АВТОМАТИЗАЦИЯ ПРОЕКТИРОВАНИЯ

УДК 004.056.53, 681.32

С.С. Заливако, А.А. Иванюк

ОБЗОР МЕТОДОВ АКТИВНОЙ ИДЕНТИФИКАЦИИ ЦИФРОВЫХ УСТРОЙСТВ

Рассматриваются существующие методы активной идентификации цифровых устройств и приводится обоснование необходимости использования таких методов компаниями – проектировщиками интегральных схем. Представляется описание методов, основанных на модифицирующих преобразованиях цифрового конечного автомата и протоколах асимметричного шифрования. Анализируются преимущества и недостатки методов активной идентификации и предлагаются пути решения проблем, актуальных в настоящее время.

Введение

Процесс производства современных интегральных схем (ИС) состоит из двух этапов: проектирования и изготовления. На первом этапе разработчик, как правило, при помощи системы автоматизированного проектирования (САПР) создает HDL-описание, производит RTL- и технологический синтез, связывание абстрактных компонентов с определенными физическими ресурсами кристалла, проектирование топологии ИС, размещение компонентов в логические ячейки, соединение компонентов внутренними трассировочными ресурсами, а также параметрическое моделирование созданного проектного описания. На втором этапе, получив проектное описание ИС, производитель осуществляет изготовление полупроводниковых пластин и их обработку, фотолитографию, разделение пластин на кристаллы, монтаж в корпус, герметизацию, электрические измерения, выходной контроль (тестирование), маркировку и упаковку. В результате получается готовая ИС, которая может быть самостоятельным цифровым устройством (ЦУ) либо системой на кристалле, а также использоваться как компонент более сложной системы.

В настоящее время стоимость средств производства ИС с использованием современных технологических процессов (от 45 нм и меньше) оценивается в несколько миллиардов долларов США [1]. В связи с этим большое количество компаний избрало горизонтальную бизнес-модель [2] для выхода на рынок полупроводниковых устройств. Данная тенденция привела к тому, что за последние 20 лет значительная часть продаж ИС (около 30 %) приходится на компании, не обладающие собственными производственными мощностями (рис. 1). Таким образом, горизонтальная модель ведения бизнеса позволяет небольшим компаниям – проектировщикам ИС конкурировать с такими крупными производителями, как Intel, Samsung, Sony, Texas Instruments и др. Другой важной тенденцией, обусловленной текущим состоянием рынка полупроводниковых устройств, является разработка IP-компонент [3] (Intellectual Property – IP) компаниями – поставщиками САПР.

В связи с тем что компании без собственных производственных мощностей доказали свою состоятельность и заняли значительную часть рынка, они, разумеется, столкнулись с новыми проблемами, связанными с нелегальным копированием их проектов ИС и подделкой изготовленных полупроводниковых устройств [4]. Законодательство не позволяет защитить права интеллектуальной собственности на разработанные такими компаниями IP-компоненты. Это отчасти привело к тому, что доля поддельных (или нелегально изготовленных) ИС составляет сегодня порядка 5 % [5], а также к ежегодным потерям порядка 4 млрд долл. Существует ряд критических приложений для ИС (системы для обработки персональных данных, медицинская электроника, вооружение и др.), для которых характерны более жесткие требования к неклонируемости, защите от нелегального копирования и обратного проектирования. Соответственно,

для перечисленных выше типов полупроводниковых устройств наличие данной проблемы представляет собой серьезную угрозу для безопасности.

Рис. 1. Объемы продаж компаний – производителей полупроводниковых устройств [1]

Одним из эффективных методов защиты проектных описаний от несанкционированного копирования и клонирования является идентификация аппаратного обеспечения (Hardware Metering), которая впервые была рассмотрена в работах [6, 7]. Под термином «идентификация» понимается считывание данных с аппаратного обеспечения, которое помогает распознать устройство и доказать принадлежность к обладателю прав интеллектуальной собственности на него. Изначально это понятие было определено для пассивной идентификации аппаратного обеспечения (Passive Hardware Metering) в качестве протокола безопасности, который позволяет компании-проектировщику осуществить распознавание изготовленного ЦУ. Особенностью активной идентификации аппаратного обеспечения (Active Hardware Metering) является возможность контроля ЦУ (ограничения или отключения некоторых его функций) после его изготовления, что позволяет решать проблемы, характерные для горизонтальной бизнес-модели.

1. Классификация методов идентификации аппаратного обеспечения

Методы идентификации аппаратного обеспечения (рис. 2) в настоящее время делятся на два больших класса: пассивные и активные [8]. Методы пассивной идентификации позволяют уникально идентифицировать IP-компоненты, входящие в состав ЦУ, или ЦУ целиком. Термин «пассивный» означает, что владелец прав на проектное описание может установить, является ли ЦУ подлинным, но не может изменить или в дальнейшем контролировать его функциональность. Методы пассивной идентификации, в свою очередь, также подразделяются на два подкласса: пассивные функциональные и нефункциональные. Нефункциональные методы основаны на уникальной идентификации ЦУ, которая не зависит от его функциональности. Вместе с тем функциональные методы генерируют уникальный идентификатор, в основе которого лежит определенная функция ЦУ. Оба класса методов могут использовать как воспроизводимые, так и неклонируемые (невоспроизводимые) идентификаторы.

В отличие от пассивной идентификации методы активной идентификации предоставляют владельцу прав собственности на ЦУ или его проектное описание возможность включения или отключения функциональности ЦУ для предотвращения его несанкционированного использования. В соответствии с определением методы активной идентификации похожи на методы пассивной функциональной идентификации, поскольку используют некую функцию ЦУ в качестве блокирующей схемы, которая позволяет ЦУ работать в обычном или ограниченном (неактивном) режиме. Особенностью блокирующей схемы в методах активной идентификации является то, что она проектируется зависимой от идентификатора ЦУ и, следовательно, попытки изменения значения идентификатора приведут к нарушению функционирования ЦУ. Методы активной идентификации, в свою очередь, подразделяются на два подкласса: закрытые

и открытые. В закрытых методах для построения блокирующей схемы применяются только средства той IP-компоненты, которую планируется защитить. В открытых методах совместно с внутренними средствами используются также дополнительные (внешние) модули или устройства.

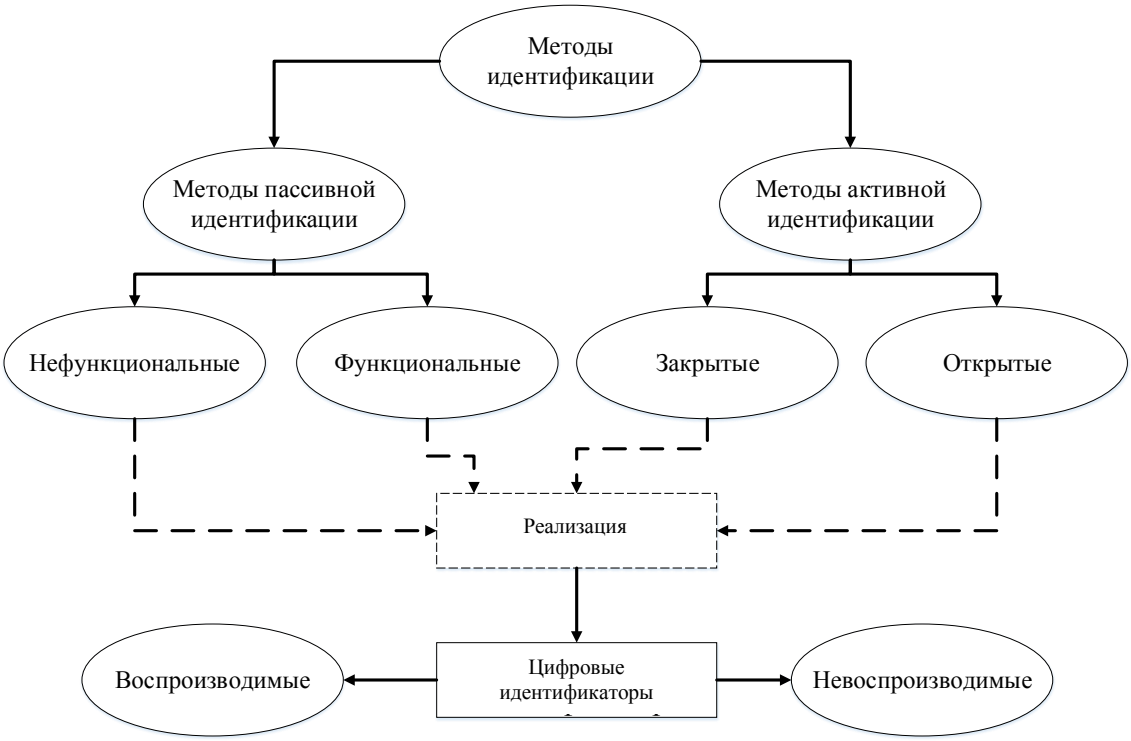

Рис. 2. Классификация методов идентификации аппаратного обеспечения

Рассмотрим подробнее методы активной идентификации.

2. Методы активной идентификации цифровых устройств

Основной особенностью методов активной идентификации является возможность активного контроля над ЦУ после изготовления. Благодаря данной особенности все методы активной идентификации применяют два базовых компонента для практической реализации: блокирующую схему и источник энтропии для генерирования секретных криптографических ключей, которые обладают свойствами уникальности, неклонируемости, случайности, а также не изменяются при внешнем воздействии на одном и том же ЦУ. Текущие реализации методов активной идентификации в качестве блокирующей схемы используют либо модифицированный цифровой конечный автомат (ЦКА) [9–11], либо схему на базе комбинационной логики [12]. Применение физически неклонируемых функций (ФНФ) [13] позволяет генерировать уникальные, неклонируемые, невоспроизводимые и надежные идентификаторы ЦУ, которые могут быть использованы в качестве секретных ключей. Блокирующая схема проектируется зависимой от ключей, генерируемых ФНФ, что позволяет ей быть уникальной для каждого ЦУ. Таким образом, даже обладание секретной информацией для разблокирования одного ЦУ не даст злоумышленнику существенных преимуществ для взлома другого ЦУ, изготовленного по тому же проекту.

Общая схема активной идентификации ЦУ изображена на рис. 3 [9], в качестве блокирующей схемы используется ЦКА, а в качестве источника энтропии – ФНФ. Как правило, модель активной идентификации включает две стороны, взаимодействующие между собой: компанию, проектирующую ЦУ и владеющую правами интеллектуальной собственности на

проект, и компанию-изготовитель, которой передается необходимое для производства ИС проектное описание.

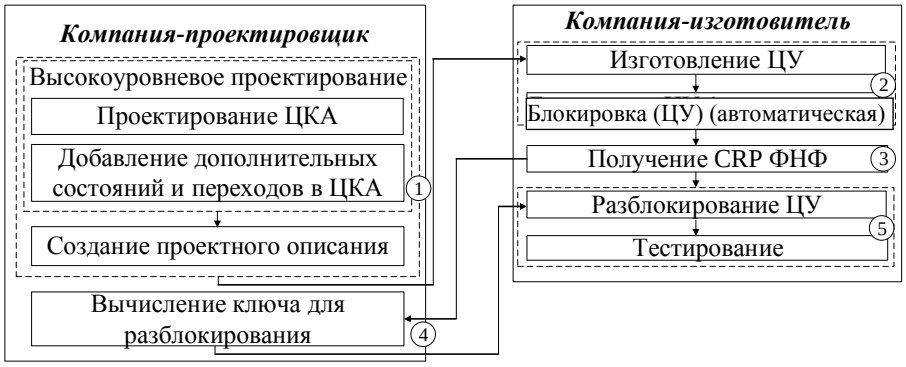

Рис. 3. Общая схема функционирования методов активной идентификации

Рассмотрим этапы проектирования и изготовления ЦУ:

1. Проектировщик создает начальное HDL-описание и проектирует структуру ЦКА как основу для блокирующей схемы. Далее разработчик расширяет структуру исходного ЦКА с помощью добавления фиктивных состояний и (или) переходов. Таким образом, получается расширенный ЦКА (РЦКА), который и является блокирующей схемой. После этого в результате синтеза создается готовое проектное описание, которое отправляется компании – изготовителю ЦУ.

2. Компания-изготовитель производит заказанное проектировщиком число копий ЦУ, каждое из которых содержит неклонируемый идентификатор, реализованный, как правило, с помощью слабой ФНФ совместно с кодами коррекции ошибок [14]. Для повышения надежности ФНФ эталонные пары «запрос – ответ» (Challenge Response Pairs – CRP) сохраняются заранее в энергонезависимой памяти, а затем используются для корректировки нестабильных ответов. На этом этапе возникает риск, что производитель, зная проектное описание ЦУ, может произвести большее число нелегальных копий. Именно поэтому функциональность изготовленного ЦУ изначально находится в заблокированном состоянии и разблокировать его может только обладатель прав интеллектуальной собственности на проектное описание, т. е. компания-проектировщик.

3. Далее производитель извлекает информацию о CRP с помощью изготовленного ЦУ и отправляет их компании-проектировщику. Поскольку структура РЦКА зависит от ФНФ, функциональность ЦУ может быть восстановлена тогда и только тогда, когда известны и структура РЦКА, и множество CRP ФНФ.

4. Проектировщик вычисляет лицензионный ключ, который способен восстановить функциональность ЦУ на основании CRP, предоставленных производителем. Вычисленный ключ применим только к конкретному ЦУ, поскольку информация о CRP не может быть воспроизведена на другом ЦУ, реализованном по такому же проекту, и, следовательно, является уникальной и неклонируемой.

5. На последнем этапе компания-изготовитель осуществляет разблокировку готового ЦУ с использованием лицензионного ключа, предоставленного проектировщиком, а также тестирование функциональности ЦУ с целью подтверждения его работоспособности.

Таким образом, методы активной идентификации дают возможность предотвратить нелегальное копирование проектных описаний ЦУ сторонней компанией-изготовителем.

2.1. Закрытые методы активной идентификации

Особенность закрытых методов активной идентификации заключается в том, что блокирующая схема формируется с помощью создания фиктивных состояний и (или) переходов ЦКА [9, 10].

Пусть первоначально спроектированный ЦКА содержит M состояний, что может быть реализовано с использованием как минимум $K = \lceil \log_2(M) \rceil$ триггеров. Тогда для формирования РЦКА требуется добавить в исходный ЦКА дополнительно M_1 состояний, что приведет к суммарному расходу $K_2 = \lceil \log_2(M + M_1) \rceil$ триггеров. Добавочные состояния должны быть дополнены переходами, которые сохранят связность графа, соответствующего РЦКА, т. е. каждое из добавленных состояний должно быть достижимо из уже имеющихся в ЦКА. Таким образом, число добавочных триггеров может быть вычислено как $K_1 = K_2 - K$. Отметим, что экспоненциальный рост числа состояний в РЦКА вызовет только линейный рост числа триггеров, поэтому можно добавить столько состояний, чтобы $M_2 >> M$.

ЦУ должно иметь в своем составе реализацию ФНФ для генерирования кода случайного начального состояния, который является ответом на заранее определенный запрос, формируемый компанией-проектировщиком в виде тестового вектора. Поскольку для реализации РЦКА требуется K_2 триггеров, то размерность ответа ФНФ должна составлять K_2 бит.

После инициализации ФНФ генерирует код начального состояния в РЦКА (рис. 4). На рисунке состояния первоначально спроектированного (оригинального) ЦКА обозначены черным цветом, а добавочные состояния – белым. Кодирование состояний РЦКА осуществляется с помощью битовой карты, номера бит в которой определяются случайным образом компанией-проектировщиком: биты, обозначенные на рис. 4 черным цветом, предназначены для кодирования состояний первоначального ЦКА, а белым – для кодирования остальных (добавочных) состояний соответственно. Все добавочные состояния таковы, что если пользователь не знает структуры РЦКА, то он не может выйти из этих состояний и достичь начального состояния (S_0) оригинального ЦКА. При этом состояния S_0 можно достичь тогда и только тогда, когда код состояния S_x окажется среди кодов состояний первоначально спроектированного ЦКА, однако вероятность такого события крайне мала: $P_g = 2^{-K_1}$ и $2^{K_2} >> 2^K$. Следовательно, $2^{-K_1} \approx 0$.

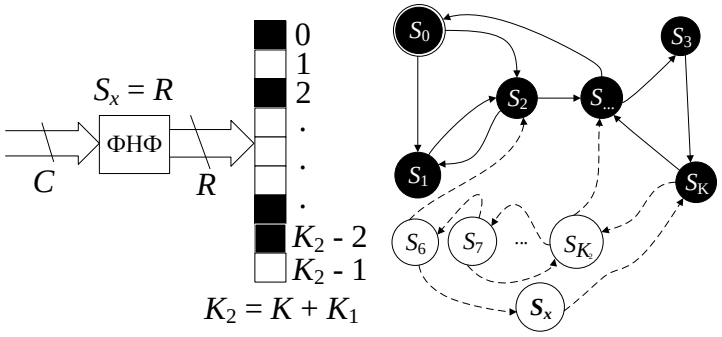

Рис. 4. Схема активной идентификации с использованием избыточных состояний (S_x обозначает начальное состояние, $0 \le x \le K_2$)

РЦКА проектируется таким образом, чтобы путь из каждого добавочного состояния в состояние S_0 был единственным и, соответственно, осуществление его подбора было бы затруднено. Следовательно, злоумышленник не сможет восстановить функциональность ЦУ без знания реальной структуры РЦКА, которая является секретной и не передается производителю на этапе 2 (см. общую схему методов активной идентификации). Таким образом, путь из состояния S_x в S_0 (последовательность кодов переходов) и является ключом, который уникален для каждого изготовленного ЦУ, поскольку выбор начального состояния РЦКА (S_x) полностью зависит от кода, сгенерированного ФНФ.

Другой закрытый метод активной идентификации, основанный на применении ЦКА в качестве блокирующей схемы, был предложен в работе [11]. В отличие от метода, описанного выше, генерируются не дополнительные состояния ЦКА, а копии, дублирующие некоторые существующие состояния с соответствующими переходами. Таким образом, использование описываемого метода влечет за собой меньшие затраты на генерирование дублирующих состояний, но усложняет механизм работы с ФНФ.

Пусть некоторое состояние S_i выбрано для дублирования и создана копия S_{ij}. Тогда все переходы из состояния S_i и в него также дублируются для S_{ij}. Как и в предыдущем методе, в качестве источника энтропии была выбрана ФНФ, запрос для которой (C) является кодом состояния S_i, а часть ответа (i_c) используется в качестве кода перехода в копию этого состояния (S_{ij}). В свою очередь, вторая часть ответа ФНФ (seed) применяется как инициализирующее значение в блоке коррекции, чтобы сгенерировать код перехода, соответствующего выходу из состояния S_{ij} (o_c). Допустим, начальным состоянием было выбрано S_i, тогда после инициализации ЦУ ФНФ сгенерирует код перехода в состояние S_{ij}, код выхода из которого известен только проектировщику. Таким образом, для выхода из этого состояния требуется сгенерировать код выходного перехода, алгоритм построения которого основан на второй части ответа ФНФ и ключе (key) (рис. 5), т. е. $o_c = h(\text{seed}, \text{key})$, где h – хеш-функция, реализуемая блоком коррекции. Только знание ответа ФНФ и секретного ключа позволит сгенерировать код перехода, позволяющего выйти из состояния-копии и таким образом вернуть работоспособность ЦУ.

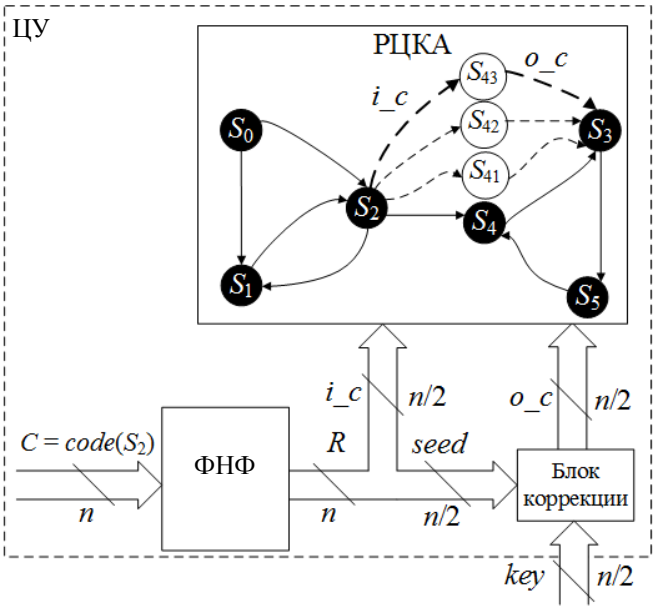

Рис. 5. Схема активной идентификации с использованием копий исходных состояний

Для пояснения описанной выше схемы приведем пример с использованием конкретных числовых значений. Допустим, что в ФНФ поступил запрос «01001101», который является кодом состояния S_2, выбранного в качестве начального состояния ЦКА. Далее ФНФ генерирует ответ «11001010», поэтому после инициализации ЦУ i_c = «1100». Не нарушая общности, предположим, что блок коррекции в данном случае реализует функцию исключающего ИЛИ (XOR), однако он может использовать и более сложное преобразование значений seed и key, например, с помощью адаптивного сигнатурного анализатора [15]. Тогда, для того чтобы сгенерировать код выходного перехода из состояния S_{43} (o_c = «0110»), необходимо подать в блок коррекции в качестве ключа значение «1100»: действительно, операция исключающего ИЛИ для ключа и второй части ответа ФНФ («1010») в результате даст необходимое значение, которое применимо для осуществления перехода в состояние S_3. Отметим, что количество бит в ответе ФНФ должно быть достаточным для невозможности применения метода полного перебора вариантов в качестве криптографической атаки, т. е. время подбора правильного кода выходного перехода должно быть достаточно велико для применения на практике [16]. Таким образом, описанный метод расходует меньшее количество аппаратурных ресурсов, но требует ФНФ большей разрядности и надежный блок коррекции, реализующий нелинейную хеш-функцию, затрудняющую криптографические атаки на секретные ключи.

2.2. Открытые методы активной идентификации

В отличие от закрытых открытые методы активной идентификации используют алгоритмы асимметричного шифрования для проектирования блокирующей схемы, что, соответственно, требует наличия внешних ключей для осуществления работы протокола. Впервые такой метод был упомянут в работе [12]. Общая схема предложенного метода представлена на рис. 6.

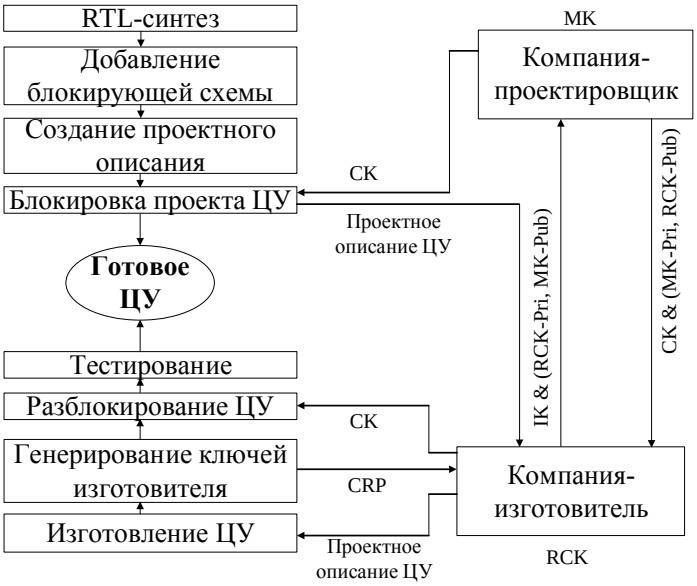

Рис. 6. Схема активной идентификации с использованием алгоритма асимметричного шифрования

В соответствии с алгоритмами криптографии с открытым ключом проектировщику необходимо сгенерировать пару ключей (Master Keys – MK). Закрытый ключ (MK-Pri) должен держаться в секрете и не передаваться ни при каких обстоятельствах, а открытый ключ (MK-Pub) передается по незащищенным каналам и поэтому известен компании-изготовителю. Как правило, эта пара ключей генерируется для каждого ЦУ с использованием программного обеспечения, которое может генерировать пары ключей для определенного протокола шифрования. Блокирующая схема реализована на уровне RTL и встроена в проектное описание ЦУ.

Согласно предложенному методу блокирующая схема проектируется с помощью элементов исключающего ИЛИ, соединенных с регистром хранения общего ключа (Common Key – CK). Только наличие правильного CK переводит ЦУ в нормальный режим работы, в противном случае поведение ЦУ может быть непредсказуемым. Для предотвращения похищения CK на стороне проектировщика он генерируется случайным образом для каждого конкретного ЦУ. После внедрения блокирующей схемы и генерирования всех необходимых ключей (MK, CK) проектное описание отправляется компании-изготовителю.

Для активации ЦУ производитель обязан сгенерировать пару секретных ключей (Random Chip Keys – RCK) асимметричного шифрования (закрытый ключ RCK-Pri и открытый ключ RCK-Pub) после изготовления каждого ЦУ с помощью встроенной ФНФ. Как правило, ответы, сгенерированные ФНФ, используются в качестве инициализирующего значения для программного обеспечения, генерирующего пары секретных ключей асимметричного шифрования. Далее производитель осуществляет шифрование персональной информации (Input Key – IK) ключом RCK-Pri и использует MK-Pub для подписи. Таким образом, компания-проектировщик может аутентифицировать изготовителя с помощью имеющихся MK-Pri и RCK-Pub соответственно. В результате успешной аутентификации компания-проектировщик отправляет CK, зашифрованный MK-Pri и подписанный RCK-Pub. Аналогичным образом компания-изготовитель расшифровывает CK, осуществляет разблокирование и тестирование ЦУ и отправляет его компании-проектировщику.

Поскольку ключи на стороне производителя генерируются встроенной ФНФ, то они будут уникальны для каждого ЦУ, что исключает применение одной и той же лицензионной информации для других ЦУ, изготовленных по одному проектному описанию.

2.3. Преимущества и недостатки существующих методов активной идентификации

Методы активной идентификации показали себя эффективным и многообещающим решением в борьбе против пиратства и нелегального копирования проектных описаний ЦУ, поскольку злоумышленнику требуется одновременно решить две проблемы: осуществить взлом блокирующей схемы и получить информацию из источника энтропии (как правило, это ФНФ). Такая необходимость возникает по той причине, что блокирующая схема изначально проектируется зависимой от множества CRP ФНФ. Это делает практически невозможным изготовление дополнительных копий ЦУ даже при условии, что попытка взлома была успешно осуществлена на одном из них. Соответственно, продажа таких ЦУ не принесет большой прибыли компании-изготовителю, так как взлом одного из них является достаточно трудоемким процессом и даже в результате успеха не дает значительных преимуществ при попытках взлома других копий, произведенных по одинаковому проектному описанию.

Тем не менее существующие методы активной идентификации обладают двумя существенными недостатками. Во-первых, проектирование блокирующей схемы с использованием избыточных состояний и (или) переходов в ЦКА несет в себе дополнительные аппаратурные затраты, которые недопустимы в условиях ограничения на применение ресурсов и потребляемой мощности. В случае использования протоколов асимметричного шифрования для реализации блокирующей схемы также применяются значительные аппаратурные ресурсы, усложняется проектное описание ЦУ и возникает необходимость генерирования и хранения нескольких пар секретных ключей для поддержания работоспособности протокола. Перспективным является применение блокирующих схем, основанных на комбинационной логике [17].

Во-вторых, фиксированная блокирующая схема делает определенное устройство уязвимым к возможным взломам и, соответственно, последующему изучению проектного описания на корректно функционирующем ЦУ. Для решения этой проблемы авторами предлагается схема повторного лицензирования (рис. 7), основанная на применении реконфигурируемых ФНФ (РФНФ) [18] вместо фиксированных классических [19].

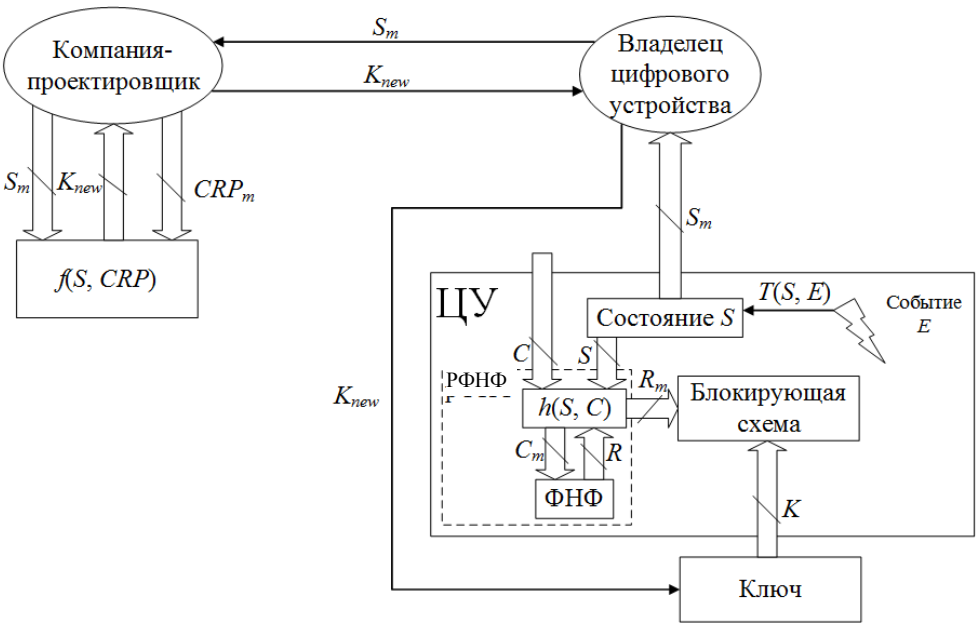

Рис. 7. Схема повторного лицензирования, основанная на методах активной идентификации

Цифровое устройство проектируется таким образом, чтобы оно содержало в себе компоненты методов активной идентификации: блокирующую схему и ФНФ в качестве источника энтропии. К ФНФ предъявляется требование реконфигурируемости: ответы на запросы становятся зависимыми не только от вариаций технологического процесса, но и от некоторого состояния (конфигурации) S, определяемого параметрами ФНФ (например, для случая мультиарбитральной ФНФ [20] номерами арбитров, которые используются для генерирования ответа; конфигурацией симметричных путей; идентификаторами, формируемыми метастабильными арбитрами). Таким образом, ответ на один и тот же запрос для конфигурации S будет отличаться от ответа для модифицированной конфигурации S_m.

Генерирование CRP осуществляется при помощи аппаратной хеш-функции h: $C_m = h(S, C)$ и $R_m = h(S, R)$, где C, R, C_m, R_m – запрос и ответ ФНФ до хеширования и после соответственно. Поскольку блокирующая схема является зависимой от ФНФ, ее реконфигурация осуществляется также в соответствии с состоянием S. Как и во всех методах активной идентификации, описанных ранее, изначально ЦУ находится в заблокированном состоянии и для его разблокирования компании-проектировщику необходимо получить CRP. Таким образом, для конкретной конфигурации ФНФ S и множества CRP формируется ключ $K = f(S, \text{CRP})$, где f – функция генерирования ключа на основании информации о ФНФ и блокирующей схеме. Для подготовки устройства к повторному лицензированию проектировщику необходимо сгенерировать N возможных ключей $K_1, K_2, \ldots, K_N$, где N – максимально возможное число случаев повторного лицензирования.

Протокол взаимодействия между компанией-проектировщиком и владельцем ЦУ при повторном лицензировании состоит из следующих этапов:

1. ЦУ в конфигурации S было разблокировано с помощью ключа K, но произошло событие E (ключ украден третьим лицом, срок его действия истек или владелец осуществил попытку изменения лицензионной информации), которое сделало ключ недействительным, поскольку была принудительно изменена конфигурация $S_m = T(S, E)$, где T – функция преобразования состояния S, срабатывающая по наступлении события E.

2. Поскольку устройство после реконфигурирования является заблокированным в силу недействительности ключа, владелец ЦУ вынужден обратиться к компании-проектировщику с просьбой о повторном предоставлении лицензионного ключа K_{new}. Для этого он отправляет по защищенному каналу текущее состояние S_m.

3. После получения от владельца необходимой информации проектировщик осуществляет генерирование нового ключа $K_{new} = f(S_m, \text{CRP}_m)$, где CRP_m – пары «запрос – ответ» ФНФ для состояния S_m.

4. Новый ключ отправляется владельцу по защищенному каналу. Далее осуществляется разблокирование ЦУ с помощью K_{new}. Таким образом, ЦУ переводится вновь в работоспособное состояние до наступления следующего события E и соответственно повторного лицензирования.

Текущие реализации методов активной идентификации в качестве блокирующей схемы используют ЦКА, реконфигурацию которого невозможно осуществить после синтеза. В связи с этим разработка реконфигурируемых блокирующих схем, работающих совместно с РФНФ, является неразрешенной и актуальной в настоящее время проблемой в области активной идентификации ЦУ.

Заключение

В статье рассмотрены существующие методы активной идентификации ЦУ, основанные на применении как цифровых конечных автоматов, так и протоколов асимметричного шифрования в качестве блокирующей схемы. Предложены варианты реализации блокирующих схем, которые проектируются зависимыми от пар «запрос – ответ» физически неклонируемой функции, что делает затруднительными криптографические атаки на один из компонентов схем активной идентификации ЦУ. Проанализированы также преимущества и недостатки существующих подходов. Предложены возможные пути преодоления проблем, не имеющих решения в настоящее время.

Список литературы

1. Wafer fabrication yield learning and cost analysis based on in-line inspection / I. Tirkela [et al.] // Intern. J. of Production Research. – 2016. – Vol. 54, no. 1. – P. 1–13.

2. Koushanfar, F. Hardware metering: A survey / F. Koushanfar // Introduction to Hardware Security and Trust / M. Tehranipoor, C. Wang (eds.). – N. Y. : Springer, 2012. – Ch. 5. – P. 103–122.

3. Choosing an Intellectual Property Core [Electronic resource]. – 2002. – Mode of access : http://wiki.prplfoundation.org/w/images/9/9e/Choosing_an_Intellectual_ Property_Core.pdf. – Date of access : 17.02.2016.

4. Tehranipoor, M. Counterfeit Integrated Circuits. Detection and Avoidance / M. Tehranipoor, U. Guin, D. Forte. – Switzerland : Springer International Publishing, 2015. – 269 p.

5. Integrated Circuit Security Threats and Hardware Assurance Countermeasures / K.M. Goertzel [et al.] // CrossTalk. – 2013. – Vol. 26, no. 6. – P. 33–38.

6. Koushanfar, F. Intellectual property metering / F. Koushanfar, G. Qu, M. Potkonjak // 4th Intern. Workshop Information Hiding (IH'01); ed. I. Moskowitz; Pittsburg, USA, April 25–27, 2001. – Pittsburg, 2001. – P. 81–95.

7. Koushanfar, F. Hardware Metering / F. Koushanfar, G. Qu // Proc. IEEE Design Automation Conference (DAC'01), Scottsdale, USA, June 18–22, 2001 / ACM, New York. – Scottsdale, 2001. – P. 490–493.

8. Koushanfar, F. Integrated circuits metering for piracy protection and digital rights management: an overview / F. Koushanfar // Great Lakes Symp. on VLSI (GLSVLSI'11), Salt Lake City, USA, May 3–4, 2012 / ACM, New York. – Salt Lake City, 2011. – P. 449–454.

9. Alkabani, Y. Active hardware metering for intellectual property protection and security / Y. Alkabani, F. Koushanfar // USENIX Security Symposium (SS'07), Boston, USA, August 6–10, 2007 / Addison Wesley, Indianapolis. – Boston, 2007. – P. 291–306.

10. Koushanfar, F. Provably secure active IC metering techniques for piracy avoidance and digital rights management / F. Koushanfar // IEEE Trans. Inf. Forensics and Security. – Vol. 7, no. 1. – P. 51–63.

11. Alkabani, Y. Remote activation of ICs for piracy prevention and digital right management / Y. Alkabani, F. Koushanfar, M. Potkonjak // EEE/ACM Intern. Conf. on Comp.-Aided Design (ICCAD'07), San Jose, USA, Nov. 4–8, 2007 / ACM, New York. – San Jose, 2007. – P. 674–677.

12. Ending piracy of integrated circuits / J. Roy [et al.] // Computer. – 2010. – Vol. 43, no. 10. – P. 30–38.

13. Ярмолик, В.Н. Физически неклонируемые функции / В.Н. Ярмолик, Ю.Г. Вашинко // Информатика. – 2011. – № 2. – С. 92–103.

14. Maes, R. PUFKY: A Fully Functional PUF-Based Cryptographic Key Generator / R. Maes, A. Van Herrewege, I. Verbauwhede // Cryptographic Hardware and Embedded Systems (CHES'12), Leuven, Belgium, Sept. 9–12, 2012 / Springer, New York. – Leuven, 2012. – P. 302–319.

15. Иванюк, А.А. Проектирование контролепригодных цифровых устройств / А.А. Иванюк, В.Н. Ярмолик. – Минск : Бестпринт, 2006. – 295 с.

16. How secure is AES against brute force attacks? [Electronic resource]. – 2012. – Mode of access : http://www.eetimes.com/document.asp?doc_id=1279619. – Date of access : 23.02.2016.

17. Solving the Third-Shift Problem in IC Piracy With Test-Aware Logic Locking / S.M. Plaza [et al.] // IEEE Trans. on Comput.-Aided Design of Integrated Circuits and Syst. – 2015. – Vol. 34, no. 6. – P. 961–971.

18. Reconfigurable physical unclonable functions – enabling technology for tamper-resistant storage / K. Kursawe [et al.] // IEEE Intern. Workshop on Hardw.-Orient. Secur. and Trust (HOST'09), San Francisco, USA, July 27, 2009 / IEEE, New York. – San Francisco, 2009. – P. 22–29.

19. Заливако, С.С. Схема удаленного контроля для активного измерения цифровых устройств / С.С. Заливако, А.А. Иванюк // Информационные технологии и системы 2014 (ИТС 2014) : материалы Междунар. науч. конф., БГУИР, Минск, Беларусь, 29 окт. 2014 г. / редкол. : Л.Ю. Шилин [и др]. – Минск : БГУИР, 2014. – С. 73–74.

20. Multi-valued arbiters for quality enhancement of PUF responses on FPGA implementation / S.S. Zalivaka [et al.] // Special Session on Cyber-Physical Systems and Security, in Proc. 21st IEEE Asia and South Pacific Design Automation Conf. (ASP-DAC 2016), Macao, China, 26–28 Jan., 2016 / IEEE, New York. – Macao, 2016. – P. 533–538

Поступила 07.06.2016

Белорусский государственный университет информатики и радиоэлектроники,
Минск, ул. П. Бровки, 6
e-mail: zalivako@bsuir.by,
ivaniuk@bsuir.by

S.S. Zalivaka, A.A. Ivaniuk

ACTIVE METERING OF DIGITAL DEVICES: AN OVERVIEW

The paper presents existing active hardware metering approaches. The motivation of using active metering approaches by fabless integrated circuits design companies is given. The finite state machine based and asymmetrical cryptography based methods are presented. The advantages and disadvantages of existing active metering approaches are analyzed. The potential solution for modern technique issues are proposed.