СХЕМА УДАЛЕННОГО КОНТРОЛЯ ДЛЯ АКТИВНОГО ИЗМЕРЕНИЯ ЦИФРОВЫХ УСТРОЙСТВ

С.С. Заливако , А.А. Иванюк
Факультет электротехники и электроники, Наньянский технологический университет
Кафедра информатики, Белорусский государственный университет информатики и радиоэлектороники
Сингапур, Сингапур; Минск, Республика Беларусь
E-mail: zali0001@e.ntu.edu.sg, ivaniuk@bsuir.by

Проанализированы причины использования методов активного измерения при производстве интегральных схем. Предложен метод удаленного контроля, использующий реконфигурируемую физически неклонируемую функцию и адаптивный сигнатурный анализатор для генерирования ключей. Рассмотрены преимущества и недостатки предлагаемого метода.

Введение

В настоящее время наблюдается активный рост числа компаний без собственных производственных мощностей (англ. *fabless*). Такая организация производства интегральных схем (ИС) несет в себе определенные риски: изготовление бóльшего числа ИС, чем заказано; использование предоставленных проектов для своего производства и, как следствие, его значительное удешевление; задержка сроков с целью изготовления ИС по аналогичному проекту. В связи с вышеперечисленными причинами возникает необходимость в разработке таких методов защиты, которые могли бы в достаточной мере предотвратить подобные действия со стороны производителя.

I. Измерение цифровых устройств

Термин измерение интегральных схем (англ. *Integrated circuits (IC) metering*) и, в частности, цифровых устройств (ЦУ) был впервые предложен в 2001 году [1]. По определению F. Koushanfar под этим термином понимают совокупность протоколов безопасности, которые позволяют владельцам прав на объекты интеллектуальной собственности контролировать изготовленные по их проектам ИС. Таким образом, рассматриваемые методы позволяют уникально идентифицировать ИС и, следовательно, отслеживать их с помощью сгенерированной информации об устройстве. Выделяют две группы методов измерения ЦУ: пассивные и активные. Активное измерение помимо уникальной идентификации ЦУ (пассивные методы) позволяет владельцу прав на объект интеллектуальной собственности производить активацию, контроль и деактивацию устройства. Под активным контролем (измерением) понимают отслеживание числа активированных (разблокированных) ИС, которые были изготовлены по переданному для производителя проекту. Группа методов активного измерения базируется на модификации цифрового конечного автомата (ЦКА), который делается зависимым от реализации некоторой физически неклонируемой функции (ФНФ). Пример структурной схемы одного из методов названной группы приведен на рис. 1.

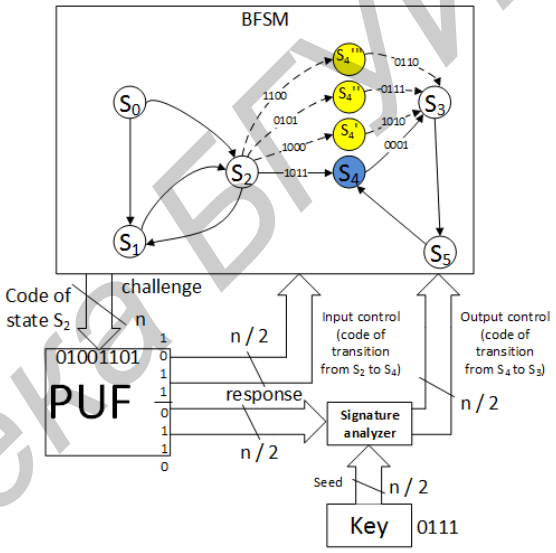

Рис. 1 – Схема метода активного измерения

На этапе проектирования ЦУ разработчик расширяет ЦКА за счет добавления фиктивных состояний и переходов между ними (на рис. 1 дублируется состояние S_4), а также реализует ФНФ. Изначально ЦУ является деактивированным: без знания структуры ЦКА попасть из состояния S_2 в состояние S_3 затруднительно, поскольку код перехода из S_2 в S_4 является зависимым от ответа ФНФ, а код перехода из S_4 в S_3 – от ответа ФНФ и ключа, предоставляемого разработчиком ЦУ. Соответственно, угадывание или перебор упомянутых выше кодов в случае их большого количества (экспоненциально зависящего от n) является NP-трудной задачей. Рассмотрим процесс активации ЦУ. Код состояния S_2 является n-битным запросом к ФНФ, ответ на который (также n-битное число) разбивается на 2 $n/2$-битных числа: первое используется для кодирования перехода из состояния S_2 в состояние S_4, а второе является источником получения кода перехода из S_4 в S_3. Далее проектировщик ЦУ предоставляет ключ, который является инициализирующим числом для сигнатурного ана-

лизатора (англ. *Signature analyzer*). На основании ключа и второй половины ответа ФНФ генерируется корректный код перехода из состояния S_4 в состояние S_3. Таким образом, ЦУ становится работоспособным (активированным). Ответы ФНФ являются уникальными для каждого ЦУ, поскольку зависят от физических вариаций технологического процесса изготовления, что, в свою очередь, обеспечивает уникальность ключа, генерируемого на основании зависимости от пары запрос-ответ ФНФ.

II. Удаленный контроль

В случае истечения времени действия ключа, несанкционированной активности пользователя при работе с ЦУ (например, попытке переписывать запрещенные к записи участки памяти), кражи ключа возникает необходимость в удаленном контроле и замене ключа. Для осуществления такой возможности предлагается использовать реконфигурируемые ФНФ (рФНФ)[2] и адаптивный сигнатурный анализатор (АСА) для быстрого перегенерирования ключа.

Реконфигурируемая ФНФ представляет собой систему, состоящую из реконфигурируемой логики, которая формирует запросы к некоторой встроенной ФНФ. Изменения конфигурации рФНФ влекут за собой изменения запросов и, соответственно, ответов встроенной ФНФ. Таким образом, ответ рФНФ можно представить в виде функции множества параметров $rPUF(\theta_1, \theta_2, \ldots, \theta_n, c) = r$, где $\theta_1, \theta_2, \ldots, \theta_n$ – параметры конфигурируемой логики рФНФ, n – количество параметров рФНФ, c – запрос к рФНФ, r – ответ рФНФ.

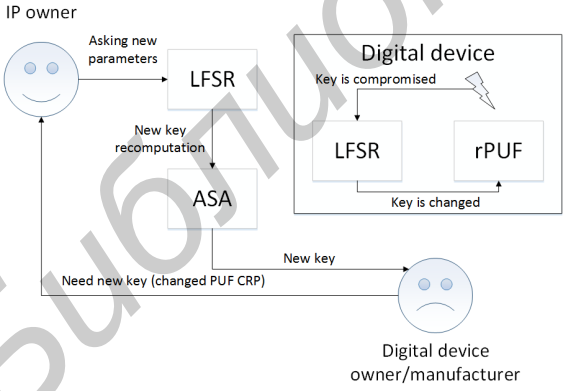

Рис. 2 – Схема удаленного контроля

Пронумеруем множества возможных значений параметров $((\theta_1^i, \theta_2^i, \ldots, \theta_n^i)$, i - порядковый номер некоторого множества параметров). Пусть k – количество множеств возможных значений параметров рФНФ, тогда для замены параметров можно использовать линейный сдвиговый регистр с обратной связью (англ. *Linear Feedback Shift Register (LFSR)*), примитивный полином для которого является секретным. Для повышения безопасности LFSR так же можно сделать реконфигурируемым. Схема предлагаемого метода удаленного контроля приведена на рис. 2.

Рассмотрим алгоритм работы удаленного контроля на примере ЦКА, приведенного на рис. 1. Пусть номер состояния S_2 кодируется числом 01001101_2, а ответ рФНФ на данный запрос число 10110110_2. Используя первую часть числа, получаем код перехода из состояния S_2 в состояние S_4 (1011_2), вторую часть числа (0110_2) обрабатываем на АСА ($01_2 \oplus 10_2 = 11_2$), а также производим сложение по модулю два с ключом 0111_2, чтобы получить значение кода перехода из S_4 в S_3 (0001_2). Далее в результате того, что ключ утрачивает свою актуальность в виду описанных выше причин, параметры рФНФ меняются принудительно или по запросу владельца ЦУ, и уже на запрос 01001101_2 ответом является число 11001110_2. Таким образом, переход из S_2 в S_4 кодируется числом 1100_2, а переход из S_4 в S_3 после обработки на АСА (поскольку изменился только один бит числа $0110_2 \rightarrow 1110_2$, то необходимо произвести пересчет предыдущего значения 11_2 с учетом изменения одного бита $11_2 \oplus 11_2 = 00_2$) и при сложении по модулю два со старым ключом получается код 0111_2, который не соответствует значению, на котором осуществляется переход. Таким образом, необходимо изменить ключ 0111_2 на 0001_2, чтобы код перехода был корректен. Изменение параметров рФНФ делает ключ, используемый в данный момент недействительным и, соответственно, деактивирует ЦУ. АСА позволяет быстро пересчитывать значение, используемое для генерирования ключа.

Заключение

Предложен метод удаленного контроля для активного измерения ЦУ, основанный на применении рФНФ и АСА для генерирования (перегенерирования) ключа для активации. К преимуществам предлагаемого подхода можно отнести гибкость изменения, сложность подделки и адаптивное обновление ключа, небольшой прирост аппаратных ресурсов по сравнению с оригинальным методом активного измерения. Недостатком является уязвимость LFSR, если он реализован без должной обфускации (т.е. возможно установить примитивный полином по проектной информации) или реконфигурируемости.

1. Koushanfar, F. Intellectual property metering / F. Koushanfar, G. Qu, M. Potkonjak. // International Workshop on Information Hiding (IHW). – London: Springer, 2001. – P. 81—95.
2. Kursawe, K. Reconfigurable physical unclonable functions enabling technology for tamper-resistant storage / K. Kursawe, A.-R. Sadeghi, B. Scoric, P. Tuyls // Hardware-Oriented Security and Trust (HOST), San Francisco, USA, July 27, 2009. – New York: IEEE, 2009. – P. 22–29.