ИСПОЛЬЗОВАНИЕ МОДИФИЦИРОВАННОГО АРБИТРА ДЛЯ СХЕМНОЙ РЕАЛИЗАЦИИ ФИЗИЧЕСКИ НЕКЛОНИРУЕМОЙ ФУНКЦИИ

Прощеряков А.А.
Кафедра вычислительных методов и программирования
Научный руководитель: Иванюк А.А., зав.каф. ВМиП, д.т.н., доцент
e-mail: proshcheryakov@bsuir.by

***Аннотация* — Рассматривается схемная реализация модифицированной физически неклонируемой функции типа арбитр. Предлагается использование четырёх триггеров для повышения достоверности PUF.**

Ключевые слова: PUFтипа арбитр,идентификация ПЛИС

Для решения задачи идентификации ПЛИС предлагается использовать физически неклонируемые функции (Physical Unclonable Function – PUF), работа которых основана на достоверном определении физических вариаций технологического процесса при изготовлении интегральных схем. Для увеличения достоверности идентификации предлагается использовать модифицированную схему PUF типа арбитр.

Модифицированный PUF типа арбитр

Классическая схема PUF типа арбитр представляет собой множество последовательно соединённых конфигурируемых блоков, образующих конфигурируемый путь, коммутация линий прохождения сигналов в котором определяется настроечными константами C_i. На вход конфигурируемого пути подаются два идентичных одиночных импульса. На выходе устанавливается арбитр, построенный на D-триггере и регистрирующий опережение одного сигнала другим [1].

Однако данный тип PUF не регистрирует такой показатель как изменение скважности импульсов.

Для устранения недостатков классического PUF предлагается на выход конфигурируемого пути установить четыре D-триггера (см. рис.1.)

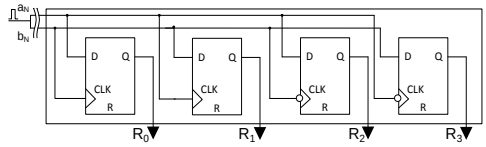

Рис.1. Модифицированный арбитр

Табл.1. Времменные диаграмы сигналов и устанавливыемые значения арбитра

	R_0	R_1	R_2	R_3
0				
1				

В табл.1 представлены все возможные взаиморасположения приходящих импульсов *a* и *b* (верхний импульс – *a*, нижний -*b*). Два младших бита R_0, R_1 выходного ниббла *R* характеризуют взаиморасположение передних фронтов импульсов, два старших бита R_2, R_3 — взаиморасположение задних фронтов импульсов.

Увеличение чувствительности арбитра

Можно заметить, что пары временных диаграмм (R_0–0; R_1–1),(R_0–1; R_1–0), как и пары (R_2–0; R_3–1),(R_2–1; R_3–0) описывают одну и ту же конфигурацию импульсов, что позволяет делать ошибочный вывод об избыточности использования четырёх триггерови достаточности двух.

В ходе одного эксперимента для конфигурируемого пути, состоящего из восьмиблоков, на ПЛИС Xilinx Spartan-3E-250 CP132, для одного полного изменения настроечной константы *C* от 0 до 255 были получены следующие *R* (табл.2.):

Табл.2. Результаты эксперимента

Ниббл (R_3-R_0)	Число появлений
0001	99
0010	25
0011	26
0110	35
0111	2

Полученные результаты (например, появление 26 раз ниббла 0011) указывают на то, что установление R_i в‘1’ происходит не только при высоком уровне *D*в момент фронта сигнала *CLK*.

Данный эффект объясняется тем, что описанный на языке VHDL триггер синтезируется на универсальную элементную базу ПЛИС, входе чего сигналы, приходящие на slice, пропускаются через мультиплексоры с различными характеристиками задержки. Например, усреднённая задержка мультиплексора сигнала *D*составляет 3,936 нс, мультиплексора сигнала *CLK*– 0,121 нс. В результате, когда разница фронтов *a* и *b* не велика, два триггера, в отличии от одного, позволят достоверно установить конфигурацию импульсов.

Интерпретируя такой тип PUF, как четыре независимых классических PUF типа арбитр для одного и того же пути, получаем, что третий арбитр (R_3) выдавал всегда значение 0 (один символ), второй – в 14,5% случаев выдает 1, первый – в 61,3%, нулевой – в 49,6%.Таким образом, использование трех арбитров уже порождает в 2,5 раза больше символов ответа, что увеличивает точность идентификации.

Выводы

Предлагаемая нами модификация PUF типа арбитр позволяет точно охарактеризовать конфигурацию импульсов, приходящих с конфигурируемого пути, и увеличить число символов ответа, что позволит с большей достоверностью идентифицировать цифровое устройство на базе ПЛИС.

[1] Ярмолик, В.Н. Физически неклонируемые функции / В.Н. Яролик, Ю.Г. Вашинко // Информатика. – 2011. - №2. – С. 20-30.