ОБЗОР МЕТОДОВ АКТИВНОГО ИЗМЕРЕНИЯ ЦИФРОВЫХ УСТРОЙСТВ С ИСПОЛЬЗОВАНИЕМ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Заливако С. С.

Иванюк А. А. – д-р. техн. наук, доцент

В работе приведены основные методы активного измерения с использованием физически неклонируемых функций. Все методы основаны на модификации конечного автомата цифрового устройства и его блокировании до тех пор пока не будет дана возможность легального использования. Ключ для разблокирования основан на данных, генерируемых физически неклонируемой фунцией, поэтому он будет уникальным для каждой произведенной интегральной схемы.

Процесс изготовления интегральных схем (ИС) по технологии КМОП усложняется с каждым годом, что влечет за собой увеличение стоимости оборудования и, как следствие, производства в целом. В связи с этим обстоятельством все большее число компаний-разработчиков вынуждено заказывать производство ИС по своим проектам на внешних фабриках. Существующее законодательство и средства защиты от нелегального копирования объектов авторского права не позволяют защитить разработчиков проектных описаний. Такое состояние дел вынуждает разработчиков использовать специальные методы предотвращения нелегального копирования проектных описаний, которые позволяют не только доказать авторство (идентифицировать), но и контролировать число выпущенных ИС.

Одним из таких методов является *активное измерение*. Впервые данный термин был упомянут в работе [1] в 2007 году. Опишем производственный процесс, в котором используется активное измерение для защиты прав разработчика на проектное описание.

Изначально разработчик создает проектное описание на HDL-языке (англ. Hardware Description Language). Такому описанию соответствует цифровой конечный автомат (ЦКА), который модифицируется путем добавления новых (фиктивных) состояний и/или переходов между ними. В результате чего получается расширенный цифровой конечный автомат (РЦКА). Далее происходит процесс синтеза, связывание абстрактных компонентов с определенными физическими ресурсами кристалла (англ. Map), размещение компонентов в логические ячейки (англ. Place), соединение компонентов внутренними трассировочными ресурсами (англ. Route). В итоге разработчик получает файлы готового проектного описания и тестовые векторы к ним. Эта информация и передается производителю, который, в свою очередь, осуществляет производство заказанного числа ИС по переданному проектному описанию. После создания ИС является заблокированной, поэтому производитель посылает разработчику ключ, который генерируется как отклик физически неклонируемой функции (ФНФ) [2]. По переданному ключу и структуре РЦКА разработчик посылает производителю ключ для разблокировки устройства. После чего ИС подвергается разблокировке, тестируется и в готовом виде возвращается разработчику. Отметим, что ключ для разблокировки генерируется на основе отклика ФНФ, поэтому является уникальным для каждой ИС, неклонируемым и невоспроизводимым, т.е. обладание ключом для конкретной ИС не даст производителю или злоумышленнику никаких преимуществ, кроме обладания системой, права на использования которой уже даны разработчиком.

Рассмотрим возможные схемы модификации конечного автомата. В первом случае для формирования РЦКА в исходный ЦКА добавляются избыточные состояния. Пусть конечный автомат имеет m исходных состояний, добавим такое число состояний, чтобы суммарное их число было 2^k, причем $2^k - m >> m$. Предположим, что в исходном ЦКА есть единственное состояние (нулевое состояние), попадание в которое позволяет устройству работать корректно. Тогда производитель практически не может попасть из любого произвольно выбранного состояния (в т.ч. избыточного) в нулевое, поскольку не имеет сведений о структуре конечного автомата. Выбор состояния осуществляется на основе отклика ФНФ, который, в свою очередь, является уникальным для каждой ИС и вероятность попасть в нулевое состояние крайне мала (2^{-k}). Схематично эта структура изображена на рисунке 1. Этот подход предложен в работе [1].

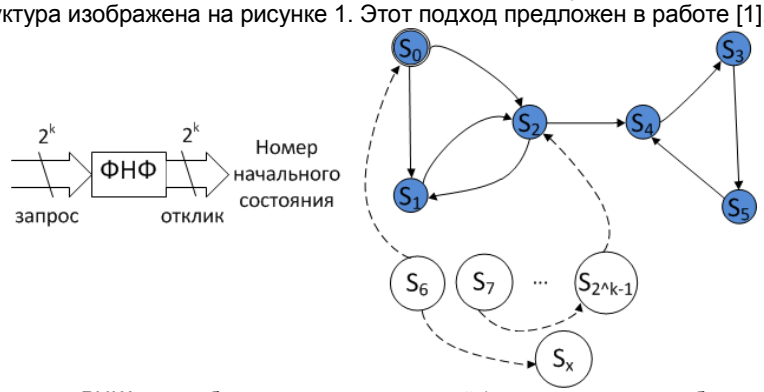

Рис. 1 – Структура РЦКА при добавлении новых состояний (темными кружками обозначены изначальные состояния, светлыми – добавленные, сплошными стрелками – изначальные переходы, пунктирными – добавленные).

В работе [3] предложен другой алгоритм построения РЦКА. В данном случае некоторые состояния исходного ЦКА дублируются и к ним добавляются избыточные переходы. Выбор переходов, обеспечивающих корректную работу устройства осуществляется на основании отклика ФНФ, а также ключа, который предоставляется разработчиком. Поскольку выбор переходов и ключ зависят от ФНФ, они будут уникальны для каждой ИС. Данный подход показан на рисунке 2.

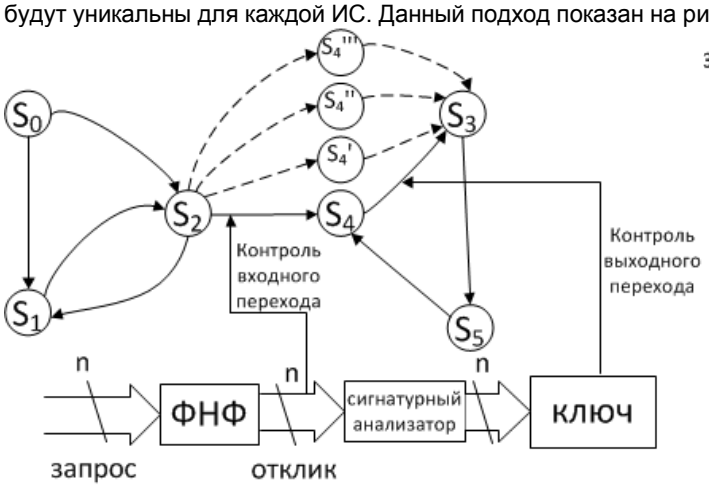

Рис. 2 – Структура РЦКА при добавлении избыточных состояний, переходов и сигнатурного анализатора.

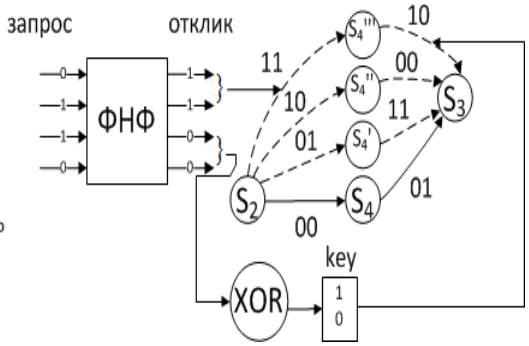

Рис. 3 – Выбор необходимых переходов сигнатурным анализатором.

На рисунке 3 показано, как осуществляется выбор пары переходов между исходным и избыточным состоянием и наоборот. В данном примере применяется побитовое «исключающее или» для половины бит отклика ФНФ. Заметим, что алгоритм работы сигнатурного анализатора может быть гораздо сложнее.

Аппаратурные затраты в первом случае пропорциональны *k*, т.е. для того, чтобы поддержать дополнительно 2^k состояний необходимо порядка *k* триггеров. Таким образом, экспоненциальный рост числа состояний влечет за собой линейный рост аппаратурных затрат.

Во втором случае дополнительно нужно обеспечить работу сигнатурного анализатора. В простейшем случае, описанном выше, для этого требуется k-входовой элемент XOR.

ФНФ в двух случаях используется для генерирования уникального идентификатора цифрового устройства. Это может быть реализовано, например, с использованием ФНФ типа арбитр [4], а также ФНФ на основе статического ОЗУ [5]. Аппаратурные затраты на реализацию упомянутых ФНФ также невелики и их использование оправданно.

Рассмотренные методы могут быть успешно использованы для защиты авторских прав на проектные описания. В силу использования ФНФ в качестве идентификатора клонирование проекта на идентичной интегральной схеме не даст должного результата, т.к. отклик будет другой, и, соответственно, ранее полученный ключ не подойдет.

Несмотря на явные преимущества такого подхода в настоящее время некоторые задачи являются нерешенными до сих пор:

- стабилизация откликов ФНФ. Как известно, отклики ФНФ могут меняться в силу различных причин: изменение температуры окружающей среды, вариации питающего напряжения, старение ИС и т.п.;
- быстрое изменение РЦКА разработчиком для того, чтобы заблокировать функциональность ИС удаленно;
- обфускация структуры РЦКА для затруднения атак обратного проектирования;
- сложные алгоритмы сигнатурного анализа для затруднения установления зависимости между произвольным откликом ФНФ и ключом.

Список использованных источников:

1. Alkabani, Y., Koushanfar, F. Active hardware metering for intellectual property protection and security // USENIX Security Symposium. – 2007. – p. 291 – 306.
2. Tuyls, P. Security with Noisy Data / P. Tuyls // Springer. – New York, 2007. – 339 p.
3. Alkabani, Y., Koushanfar, F., Potkonjak, M. Secure active IC Metering Techniques for Piracy Avoidance and Digital Rights Management // Information Forensics and Security, IEEE Transactions. – 2012. – Vol. 7(1). - p. 51 – 63.
4. Иванюк, А. А. Аппаратная реализация алгоритма идентификации ПЛИС на основе физически неклонируемой функции / А. А. Иванюк // Информационные технологии и системы 2013 (ИТС 2013): материалы междунар. науч. конф., БГУИР, Минск, Беларусь, 23 октября 2013 г. / редкол. : Л.Ю. Шилин [и др]. – Минск : БГУИР, 2013. – с. 184–185.
5. Заливако, С.С. Схемная реализация комбинированной физически неклонируемой функции для генерирования действительно случайных числовых последовательностей / С.С. Заливако, А.А. Иванюк // Доклады БГУИР. – 2013. - № 7(77). – С. 37-43.