Кольцевой генератор и его неповторимый температурный коэффициент линейной регрессии

Прощеряков А.А.; Иванюк А.А.
Кафедра ВМиП
Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
e-mail: {proshcheryakov, ivaniuk}@bsuir.by

***Аннотация* — В докладе рассматривается вопрос реализации кольцевого генератора на инверторах в цепи обратной связи как элемента физически неклонируемой функции, приводится простейший метод подсчёта частоты кольцевого генератора, обращается внимание на уникальность изменения частоты генератора при изменении температуры устройства.**

Ключевые слова: физически неклонируемая функция, кольцевой генератор, температурный коэффициент линейной регрессии

I. Введение

Развитие технологического процесса производства программируемых логических интегральных схем (ПЛИС) привело к значительному удешевлению стоимости производства ПЛИС. При этом на базе ПЛИС стала возможной реализация практически любой пользовательской логики: от простейшего вычислительного устройства до многоядерных систем.

Однако крупные корпорации не спешат использовать данную аппаратную базу для реализации своих крупных проектов. Причиной этому является проблематичность защиты авторских прав на проектируемые и реализуемые компоненты интеллектуальной собственности, поскольку бит-файл конфигурации хранится во внешней памяти и, даже при её защите, во время передачи данных для конфигурирования устройства, файл конфигурации может быть перехвачен злоумышленниками и скопирован, что позволит выпускать продукцию без уплаты авторских вознаграждений. По самым скромным оценкам ущерб IT-отрасли от подобных действий «пиратов» достигает 100 млрд. долларов США [1]. Кроме этого у злоумышленников появляется возможность внедрять в реализованную систему вредоносные элементы, например аппаратные трояны [2].

Эффективным механизмом, нивелирующим вышеописанные проблемы, является использование так называемых физически неклонируемых функций (PUF, Physical Unclonable Functions), 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. PUF могут быть реализованы с использованием различных структур, одной из которых является кольцевой генератор.

II. Кольцевой генератор

Простейший кольцевой генератор (RO, ring oscillator) состоит из нечётного числа инверторов, соединённых последовательно, а выход последнего соединён со входом первого инвертора, образуя линию обратной связи [3]. Для управления таким генератором в его схему можно включить двухвходовый логический элемент «И», на один вход которого подаётся сигнал, определяющий начальное состояние генератора и задающий время его работы, на второй вход подаётся сигнал с последнего инвертора цепи обратной связи. Сигнал с выхода логического элемента «И» является входным сигналом первого инвертора цепи генератора. Обобщённая функциональная модель генератора представлена на рисунке 1.

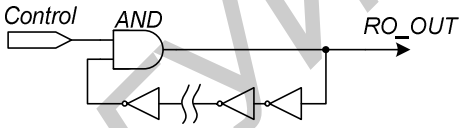

Рис.1. Функциональная модель кольцевого генератора

При нулевом значении сигнала *Control* генератор находится в состоянии равновесия, при этом на выходе логического элемента «И» значение сигнала всегда будет равно ‘0’, генератор, можно сказать, находится в режиме ожидания. При изменении сигнала *Control* на ‘1’, значение выходного сигнала логического элемента «И» ставится в прямую зависимость от выходного сигнала генератора *RO_OUT*, который пройдя через нечётное число инверторов изменится на противоположный, и опять же изменит значение выходного сигнала логического элемента «И», такая взаимозависимость сигналов и вызывает колебания данной системы.

Выходной сигнал генератора предлагается снимать именно с выхода логического элемента «И», поскольку он наименее смещён во времени относительно управляющего сигнала *Control*, и это смещение равно задержке логического элемента «И» (D_{AND}) как по фронту, так и спаду (см. рисунок 2) [4].

Частота такого генератора определяется суммой задержек инверторов, это время задержки (t_{inv}) зависит от множества параметров, таких как особенности производства ПЛИС, варьирования толщины проводников и полупроводников, напряжения питания и даже температуры окружающей среды, поэтому данный параметр можно считать случайным значением, но постоянным для одного инвертора [5].

Частота генератора f_{os} с числом инверторов равным N_{inv}, может быть определена следующей формулой:

$$f_{os} = \frac{1}{2\sum_{j=1}^{N_{inv}} t_{inv,j}}. \qquad (1)$$

Таким образом, индивидуальные задержки накапливаются и отображаются на частоте колебаний кольцевого генератора.

Для определения частоты генератора можно использовать следующий механизм. В качестве сигнала *Control* подаётся сигнал со значением ‘1’ с точно определённым интервалом, например, сигнал внешнего стабильного кварцевого осциллятора, обозначим длительность такого сигнала как D_S. Далее подсчитывается число фронтов сигнала *RO_OUT*, обозначим его как N_R. Тогда частоту f_{os} можно определить по формуле 2:

$$f_{os} = \frac{N_R}{D_s}. \qquad (2)$$

Однако такая методика даёт большую погрешность вычисления. Если частоты двух генераторов отличаются на небольшую величину и задержки распространения сигнала приблизительно равны ($D_{RO1} \approx D_{RO2}$), то N_R может оказаться одинаковым, но скважности последних импульсов (φ_1 и φ_2) будут отличаться, пример такого поведения показан на рисунке 2 [4].

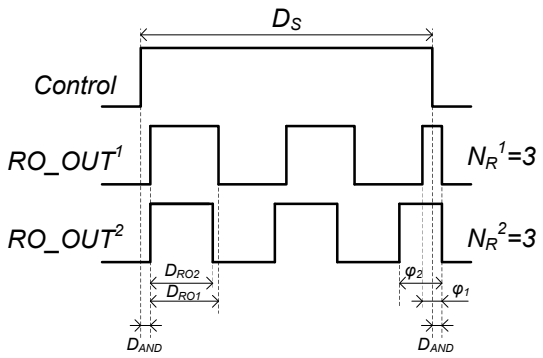

Рис.2. Различие временных характеристик различных кольцевых генераторов

Решение данной проблемы предложено в [4], где экспериментальным путём доказана возможность идентификации ПЛИС при увеличении времени D_S.

III. Влияние температуры на частотную характеристику генераторов

Сильное влияние на задержку прохождения сигнала в аппаратуре, произведённой по субмикронной технологии, оказывает температура. Доказано, что увеличение температуры на каждые 15°C приводит к 10%-15% увеличению задержки распространения сигналов [5].

Экспериментальные исследования [6] указывают на линейный характер зависимости между температурой и временем задержки в кольцевом генераторе. На рисунке 3 изображены графики, показывающие, как изменялась частота кольцевого генератора на трёх различных устройствах.

На графике следует отметить, что различные устройства имеют различные температурные коэффициенты линейной регрессии (27 kHz/°C для устройства s1, 54 kHz/°C для устройства s2 и 50 kHz/°C для устройства s3).

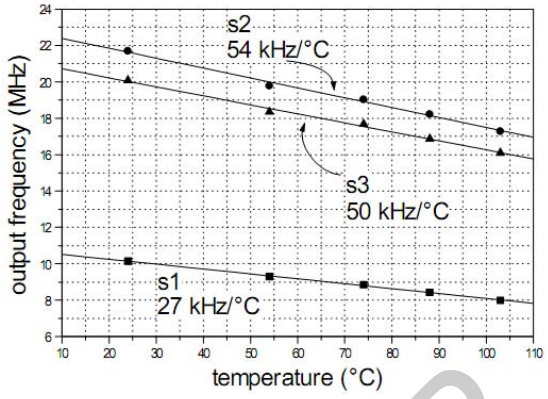

Рис.3. Графики изменения частоты RO при изменении температуры

Это различие делает невозможным идентификацию устройства на основе простого подсчёта числа колебаний генератора, без учёта данного коэффициента. Поскольку постоянность температуры устройства обеспечить практически невозможно, то игнорирование этого температурного коэффициента линейной регрессии может привести к ложноотрицательной идентификации устройства, как при проверке его оригинальности, так и при анализе на отсутствие вредоносных элементов в его структуре [2].

С учётом влияния температуры на частоту кольцевого генератора, формулу 1 можно представить в следующем виде:

$$f_{os}(T) = \frac{\tau \cdot T}{2\sum_{j=1}^{N_{inv}} t_{inv,j}}, \qquad (3)$$

где τ – температурный коэффициент линейной регрессии, кГц/°C;

T – температура интегральной схемы, °C.

Предполагается также возможность идентификации устройств по данному температурному коэффициенту, который, как отмечается выше, уникален для каждого устройства.

[1] Jorge Guajardo, Sandeep S. Kumar , Geert-Jan Schrijen, Pim Tuyls “Physical unclonable functions, FPGAs and public-key crypto for IP protection”, International Conference on Field Programmable Logic and Applications, 2007. FPL 2007, id: 10.1109/FPL.2007.4380646

[2] M. Tehranipoor, H. Salmani, Xuehui Zhang, Xiaoxiao Wang, R. Karri, J. Rajendran, K. Rosenfeld, “Trustworthy Hardware: Trojan Detection and Design-for-Trust Challenges”, Computer, Jul. 2011, pp.66 – 74.

[3] Xiaoxiao Wang and M. Tehranipoor, “Novel Physical Unclonable Function with process and environmental variations”, Design, Automation & Test in Europe Conference & Exhibition (DATE), 2010

[4] А. А. Иванюк, “Применение конфигурируемых генераторов импульсов для идентификации ПЛИС”, в печати

[5] Gang Qu and Chi-En Yin “Temperature-aware cooperative ring oscillator PUF”, IEEE International Workshop on Hardware-Oriented Security and Trust, 2009, pp.36 – 42.

[6] Eduardo Boemo and Sergio Lypez-Buedo, “Thermal Monitoring on FPGAs Using Ring-Oscillators”, Lecture Notes in Computer Science, №1304, pp.69-78, Berlin: Springer-Verlag, 1997.