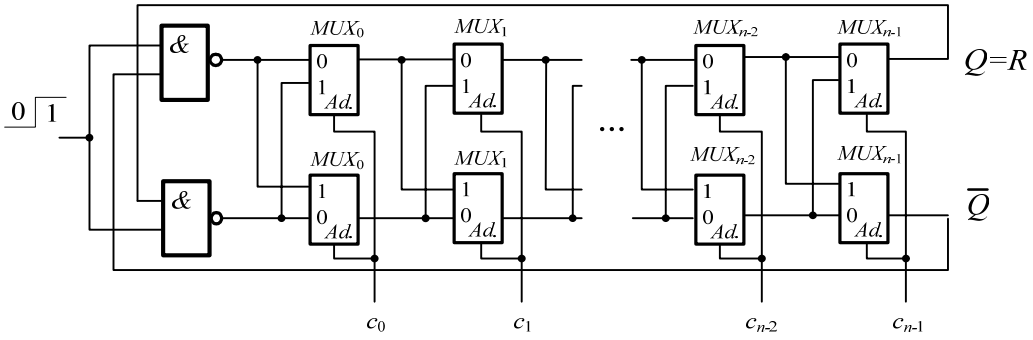

Рис. 6. ФНФ на основе арбитра и *RS*-триггера

Основной идеей предложенной схемы является увеличение пути между выходом одного из двух элементов 2И-НЕ *RS*-триггера и входом другого элемента 2И-НЕ (см. рис. 5 и 6). Длина пути для двух обратных связей увеличивается за счет последовательно включенных *n* двухвходовых мультиплексоров. При такой реализации задержка зависит не только от технологических вариаций во время производства логических элементов 2И-НЕ и соответственно их задержек, но и от значения запроса C_i, который определяет множество мультиплексоров, вариации задержек которых влияют на значение ответа. В зависимости от C_i значение ответа $Q = R$ формируется на выходе мультиплексора MUX_{n-1}. Для расчета эффективности предложенного решения может быть использована та же линейная модель, что и применяемая для оценки качества ФНФ, использующих различие задержек по двум путям [13].

Следующим решением является комбинированная ФНФ на основе КГ и ФНФ на базе *RS*-триггера (рис. 7).

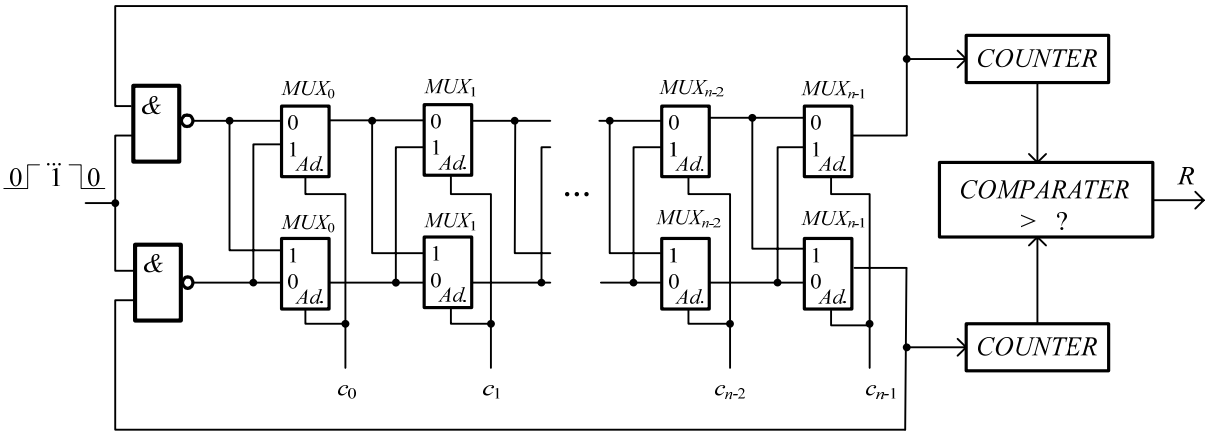

Рис. 7. ФНФ на основе КГ и *RS*-триггера

На рис. 7 видно, что для заданного запроса C_i образуются два КГ, причем количество пар КГ определяется только разрядностью n запросов C_i, для каждого из которых формируется своя уникальная пара КГ. Количество высокочастотных импульсов, подаваемых на входы двоичных счетчиков *COUNTER*, определяется окном измерения, задаваемым длительностью единичного сигнала на входе схемы ФНФ. Обе схемы комбинированных ФНФ, приведенных на рис. 6 и рис. 7, могут быть реализованы с применением схем буферов с тремя состояниями [13].

Для экспериментальной проверки работоспособности ФНФ на основе арбитра и *RS*-триггера, а также ФНФ на основе КГ и *RS*-триггера применялись FPGA Spartan 2 фирмы Xilinx. Эксперименты проводились на Prototyping Board Xess XSA-10 с дополнительным модулем Extension Board XST-2.1, что позволило реализовывать ФНФ для запросов C_i, состоящих из 8 бит. Все необходимые компоненты для проведения экспериментов синтезировались с применением Xilinx ISE 9.2i. Полученные результаты подтверждают работоспособность предложенных комбинированных ФНФ. Для случая ФНФ на основе КГ и *RS*-триггера в среднем было получено 39 % значений ответов, равных 0, и 61 % значений $R = 1$.

4. Применение физически неклонируемых функций

Главным достоинством ФНФ является их уникальность (неклонируемость), которая эффективно может быть использована для целей аутентификации цифровых интегральных устройств. Предварительно для конкретной ФНФ регистрируются значения пар запрос – ответ для случайных значений запросов, которые могут в дальнейшем использоваться для сравнения с вновь сгенерированными значениями запрос – ответ, таким образом идентифицируя ФНФ, являющуюся неотъемлемой частью цифрового устройства.

В работе [19] описан механизм аутентификации с использованием доверенной стороны, который позволяет предотвратить возможный перехват пар запрос – ответ во время процедуры аутентификации. Данный механизм лег в основу протокола гарантированной передачи исходного кода встроенного программного обеспечения к конечному устройству [20]. Используя данный протокол, на первом этапе производитель передает свое программное обеспечение, записанное на носителе информации со встроенной ФНФ, потребителю, предварительно зарегистрировав пары запрос – ответ ФНФ данного устройства. Это позволит в дальнейшем выполнить обновление программного обеспечения с гарантированной доставкой нужному пользователю [19, 20].

Заключение

В работе проведен анализ методов построения ФНФ для интегральных цифровых схем. Показана эффективность применения ФНФ, использующих девиацию времени задержки на логических элементах цифровых устройств. Как развитие методов, основанных на задержках, в работе рассмотрены комбинированные ФНФ для случая применения их в FPGA, которые позволят обеспечить высокий уровень защиты интеллектуальной собственности на проекты современных цифровых устройств.

Дальнейшие исследования в этой области могут быть продолжены в направлении совершенствования архитектур комбинированных ФНФ, оптимизации их параметров и оценки качественных характеристик. Весьма интересными представляются исследования в части количества мультиплексоров для ФНФ типа арбитр и количества последовательно включенных инверторов для ФНФ типа КГ в зависимости от разновидностей FPGA и особенностей их архитектуры.

Список литературы

1. Physical One-Way Functions / R. Pappu [et al.] // Science. – 2002. – Vol. 297. – P. 2026–2030.

2. Pappu, R. Physical One-Way Functions: PhD Thesis in Media Arts and Sciences / R. Pappu // Massachusetts Institute of Technology (MIT). – Cambridge, 2001. – 154 p.

3. Controlled physical random functions / B. Gassend [et al.] // Proc. of 18th Annual Computer Security Applications Conf. (ACSAC), Las Vegas, Nevada, USA, 2002. – Las Vegas, 2002. – P. 149–160.

4. Gassend, B. Physical Random Functions: MSc Thesis / B. Gassend // Massachusetts Institute of Technology (MIT). – Cambridge, 2003. – 89 p.

5. Ekert, A.K. Quantum cryptography based on Bell's theorem / A.K. Ekert // Physical Review Letters. – 1991. – Vol. 67, № 6. – P. 661–663.

6. Bennett, C.H. Quantum cryptography using any two nonorthogonal states / C.H. Bennett // Physical Review Letters. – 1992. – Vol. 68, № 21. – P. 3121–2124.

7. Kocarev, L. Chaos-based cryptography: a brief overview / L. Kocarev // Circuits and Systems Magazine. – 2001. –Vol. 1, № 3. – P. 6–21.

8. Shannon, C.E. Communication theory of secrecy systems / C.E. Shannon // Bell System Tech. J. – 1949. – P. 656–715.

9. Tuyls, P. Security with Noisy Data / P. Tuyls, B. Skoric, T. Kevenaar (ed.). – London : Springer, 2007. – 344 p.

10. Cryptology e-print Archive / Ed. T. Rabin, C. Cachin [Electronic resource]. – 2009. – Mode of access : http://eprint.iacr.org/2009/277.pdf. – Date of access : 22.12.2010.

11. Agarwal, A. Statistical Timing Analysis for Intra-Die Process Variations with Spatial Correlations / A. Agarwal, D. Blaauw, V. Zolotov // Proc. of International Conf. on Computer Aided Design (ICCAD03), San Jose, CA, USA, 2003. – San Jose, 2003. – P. 900–907.

12. A technique to build a secret key in integrated circuits for identification and authentication applications / J. Lee [et al.] // Proc. of IEEE VLSI Circuits Symposium. – Boston, MA, USA, 2004. – P. 176–179.

13. Ozturk, E. Physical unclonable function with tristate buffers / E. Ozturk, G. Hammouri, B. Sunar // Proc. of IEEE International Symposium on Circuits and Systems (ISCAS 2008). – Seattle, WA, USA, 2008. – P. 3194–3197.

14. Gang, Q. Temperature-aware cooperative ring oscillator PUF / Q. Gang, Y. Chi-En // Proc. of IEEE International Workshop on Hardware-Oriented Security and Trust. – San Francisco, CA, 2009. – P. 36–42.

15. Holocomb, D. Power-up SRAM State as an Identifying Fingerprint and Source of True Random Numbers / D. Holocomb, W. Burleson // IEEE Transactions on Computers. – 2008. – Vol. 57, № 11. – P. 1198–1210.

16. FPGA Intrinsic PUFs and Their Use for IP Protection / J. Guajardo [et al.] // Lecture Notes in Computer Science. – 2007. – Vol. 4727. – P. 63–80.

17. Maes, R. Intrinsic PUFs from Flip-flops on Reconfigurable Devices / R. Maes, P. Tuyls, I. Verbauwhede // Proc. of 3rd Benelux Workshop on Information and System Security (WISSec 2008). – Eindhoven, The Netherlands, 2008. – P. 3–20.

18. The Butterfly PUF: Protecting IP on every FPGA / S.S. Kumar [et al.] // Proc. IEEE Intern. Workshop on Hardware-Oriented Security and Trust (HOST'2008). – Anaheim, CA, USA, 2008. – P. 67–70.

19. Suh, G.E. Physical Unclonable Functions for Device Authentication and Secret Key Generation / G.E. Suh, S. Devadas // Proc. of 44th annual Design Automation Conf. (DAC '07). – San Diego, CA, 2007. – P. 9–14.

20. Simpson, E. Runtime Intellectual Property Protection on Programmable Platforms : MSc Thesis Computer Engineering / E. Simpson; Virginia Polytechnic Institute and State University. – Blacksburg, 2007. – 50 p.

Поступила 28.02.11

Белорусский государственный университет
информатики и радиоэлектроники,
Минск, П. Бровки, 6
e-mail: yarmolik10ru@yahoo.com

V.N. Yarmolik, Y.G. Vashinko

PHYSICALLY UNCLONABLE FUNCTIONS

Recent methods for the Physical Unclonable Functions implementations in case of Integrated Digital Circuits have been presented. The main drawbacks of Physically Unclonable Functions based on digital path delay for FPGA are shown. A new combined approach for Physical Unclonable Functions implementations have been proposed and experimentally tested. The proposed solution can be used for Intellectual Properties Protection for integrated circuit design.