Использование физически неклонируемых функций типа «арбитр» для идентификации встроенных систем на базе ПЛИС

Иванюк А.А.
Кафедра ВМиП, факультет информационных технологий и управления
Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
e-mail: ivaniuk@bsuir.by

***Аннотация* — В докладе рассматриваются вопросы, связанные с идентификацией встроенных систем на базе программируемых логических интегральных схем (ПЛИС) с использованием физически неклонируемых функций (PUF, Physically Unclonable Function). Приводятся примеры существующих аппаратных реализаций PUF. Предлагается новая методика реализации PUF, основанная на модификации существующей PUF типа «арбитр» (Arbiter PUF). Показана эффективность предложенной методики для конфигурируемых встроенных систем на базе ПЛИС.**

Ключевые слова: физически неклонируемая функция; идентификация; программируемая логическая интегральная схема

I. Введение

Вычислительные ядра встроенных систем реализуются, как правило, с использованием микропроцессоров и/или микроконтроллеров. Такой подход целесообразен в виду наличия систем автоматизированного проектирования программного обеспечения, обширных библиотек готовых программных решений, программных систем эмулирования и отладки исполняемых кодов и т.д. Однако программная реализация многих алгоритмов для современных приложений встроенных систем приводит ко многим проблемам, к которым, в первую очередь, можно отнести повышенное энергопотребление цифровой аппаратуры и недостаточная производительность микропрограммной подхода. В последнее время наблюдается тенденция применения программируемых логических интегральных схем (ПЛИС) в качестве технологической платформы для реализации не только вычислительного ядра, но и всей встроенной системы в целом. Программируемые логические устройства позволяют проектировщикам более эффективно реализовывать программно-аппаратные решения для встроенных систем, а возможность динамической реконфигурации открывает широкие перспективы в построении новых вычислительных архитектур. Наличие объемного рынка готовых решений для ПЛИС в виде аппаратных и программно-аппаратных IP-компонент обеспечивает эффективное проектирование встроенных систем различного назначения. Свободное распространение IP-компонент в свою очередь ставит новые задачи, среди которых можно выделить задачи защиты готовых проектных решений от несанкционированного использования. В основе имеющихся решений по защите цифровых проектов лежат методики использования уникальных цифровых идентификаторов интегральных схем. Наличие таких идентификаторов позволяет проектировщикам встроенных систем эффективно решать многие задачи: адресация цифровых устройств, 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.

Большинство серийно выпускаемых ПЛИС не содержат регистров уникальных идентификаторов, что затрудняет разработчикам цифровых систем решать вышеперечисленные задачи. 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.

В данной работе предлагается методика получения цифровых идентификаторов встроенных систем, основанная на применении так называемых ***физически неклонируемых функций***.

II. Физически неклонируемые функции

Физически неклонируемая функция (PUF, Physical Unclonable Function) является характеристикой физической (цифровой) системы, которая не подлежит клонированию (копированию, воспроизведению) на других системах [1]. Для цифровых систем в основе PUF лежат методики достоверного определения физических вариаций технологического процесса при изготовлении интегральных схем. Подобные вариации носят случайный характер и не могут быть предсказаны, а тем более воспроизведены. Незначительные отклонения физических параметров при изготовлении идентичных по функциональности и топологии интегральных схем в первую очередь выражаются в различии их параметрических характеристиках, например в задержках распространения сигналов [2-4].

III. Физически неклонируемые функции типа «арбитр»

Одной из наиболее известных методик реализации аппаратных PUF, основанной на измерении задержек распространения сигналов, является PUF типа «арбитр» [5]. Идея реализации такого типа PUF лежит в построении двух топологически и функционально идентичных путей на одном кристалле интегральной схемы. Такие пути физически являются принципиально различными благодаря различию компонент, из которых состоят пути. Наиболее распространенная схема, реализующая PUF типа «арбитр», приведена на рисунке 1. Она содержит n входных портов запроса C_i, один выходной порт ответа R и состоит из генератора цифрового импульса PG, $2n$ двухвходовых мультиплексоров $MUX_{(i,j)}$ и одного синхронного D-триггера DFF. Генератор PG формирует импульс S, который проходит по двум симметричным путям, формируемым конфигурационными мультиплексорами. Конфигурация путей зависит от значения запроса C_i, подаваемого на селективные входы всех мультиплексоров.

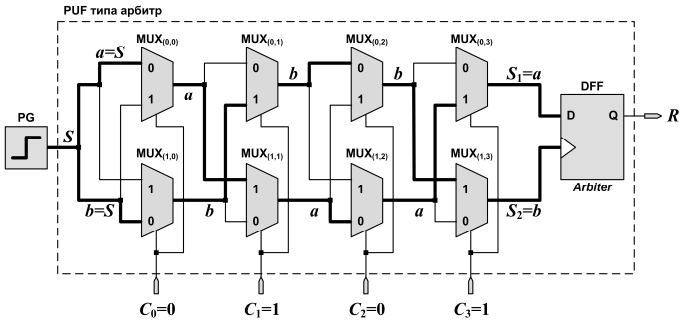

Рис. 1. PUF типа «арбитр» для n=4

Для n-разрядного запроса существует возможность сконфигурировать 2^n пар путей прохождения сигнала S. Триггер DFF выполняет роль арбитра, который определяет, какой из путей прохождения сигнала S оказался «длиннее». Для примера на рис.1 в случае R=0 путь S_1 является длиннее пути S_2 прохождения двух копий сигнала S (сигналы a и b). Аккумулируя выходные значения R для различных подаваемых k входных запросов C_i возможно формирование уникального неклонируемого k-разрядного идентификатора [6-9]. Однако для ПЛИС использование PUF типа «арбитр» является не эффективным в виду наличия заведомо ассиметричных конфигурируемых путей прохождения сигналов.

IV. Новая методика аппаратной реализации физически неклонируемых функций для ПЛИС

В данной работе предлагается модификация PUF типа «арбитр», заключающаяся не только в сравнении «протяженности» двух цифровых путей, но и в сравнении изменений скважности цифровых импульсов. Для возможности такого сравнения модифицируем арбитр DFF следующим образом (см. рис. 2).

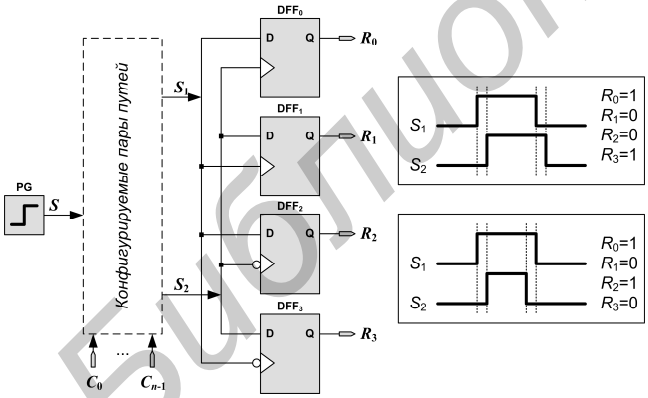

Рис. 2. Модифицированный арбитр и примеры вырабатываемых значений $R_0 - R_3$

Предложенный арбитр состоит из четырех D-триггеров $DFF_0 - DFF_3$, два из которых управляются задним фронтом сигнала синхронизации. Выходные сигналы конфигурируемых пар путей S_1 и S_2 подключены ко входам данных D и входам синхронизации триггеров так, как это показано на рисунке 2. Такое подключение позволяет контролировать моменты наступления передних и задних фронтов сигналов S_1 и S_2. Таким образом, при фиксированном запросе C различные по скважности сигналы S_1 и S_2 для одних и тех же заведомо ассиметричных путей будут вырабатывать различные ответы $R_0 - R_3$.

Проведенные эксперименты для ПЛИС типа FPGA Xilinx Spartan-3E [10], входящих в состав идентичных систем Digilent Nexys2 [11], показали практическую возможность реализации и высокую достоверность получения цифровых идентификаторов используя предложенную методику.

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

[2] Tuyls, P. Security with Noisy Data / P. Tuyls, B. Skoric, T. Kevenaar. – London: Springer, 2007. – 344 p.

[3] Ruhrmair, U. On the Foundations of Physical Unclonable Functions / U. Ruhrmair, J. Solter, F. Sehn // Cryptology ePrint Archive [Electronic resource]. – Mode of access: http://eprint.iacr.org/2009/277.pdf. - Date of access: 01.09.2011.

[4] Agarwal, A. Statistical Timing Analysis for Intra-Die Process Variations with Spatial Correlations / A. Agarwal, D. Blaauw, V. Zolotov // Computer Aided Design (ICCAD'2003): Proc. on Int. Conf., San Jose, CA, USA, 9-13 Nov., 2003. – P. 621-626.

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

[6] A technique to build a secret key in integration circuits for identification and authentication applications / J.W. Lee [et al.] // VLSI Circuits: Proc. of Symp., Honolulu, Hawai, 17-19 Jun., 2004. – P. 176-159.

[7] Delay-Based Circuit Authentication and Applications / B. Gassend [et al.] // Applied Computing (SAC'03): Proc. of the ACM Symp., Melburne, FL, USA, 9-12 March, 2003. – P. 294-301.

[8] 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, 27-29 Aug., 2007. – P. 189-195.

[9] Suh, G.E. Physical Unclonable Functions for Device Authentication and Secret Key Generation / G.E. Suh, S. Deyadas // Design Automation Conference (DAC'07): Proc. of 44th ACM/IEEE Conf., San Diego, CA, USA, 4-8 Jun., 2007. – P. 9-14.

[10] 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.

[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.