Методы, алгоритмы и аппаратные средства защиты интегральных микросхем от несанкционированного доступа

А.С. Боронников

***Аннотация* — В работе представлены результаты исследований в области доверенного проектирования интегральных микросхем. Рассматриваются основные методы защиты интегральных микросхем. Выделяется перспективное направление в виде использования физически неклонируемых функций для использования их откликов в виде уникальных идентификаторов.**

Подробно разобрана работа физически неклонируемой функции типа арбитр и основных схем с данной функцией для генерации идентификаторов. Рассмотрены основные существующие методы и аппаратные решения идентификации интегральных микросхем и выявлены их недостатки.

Разработан метод шифрования данных с помощью метастабильных состояний арбитра физически неклонируемой функции, позволяющий генерировать уникальное значение ключа с каждым новым тактом синхросигнала. Предложен аппаратный функциональный блок, предназначенный для автоматической установки арбитра физически неклонируемой функции в метастабильное состояние для последующей работы данного блока в режиме генерации действительно случайных чисел. Предложен оригинальный метод декодирования зашифрованных данных с помощью функционального блока шифрования на основе физически неклонируемой функции типа арбитр, в основе которого лежит изменение температуры кристалла.

Разработана схема и алгоритм активации ресурсов интегральной микросхемы, которые максимально защищены от обратного проектирования.

***Ключевые слова* — интегральные микросхемы, защита, несанкционированный доступ, физически неклонируемые функции, доверенное проектирование, аппаратная криптография, идентификация, активация, ФНФ, ПЛИС, ИС.**

I. Введение

В современном мире вычислительные системы играют ключевую роль в различных сферах – от потребительской электроники до критически важных инфраструктур. Основными элементами этих систем являются интегральные микросхемы (ИС), которые выполняют разнообразные вычисления, обработку и хранение данных, а также управление разного рода устройствами.

Процесс производства ИС глобально можно разделить на два этапа: проектирование и изготовление. На первом этапе создается проектное описание ИС, по которому на втором этапе осуществляется физическое исполнение микросхемы. В полупроводниковой промышленности бизнес-модели производства ИС могут различаться. Большие компании могут выполнять полный цикл работ от проектирования до изготовления своими производственными мощностями. Другие компании избирают модель контрактного производства (fabless) для выхода на рынок полупроводниковых устройств: компании-проектировщики разрабатывают дизайн ИС, который передают на производство сторонним фабрикам-производителям. Такое разделение труда создает определенные риски. Одной из ключевых угроз является сверхпроизводство, когда ненадежные фабрики производят больше чипов, чем предусмотрено контрактом, и продают их на стороне, тем самым нарушая права интеллектуальной собственности и подрывая рынок легальной продукции. Другими проблемами являются продажа или утечка проектного описания ИС и передача технологий третьим лицам без разрешения владельца.

Еще одной значимой проблемой вне зависимости от бизнес-модели производства ИС является обратное проектирование (реверс-инжиниринг), когда злоумышленники воссоздают топологию и схемотехническую структуру ИС с целью нелегального производства клонов. Обратное проектирование может быть полным, когда копируется весь дизайн топологии ИС, или частичным, когда вносятся изменения с целью улучшения характеристик, внедрения вредоносных функций или обхода защитных механизмов. Эти действия позволяют злоумышленникам создавать контрафактные микросхемы.

Контрафактная продукция приводит к значительным экономическим потерям. Однако наиболее серьезные последствия возникают при использовании контрафактных микросхем в критически важных областях, таких как авиационная, военная и медицинская промышленность. В этих сферах надежность и безопасность компонентов являются первоочередными требованиями, и использование поддельных микросхем может привести к катастрофическим последствиям, включая сбои в работе вычислительных систем и угрозу жизни людей. Поэтому разработка надежных механизмов защиты от несанкционированного доступа к микросхемам является актуальной задачей на сегодняшний день [1-2].

Статья получена 25 мая 2024.

Антон Сергеевич Боронников, Кафедра вычислительной техники, МИРЭА – Российский технологический университет, Москва, Россия (e-mail: boronnikov-anton@mail.ru).

II. Основные методы защиты интегральных микросхем

ИС маркируются серийными номерами и кодами завода-изготовителя, что позволяет идентифицировать каждую микросхему через базу данных (БД) разработчика. Однако, существует риск взлома БД, что может привести к внесению поддельных записей в базу.

Действенным способов защиты ИС от сверхпроизводства и обратного проектирования является идентификация аппаратного обеспечения (Hardware Metering) [3-4]. Термин «идентификация» обозначает процесс извлечения данных с ИС, которые позволяют определить устройство и подтвердить его принадлежность владельцу прав на интеллектуальную собственность. Идентификатор ИС (Chip ID, CID) – это уникальный код или номер, который присваивается каждой интегральной микросхеме во время её производства. CID предназначен для однозначной идентификации ИС и может использоваться для различных целей, таких как аутентификация, управление ресурсами, отслеживание и диагностика.

Соответственно, другим способом защиты микросхем является присвоение каждому экземпляру CID во время производства. Этот идентификатор записывается в специальную область памяти микросхемы, например, в однократно программируемое запоминающее устройство (ПЗУ, ROM), что обеспечивает его сохранность и защиту от изменений. Аналогично CID вносится в БД разработчика. Для аутентификации или других целей микросхема может предоставить свой CID, который можно считать с помощью специального протокола с определенных выводов микросхемы. После чего полученный идентификатор сравнивается с известным ожидаемым значением. Это может включать сравнение с заранее сохраненным CID в БД или использование криптографических методов для проверки подлинности.

Запись CID в специализированную память микросхемы значительно усложняет задачу злоумышленникам с несанкционированным доступом. В отличие от простой маркировки, внесение CID в ПЗУ требует понимания схемотехнического описания и знаний протоколов чтения, что не указывается в технической документации на изделие [5]. Расшифровка требует значительных усилий и времени. Злоумышленник, разобравшись в топологии кристалла, произведет запись собственного CID или существующего CID с оригинального изделия. Тем самым возможные проблемы с взломом БД остаются прежними.

Методы идентификации аппаратного обеспечения в настоящее время делятся на два больших класса: активные и пассивные. Пассивная идентификация позволяет определить подлинность ИС без возможности изменения или контроля его функциональности. Активная идентификация предоставляет же владельцу прав возможность включения или отключения функциональности ИС используя различные блокирующие схемы, обеспечивая защиту от несанкционированного использования. Оба класса методов могут использовать как воспроизводимые, так и неклонируемые CID.

Наиболее перспективным направлением на сегодня является применение физически неклонируемых функций, которые позволяют генерировать уникальные, неклонируемые, невоспроизводимые и надежные CID.

III. Физически неклонируемые функции и схемы генерации уникальных идентификаторов

Физически неклонируемые функции (ФНФ) представляют собой перспективное направление в области безопасности информационных технологий. ФНФ – это односторонняя функция, реализованная в физической структуре. Свойство неклонируемости ФНФ связано с несовершенством производственного процесса, поэтому невозможно создать два идентичных физических устройства с одинаковыми характеристиками. Можно считать, что эти характеристики принимают случайные значения [6].

В общем случае ФНФ описывается значениями пар входных и соответствующих им выходных сигналов. Такая пара, состоящая из входного параметра «запрос» (Challenge, CH) и выходного параметра «отклик» (Response, R), называется парой запрос-отклик (Challenge-Response Pairs, CRP). Тем самым, ФНФ можно рассматривать как функцию f, которая преобразует запросы CH_i в ответы R_i (1).

$$R_i = f(CH_i) \tag{1}$$

Множество CRP уникально идентифицирует физическое устройство и не может быть скопировано даже при условии использования абсолютно одинакового проектного описания.

В зависимости от вида физической структуры в качестве параметров выступают различные характеристики, которые задают значение случайной величины отклика *Response*. Вид ФНФ зависит от предполагаемого применения в конкретной задаче предметной области.

ФНФ, реализованная на кремниевой интегральной схеме (ИС), формируется неконтролируемым образом на всех этапах производства микросхемы, начиная с выращивания кристалла и заканчивая литографией на нем. Следовательно, ФНФ зависит от свойств материала подложки, электрических и физических свойств электронных компонентов [7]. Выделяют следующие основные типы ФНФ, реализованные в базисе ИС [8]:

– ФНФ на базе СОЗУ (Статическое оперативное запоминающее устройство): основаны на случайных вариациях содержимого ячеек памяти при подаче питания на СОЗУ. При каждом включении устройства ячейки СОЗУ устанавливаются в случайные значения (0 или 1), которые можно использовать для создания уникального отклика.

– ФНФ типа арбитр (АФНФ): основаны на разных задержках прохождения сигналов в логических вентилях микросхемы. В силу не идеальности технологического процесса при изготовлении микросхемы значения задержек будет зависеть от физических характеристик полупроводников и проводников.

– ФНФ на базе кольцевых генераторов: основаны на различиях в частотных характеристиках колебательных контуров.

Вариативность реализации ФНФ на кристалле интегральных схем позволяет выделить основные направления применения ФНФ, такие как цифровые подписи, генерация псевдослучайных числовых последовательностей, идентификация и аутентификация устройств, реализация аппаратных хэш–функций, обнаружение аппаратных троянов, генерация ключей шифрования.

Для разработки методов и функциональных блоков неклонируемой активной идентификации ИС была выбрана АФНФ. Это решение обусловлено приемлемыми аппаратурными затратами, экспоненциально большой мощностью множества пар запрос-отклик, а также высокими значениями характеристик случайности и уникальности по сравнению с другими классическими реализациями ФНФ [9].

Классическая схема АФНФ [10] основана на цепочке сдвоенных мультиплексоров, представляющих собой линию задержки. Она позволяет образовывать пары симметричных путей, форма которых определяется параметром сигнала запроса *Challenge* на адресных входах мультиплексоров. Несмотря на то, что пути топологически симметричны, задержка на этих путях будет отличаться от кристалла к кристаллу в силу не идеальности производства. На конце цепочки размещается арбитр, который позволяет представить соотношение задержек на путях, т.е. отклик Response. В качестве арбитра могут выступать защёлки или синхронные триггеры. В рассматриваемых далее методах использовался арбитр в виде синхронного D-триггера (рис. 1).

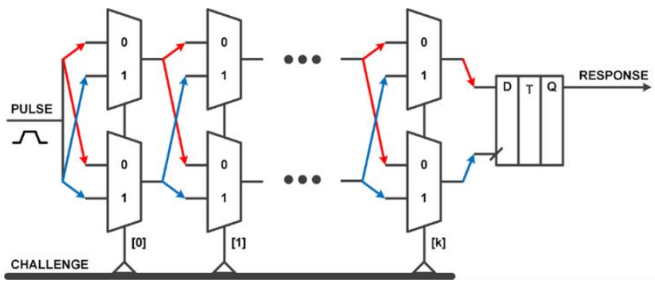

Рис. 1. ФНФ типа арбитр

Интерфейс модуля АФНФ представлен на рис. 2.

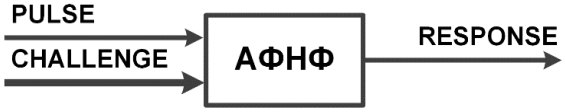

Рис. 2. Интерфейс модуля АФНФ

Чтобы получить ответ Response, на вход АФНФ подается импульс (Pulse), который вначале переходит на все информационные входы первых мультиплексоров. Далее сигналы распространяются по двум симметричным путям, и в конце результата гонки сигналов защелкиваются арбитром. На выходе Response могут быть устоявшиеся значения – 0 или 1, и метастабильные состояния (если во время апертурного времени (сумма времени предустановки «time setup» и времени удержания «time hold») работы триггера изменился сигнал на входе D) (рис. 3) [5].

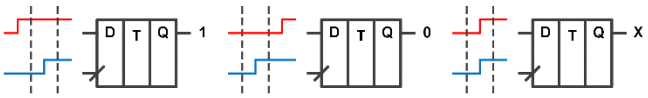

Рис. 3. Возможные значения на выходе арбитра АФНФ

На основе стабильных ответов Response можно сформировать последовательность произвольной длины (вектор откликов) и использовать ее в качестве CID. Проблемы ФНФ заключаются в изменении параметров полупроводников под воздействием температуры, времени и электромагнитных помех, что приводит к снижению стабильности ФНФ [11].

Наиболее распространенным вариантом функционального блока (ФБ) получения CID на базе ФНФ является использование регистра сдвига с линейной обратной связью LFSR, пример которого изображен на рис. 4. LFSR – сдвиговый регистр битовых слов, у которого значение входного бита однозначно задается некоторой функцией, исходя из значений остальных битов регистра до сдвига [12]. Обратная связь и функции, реализованные с помощью логических элементов исключающего ИЛИ, обеспечивают генерацию псевдослучайных чисел. Если перед каждым входом D-триггеров добавить мультиплексор, и на один из входов подавать бит с входного порта, то регистр LFSR можно установить в конкретное значение, как обычный регистр. Эта модификация важна для использования LFSR для генерации CID.

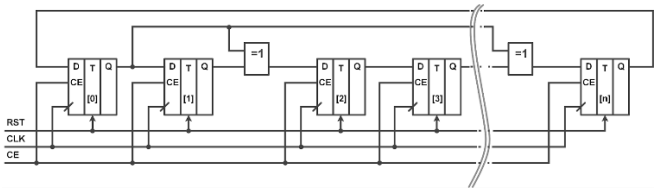

Рис. 4. Пример сдвигового регистра LFSR

ФБ получения CID на базе АФНФ и LFSR изображен на рис. 5. В LFSR загружается значение запроса *Challenge* по разрешающему сигналу CE. Следующие N тактов (в зависимости от разрядности регистра вектора откликов CID) с LFSR поступают различные значения запроса на АФНФ, отклики Response которой поступают в сдвиговый регистр вектора откликов CID. Такой подход с использованием LFSR позволяет получать уникальные отклики Response от одного загружаемого значения *Challenge*. Для обеспечения стабильности в данной реализации должна быть реализована задержка после сдвига значения LFSR.

Недостатком рассмотренной схемы является недостаточная энтропия, а также реализация необходимых задержек для корректного извлечения идентификатора.

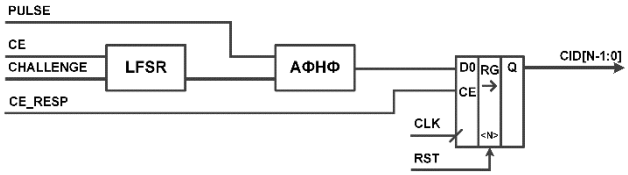

Рис. 5. ФБ получения CID на базе АФНФ и LFSR

Второй вариант ФБ извлечения CID основан на параллельном подключении модулей АФНФ (рис. 6). При одном и том же запросе *Challenge N* модулей АФНФ отрабатывают параллельно, тем самым идентификатор CID является полностью зависимым от физической структуры кристалла микросхемы. Использование такой схемы позволит получить вектор идентификатора CID, который с высокой вероятностью будет полностью стабильный.

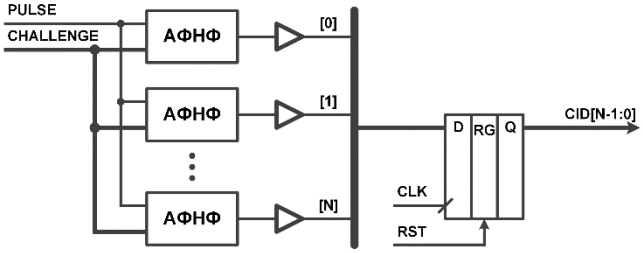

Рис. 6. ФБ получения CID на базе параллельных модулей АФНФ

В данной работе в качестве модуля генерации CID далее будет использоваться только второй вариант и сокращенно называться ФНФ-CID. Интерфейс данного ФБ изображен на рис. 7.

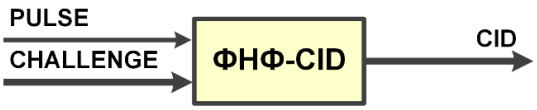

Рис. 7. Интерфейс ФНФ-CID

IV. Аппаратные решения идентификации интегральных микросхем с применением физически неклонируемых функций

В качестве методов идентификации чаще используют активные, т.е. после производства микросхемы необходимо активировать ресурсы изделия [13-19]. Активация происходит записью в чип CID на специальных тестовых стендах способом, известным лишь разработчикам.

Вариант классической архитектуры ФБ идентификации СБИС с использованием модуля ФНФ-CID представлена на рис. 8. Данный ФБ состоит из модуля ФНФ-CID, блока коррекции ошибок (ECC), ПЗУ для записи эталонных значений запроса функции Challenge и идентификатора CID.

Первым этапом считывается CID. Для этого необходимо на тестовом стенде подавать сигнал разрешения генерации импульсов CE_PULSE и значение CHALLENGE по определенному протоколу и правилам, которые заданы разработчиком (например, сколько раз подавать импульс при одном и том же значении запроса). С выхода CID считывается идентификатор и с помощью специального ПО определяется подходящий. Вторым этапом выбранный CID при задающем ему *Challenge* записывается в ПЗУ. В ИС должен быть реализован генератор всех необходимых напряжений, чтобы была возможность внутрисхемного программирования ПЗУ. В ПЗУ CID на вход CID_REF устанавливается выбранный идентификатор и сигналом разрешения на запись WR_CID_REF записывается в память. Тоже самое и с запросом *Challenge*. Необходимо установить флаг, который после записи данных в ПЗУ CHALLENGE переключит входные данные на ФНФ-CID с ПЗУ CHALLENGE. На схеме такой флаг записывается в виде дополнительного бита к последовательности CH_REF, который управляет входным мультиплексором.

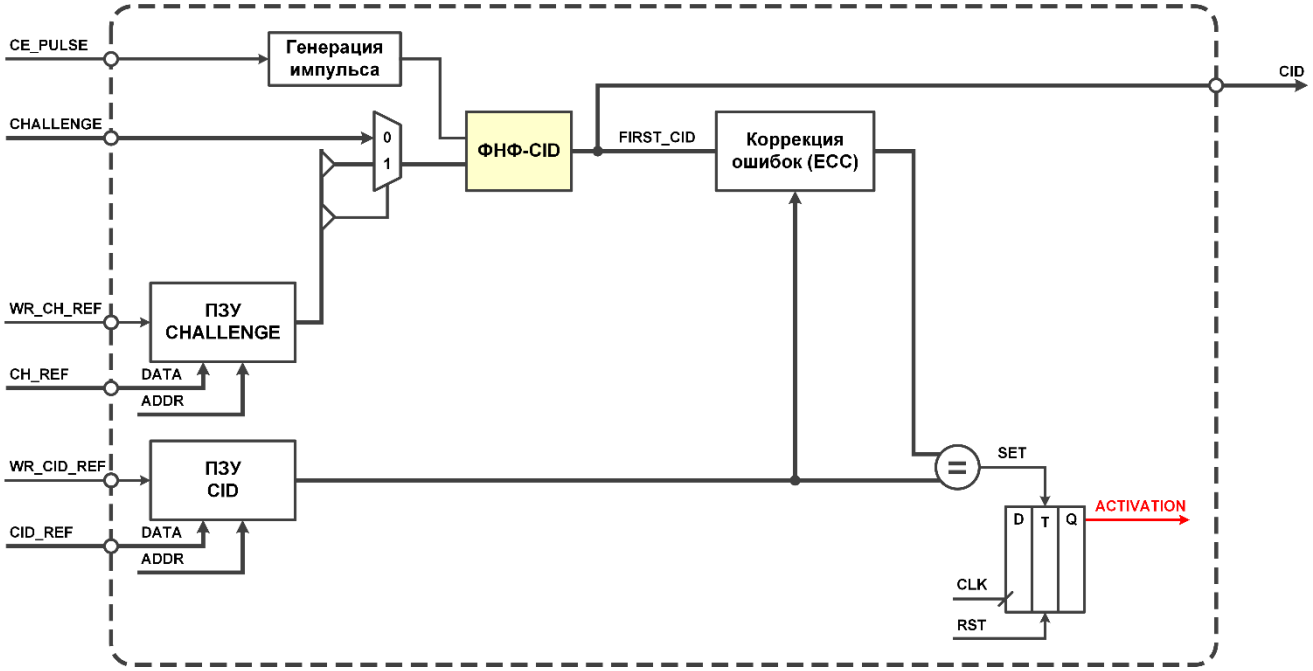

Рис. 8. Классическая архитектура ФБ идентификации ИС

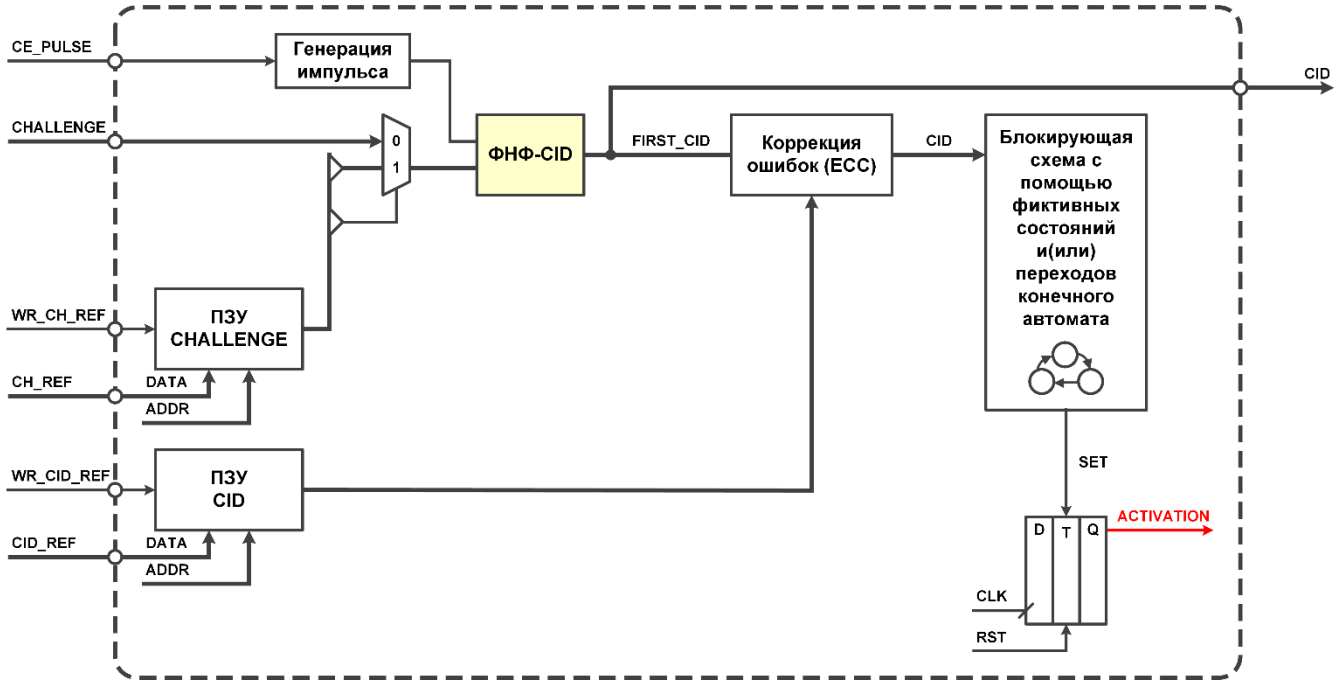

Рис. 9. Усложненная архитектура ФБ идентификации ИС

Вектор откликов ФНФ при идентификации должен быть стабильным. Но он может быть зашумлен в связи с изменением температуры, деградацией кристалла со временем и различными помехами. Для избежания этого используют блок коррекции ошибок. Возможны аппаратные реализации различных схем коррекции ошибок, таких как коды Хэмминга, БЧХ-коды и коды Рида-Соломона [20]. На вход данного блока подается идентификатор и вспомогательные данные из ПЗУ CID.

Сигнал активации ACTIVATION формируется тогда, когда результат работы ФНФ-CID будет равен эталонному CID, записанным в ПЗУ.

Рассмотренную схему активации ИС разработчики усложняют различными способами. Часто добавляют блокирующую схему в виде расширенного цифрового конечного автомата с помощью создания фиктивных состояний и (или) переходов (рис. 9), либо схем на базе комбинационной логики. Переход в финальное состояние, которое активирует ИС, зависит от CID, в котором определенные биты в последовательности должны равняться заданному значению, поэтому схема усложняется подбором пары *Challenge*-CID.

В работе [21] предлагается метод применения повторного лицензирования, но она не удобна для конечных пользователей по нескольким причинам. Во-первых, она увеличивает время на аутентификацию. Во-вторых, сложность процесса может затруднить его выполнение для обычных пользователей, требуя специальных знаний или оборудования. В-третьих, многократное лицензирование повышает риск ошибок и сбоев, что может привести к ненадежной работе устройства или его блокировке. В-четвертых, пользователи зависят от доступа к серверам компании-проектировщика.

V. Постановка задачи

Существующие методы недостаточно защищены от проблемы сверхпроизводства и полного копирования топологии ИС, что приводит к нелицензионной продукции на рынке.

Рассмотренные функциональные блоки неклонируемой идентификации имеют существенный недостаток: при обратном проектировании электрическую схему можно восстановить и понять ее работу, включая и переходы в сложно-запутанных конечных автоматов с фиктивными состояниями. Это лишь вопрос времени и ресурсов, доступных злоумышленнику. Более того ИС, использующие такие методы активной идентификации, активируют ресурсы чипа каждый раз при включении. Учитывая известные проблемы нестабильности ФНФ, в определенный момент времени блок коррекции ошибок может не сработать, что приведет к необходимости замены микросхемы, что невыгодно для пользователя.

Таким образом, поставлена задача разработки методов, алгоритмов и аппаратных средств для максимальной защиты от обратного проектирования и проблемы сверхпроизводства интегральных микросхем. В данной работе предложены методы исходя из задачи полного клонирования топологии без модификации схемы злоумышленником.

VI. Предлагаемые методы, алгоритмы и аппаратные средства для защиты интегральных микросхем

A. Шифрование уникального идентификатора CID

Для усложнения считывания идентификатора CID с модуля ФНФ-CID предлагается использовать обычные логические элементы исключающего ИЛИ (XOR), предназначенные для шифрования данных (рис. 10).

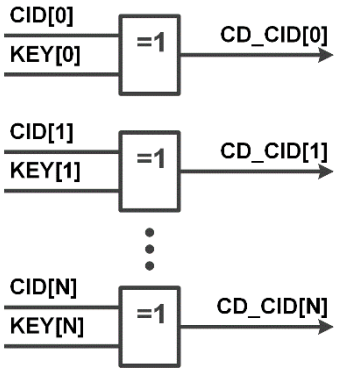

Рис. 10. Шифрование с помощью XOR

Таблица истинности XOR представлена в табл. 1. Если на входах одинаковые значения, то на выходе будет «0», иначе – «1». Таким образом, при подаче вектора идентификатора CID на одни входы элементов XOR, а на другие ключ шифрования KEY, то на выходах элементов получаются зашифрованные данные CD_CID.

Таблица 1. Таблица истинности элемента XOR

Входы		Выход
A	**B**	**XOR**
0	0	0
0	1	1
1	0	1
1	1	0

Дешифровать прочитанный CD_CID можно, подав его на элементы XOR и используя тот же ключ KEY на других входах; в этом случае на выходах снова получится исходный CID (рис. 11). Примеры шифрования и декодирования представлены в табл. 2.

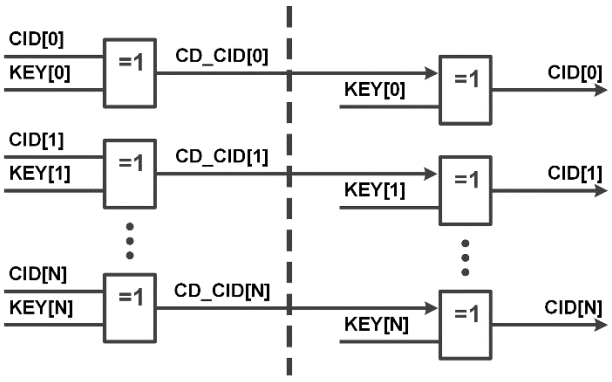

Рис. 11. Дешифрация с помощью XOR

Таблица 2. Примеры шифрования и декодирования данных с помощью элементов XOR

	Пример 1	**Пример 2**	**Пример 3**	**Пример 4**
CID	0101	0101	0101	0000
KEY	0100	0000	1111	0000
CD_CID	0001	0101	1010	0000
KEY	0100	0000	1111	0000
CID	0101	0101	0101	0000

Как видно из табл. 2, в примере 1 данные хорошо зашифрованы. В примере 2 в качестве ключа используется вектор нулей, поэтому шифрования не происходит – CD_CID равен CD. В примере 3 ключ состоит из всех единиц, поэтому шифрованные данные являются инверсными по отношению к входным. В примере 4 на все входы подаются нули, и на всех выходах также нули. Концепция примеров 2-4 пригодится далее для понимания работы предлагаемого функционального блока.

Добавив регистр в схему, получен ФБ шифрования идентификатора CID (рис. 12). Интерфейс данного блока представлен на рис. 13.

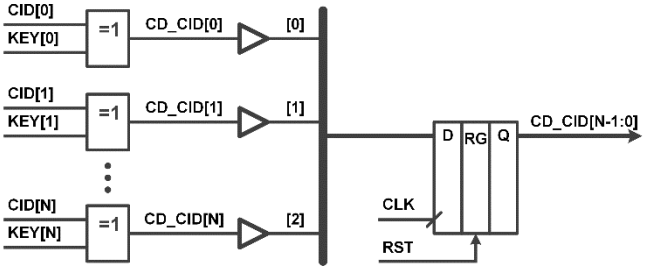

Рис. 12. ФБ шифрования CID

Рис. 13. Интерфейс ФБ шифратора CID

К модулю шифрования CID были добавлены управляющие буферы (рис. 14), которые пропускают значения KEY и CID по разрешающему сигналу EN = 1. Если EN = 0, то на выходе модуля будет вектор CD_CID, состоящий из всех нулей (табл. 2, пример 4).

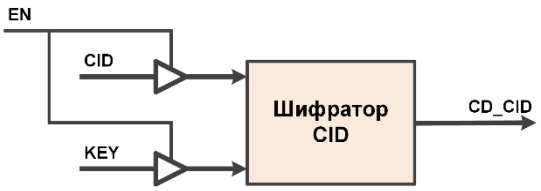

Рис. 14. Шифратор CID с управляющими буферами

B. Генерация ключа KEY для шифрования

Схемы шифрования данных на элементах XOR являются распространенными, но остро стоит задача хранения и генерации ключа. Для генерации ключей шифрования разработчики могут использовать ФНФ, однако для расшифровки данных необходимо знать ключ, который должен храниться в специализированной защищенной памяти с возможностью его считывания из микросхемы. Однако, в случае обратного проектирования чипа, злоумышленник может восстановить схему, понять алгоритм работы и потенциально считать ключ даже из защищенной памяти.

В качестве генератора ключей предлагается использовать функциональный блок с АФНФ и регистром сдвига для вектора отклика, выступающим в роли KEY. После исследования такой схемы с помощью

разработанной ранее программно-аппаратной системы [22] было установлено, что если арбитр устанавливается в метастабильное состояние, то регистр вектора откликов выполняет роль генератора действительно случайных чисел (TRNG – true random number generator). Пример вектора откликов при метастабильном состоянии арбитра изображен на рис.15 (формат – «Challenge: вектор откликов KEY»).

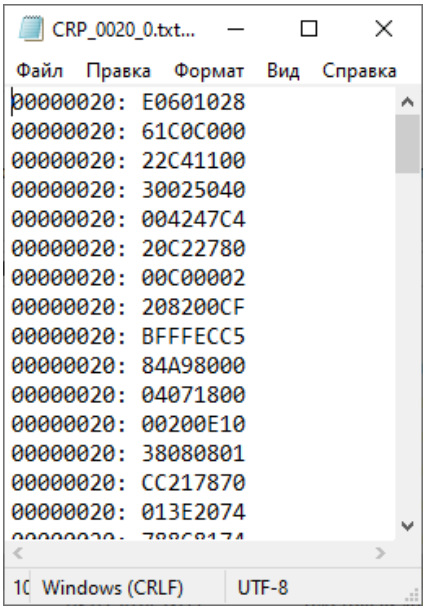

Рис. 15. Пример вектора откликов при метастабильном состоянии арбитра

На основании предложенного генератора случайных чисел предлагается функциональный блок автоматического поиска запроса *Challenge* внутри кристалла ИС, при котором арбитр устанавливается в метастабильное состояние (рис. 16).

При подаче питания счетчик CT является первоначальным источником *Challenge* для АФНФ, который по разрешающему сигналу увеличивается на единицу для выполнения перебора запросов. В регистре KEY находится вектор откликов. Для поиска метастабильного значения арбитра простой схемы сравнения регистра KEY с исключающими стабильными значениями векторов из всех нулей и единиц не получится, так как возможны помехи при записи в регистр. Поэтому чтобы найти действительно метастабильное состояние предлагается следующая схема сравнения: вектор KEY записывается в регистр VRESP при каждом новом заполнении, а в регистр COPY_VRESP только при первой генерации вектора KEY при новом значении *Challenge*. Управление выполняется разрешающими сигналы на запись, которые генерируются в блоке синхронизации. Значения VRESP и COPY_VRESP сравниваются в схеме сравнения двух векторов. Предложена следующая схема, представленная на рис. 17, но есть возможность оптимизации решения.

Сравнение битов выполняется с помощью все тех же логических элементов XOR. Если биты одинаковые – результат 0, разные – 1. Значение по разрешающему сигналу CE_CMP записывается в регистр и далее конечным автоматом опрашивается каждый бит, в основе которого лежит счетчик, который считает количество единиц, т.е. различий. Разработчик должен задать число *Num*, когда нужно считать векторы различными. Опытным путем установлено, что различие двух векторов должно быть не менее в 30% несовпадающих бит. В таком случае генерируется сигнал IF_METASTABILITY, который сигнализирует о том, что счетчик сейчас находится в таком значении *Challenge*, когда арбитр попал в метастабильное состояние. Предлагается для одного и того же *Challenge* подавать импульсы PULSE для заполнения вектора KEY минимум 3 раза.

После того, как это событие произошло, в регистр CH_MET сохраняется значение запроса *Challenge* из счетчика и устанавливается сигнал EN в значение «1», который сигнализирует об установке ФБ в режим генерации действительно случайных чисел.

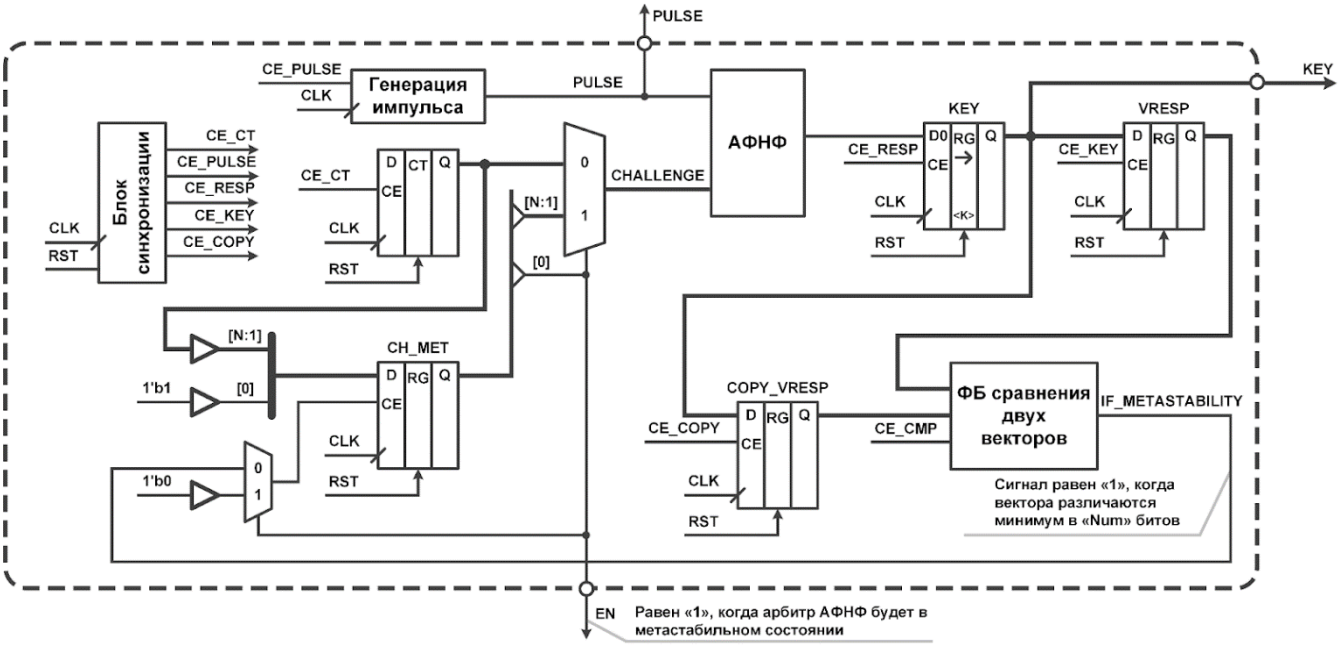

Рис. 16. ФБ генерации ключей для шифрования данных

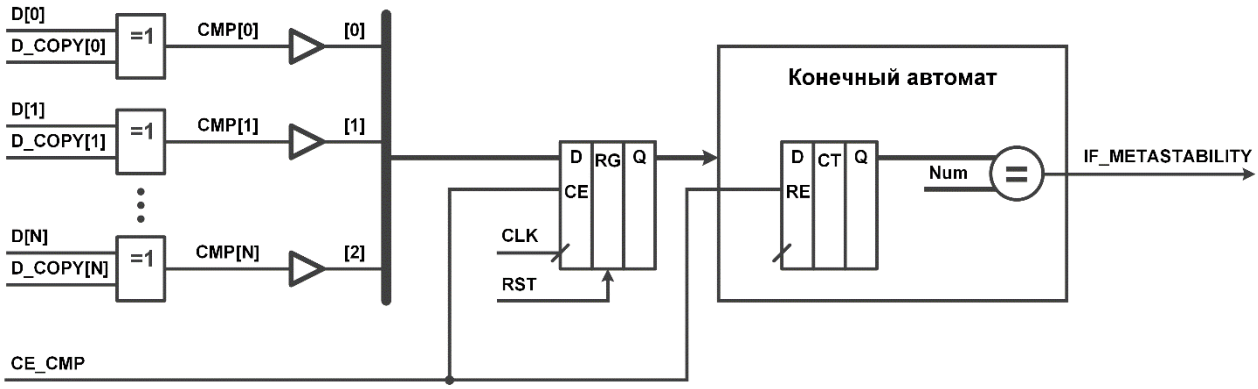

Рис. 17. Схема сравнения двух векторов

Интерфейс модуля ФНФ-KEY представлен на рис. 18.

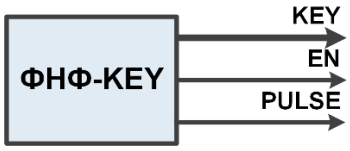

Рис. 18. Интерфейс модуля ФНФ-KEY

После того, как это событие произошло, в регистр CH_MET сохраняется значение запроса *Challenge* из счетчика и устанавливается сигнал EN в значение «1», который сигнализирует о установке ФБ в режим генерации действительно случайных чисел.

Используя такую схему с целью генерации ключей для блока шифрования CID данных внутри кристалла ИС без возможности чтения KEY с выводов микросхемы, проектировщик не сможет расшифровать данные, так как после установки в метастабильное состояние арбитра сдвиговый регистр откликов KEY будет изменяться с каждым тактом синхронизации, т.е. ключ не постоянный и устойчивый к обратному проектированию, так как отклик функции зависит от физических особенностей кристалла ИС и параметров окружающей среды.

C. Метод декодирования

Сформирована гипотеза, которая заключается в следующем: предложенный блок генерации ключа KEY находит и сохраняет значение *Challenge* в регистр, который переводит АФНФ в метастабильное состояние. Путем изменения температуры кристалла ИС меняются задержки распространения сигналов в линии АФНФ, тем самым есть возможность попадания арбитра в стабильное состояние – 0 или 1. Тогда вектор откликов KEY будет либо в нулях, либо в единицах – т.е. данные с модуля шифрования CID можно дешифровать (табл. 2, примеры 2 и 3).

Данная гипотеза подтвердилась. Выполнены эксперименты изменения температуры в климатической камере на отладочных платах различных семейств программируемых логических интегральных схем (ПЛИС) с различным техпроцессом на чипах компании AMD (Xilinx): Artix-7 – 28 нм и Spartan-6 – 45 нм. При комнатной температуре 20˚C найдены три значения *Challenge* для каждого семейства, которые устанавливали арбитр в метастабильное состояние. Причем выбирался такой *Challenge*, где биты векторов откликов изменялись в примерном соотношении 50/50 процентов из выборки 100 векторов. Связано это с тем, что возможна генерация стабильного состояния с незначительными помехами, вектора которых можно принять за метастабильное состояние. В ходе эксперимента температура увеличивалась с шагом в 10˚C, что позволило собрать необходимые данные для подтверждения гипотезы без потери точности. При различных *Challenge* векторы откликов стабилизировались по-разному. Для чипов с техпроцессов 28 нм вектора стабилизировались при температуре 30˚C, 50˚C и 70˚C. При температуре 70-90˚C все векторы находились в стабильных состояниях. Для чипов с техпроцессом 45 нм стабилизация происходила при более высоких температурах – начиная от 70˚C. На рис. 19 показан пример стабилизации векторов откликов при повышении температуры.

D. Функциональный блок и алгоритм активации ресурсов интегральной микросхемы

Предложено схемотехническое решение активации ресурсов ИС, изображенное на рис. 20.

В целях защиты от обратного проектирования в ИС предусмотрена активная идентификация после производства микросхемы, так как ресурсы чипа изначально не доступны для работы. Для активации этих ресурсов с тестового стенда необходимо на вход CH_REF подавать значения *Challenge* и снимать зашифрованные данные с выхода CD_CID. После декодирования идентификатора с помощью предложенного ранее метода производится его запись в регистр CID_REF. Если данные расшифрованы успешно, то происходит запись признака активации в ПЗУ, который активирует микросхему.

Если ИС попадает в руки злоумышленнику, то после восстановления схемы он не сможет считать ключ KEY, который автоматически генерируется модулем ФНФ-KEY. Идентификатор CID и ключ шифрования KEY поступают на управляющие буферы, которые управляются сигналом разрешения EN. Сигнал EN устанавливается в единицу, когда нашлась пара CRP, которая переводит в метастабильное состояние арбитр в модуле ФНФ-KEY. До тех пор, пока не произойдет установка, на выходе CD_CID будут нули. После открытия буферов ключ меняется каждый такт

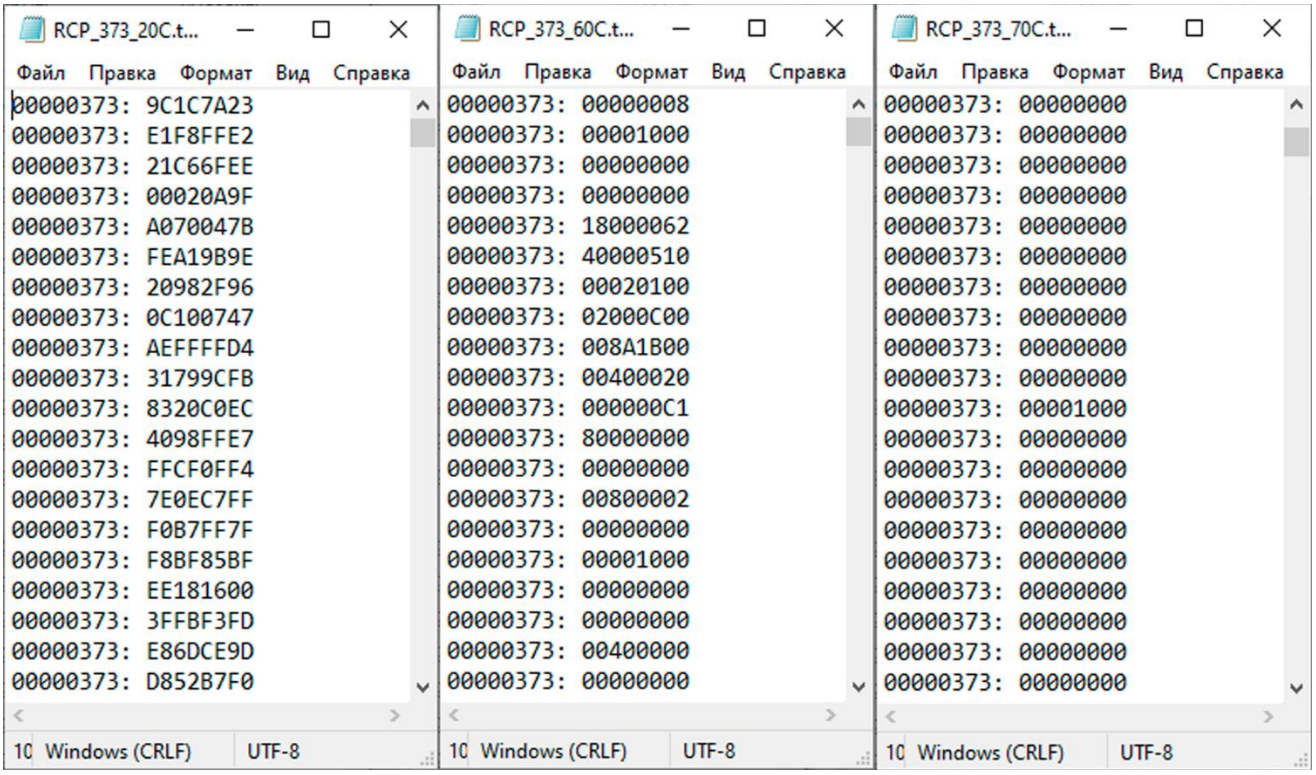

Рис. 19. Стабилизация вектора отклика

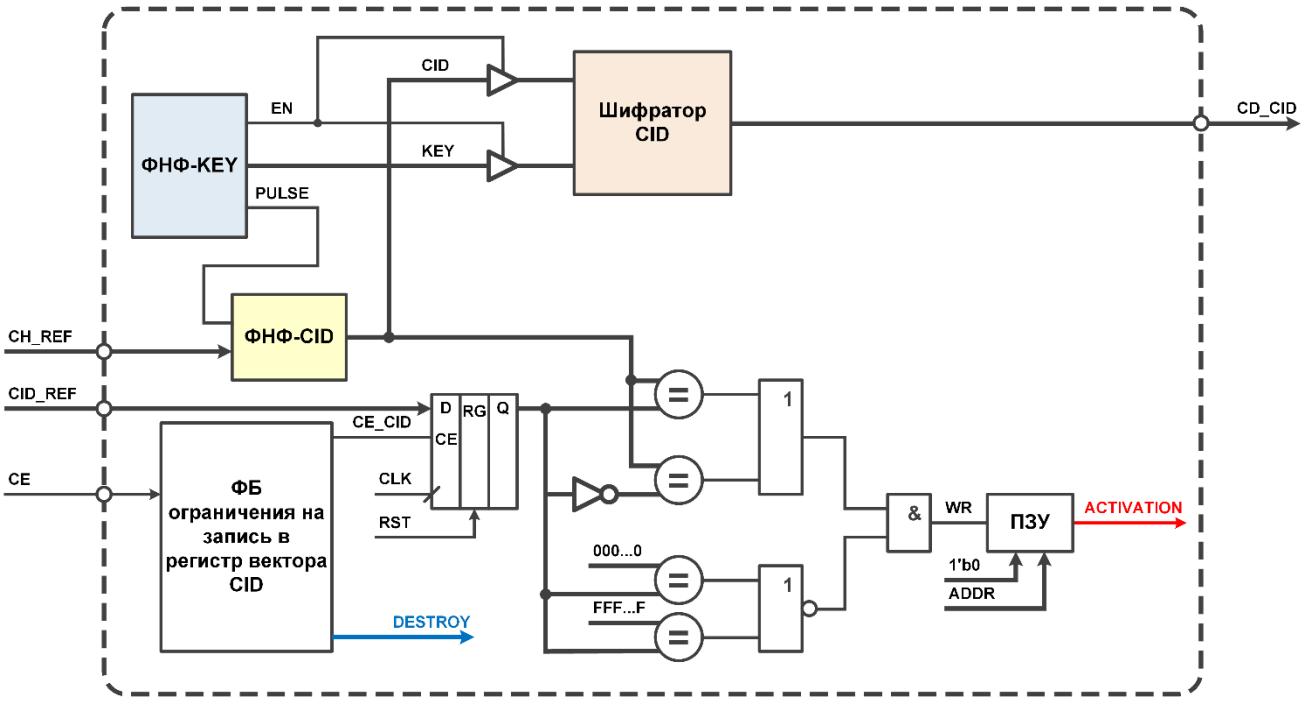

Рис. 20. Интерфейс модуля ФНФ-KEY

синхросигнала, поэтому значение CID не поддается расшифровке. Ключ невозможно определить, потому что значение регистра KEY формируется внутри микросхемы и не подается на внешние выводы для чтения.

Для дешифрации данных значения вектора CID необходимо изменить температуру до стабилизации ключа и произвести считывание данных. Так как стабильным откликом может быть либо «0», либо «1», то возможны варианты ключа состоящих из всех нулей или единиц, то есть идентификатор CID на выходе CD_CID будет либо без изменений, либо инверсным.

Для этого в схеме сравнивается значение CID с прямым или инверсным значением регистра CID_REF. Кроме того, необходимо исключить наиболее встречающиеся значения идентификаторов из всех нулей и единиц.

В ФБ в качестве защиты от перебора записи в регистр CID предложена схема ограничения на запись, представленная на рис. 21. В ее основе лежит счетчик, который увеличивается по поданному извне сигналом CE. Этот сигнал разрешает запись идентификатора в регистр CID_REF. Выход счетчика сравнивается с числом *Number*, которое устанавливает разработчик. Если счетчик достигает этого значения, то формируется

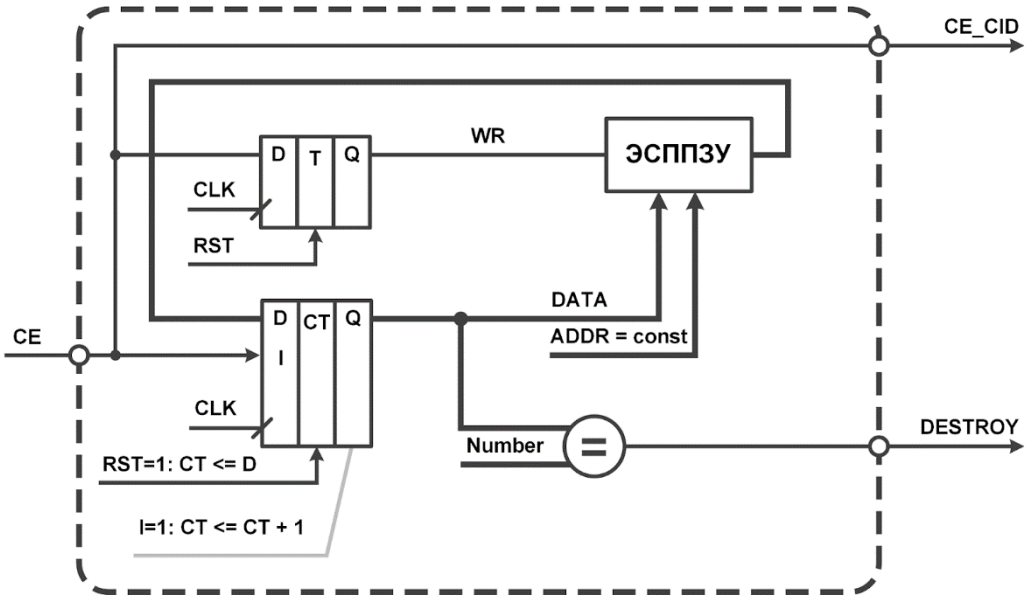

Рис. 21. Интерфейс модуля ФНФ-KEY

сигнал DESTROY, который можно использовать для разрушения ресурсов микросхемы. Сигнал CE также разрешает запись в ЭСППЗУ текущего значения счетчика, выход которого подведен ко входу CT. Тем самым после подачи питания счетчик установится в последнее значение, лишая злоумышленника использовать аппаратные средства перебора векторов CID.

Для приема-передачи данных проектировщик при необходимости разрабатывает свой протокол (рис. 22), тем самым дополнительно усложняя обратное проектирование.

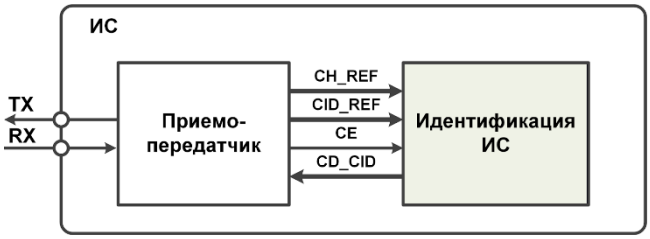

Рис. 22. Общая структура активации ресурсов ИС

Также для увеличения надежности защиты от обратного проектирования для реализации ПЗУ предлагается использовать технологию Anti-fuse [23], так как обычная ПЗУ заметна сразу после рентгена.

В предлагаемой архитектуре активация микросхемы выполняется только один раз, тем самым исключаются недостатки существующих решений активной идентификации. Предложенное решение в силу оригинальности шифрования/дешифрования данных и имеющее защиту от обратного проектирования позволяет использовать минимально допустимую разрядность CID и KEY.

Можно модернизировать предложенную архитектуру для увеличения функциональности модуля. Например, использование ФНФ-CID в качестве криптографического ключа – для этого в схеме регистр для записи эталонного значения Challenge нужно заменить на ПЗУ. Выход с модуля ФНФ-KEY использовать в качестве генерации действительно случайных чисел.

Предложенный функциональный блок активации микросхемы может быть использоваться в совместимости с другими криптографическими методами защиты, и по аналогии с двухфакторной авторизацией быть лишь одним из этапов идентификации ИС.

VII. Заключение

В работе рассматриваются вопросы защиты интегральных микросхем от несанкционированного доступа.

Разработан метод шифрования данных с помощью метастабильных состояний арбитра физически неклонируемой функции, позволяющий генерировать уникальное значение ключа с каждым тактом синхросигнала. Тем самым ключ не постоянный и устойчив к обратному проектированию.

Предложен аппаратный функциональный блок, предназначенный для автоматической установки арбитра физически неклонируемой функции в метастабильное состояние для последующей работы данного блока в режиме генерации действительно случайных чисел.

Предложен метод декодирования зашифрованных данных с помощью функционального блока шифрования на основе физически неклонируемой функции типа арбитр. В основе декодирования данных лежит изменение температуры кристалла.

Разработана схема и алгоритм активации ресурсов интегральной микросхемы, которые в силу оригинальности шифрования и декодирования данных защищают от обратного проектирования.

Полученные результаты могут быть внедрены в процесс проектирования и производства микросхем, что существенно повышает их защищенность от несанкционированного доступа и использования.

Библиография

[1] Гребенщиков П. Выявление контрафактной продукции в области микроэлектроники // Электроника: наука, технология, бизнес. – 2019. – № 6 (187). – С. 172-175.

[2] Кессаринский Л.Н., Ширин А.О., Коваль К.А., Тайибов Ф.Ф., Каменева А.С. Выявление признаков контрафакта в изделиях электронной компонентной базы в аспекте обеспечения промышленной кибербезопасности // Безопасность информационных технологий. – 2019. – Т. 26, № 2. – С. 117-128.

[3] Koushanfar F., Qu G. Hardware metering // Proceedings of the 38th Design Automation Conference. – 2001. – P. 490-493.

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

[5] Коломов Д., Золотухо Р. Использование микросхем специальной памяти для обеспечения защиты ПЛИС FPGA от копирования // Компоненты и технологии. – 2008. – № 12. – С. 24-26.

[6] Herder Ch., Yu M-D., Koushanfar F., Devadas S. Physical Unclonable Functions and Applications: A Tutorial // Proceedings of the IEEE. – 2014. – Vol. 102, № 8. – P. 1126-1141.

[7] Бельский В.С., Чижов И.В., Чичаева А.А., Шишкин В.А. Физически неклонируемые функции в криптографии // International Journal of Open Information Technologies, 2020. — Т. 8, № 10. — С. 10-26.

[8] Комлева Е.Р., Никифоров М.Б. Физически неклонируемые функции. Проблемы и перспективы. // Известия Тульского государственного университета. Технические науки, 2021. — № 6. — С. 61-69.

[9] Иванюк А.А., Заливако С.С. Физическая криптография и защита цифровых устройств // Доклады БГУИР. – 2019. – № 2. – С. 50-58.

[10] Боронников А.С., Деменкова Т.А. Методика проектирования уникальных идентификаторов интегральных микросхем на FPGA // Фундаментальные, поисковые, прикладные исследования и инновационные проекты. Сборник трудов Национальной научно-практической конференции. – 2023. – С. 6-11.

[11] Лебедев В.Р., Певцов Е.Ф., Деменкова Т.А., Малето М.И., Филимонов В.В. Метод исследования реализации физически неклонируемых функций в информационных системах // International Journal of Open Information Technologies. – 2024. – Т. 12, № 1. – С. 28-36.

[12] Принцип работы PCЛОС. – URL: https://habr.com/ru/articles/534732/ (дата обращения: 25.03.2024).

[13] Федорец В.Н., Белов Е.Н., Балыбин С.В. Технологии защиты микросхем от обратного проектирования в контексте информационной безопасности. – М.: Рекламно-издательский центр «Техносфера» – 2019. – 216 с.

[14] Семенов А. В., Костюк А. В. Защита ключей микросхем на физически неклонируемых функциях в условиях недоверия к кремниевой фабрике // Вопросы защиты информации. – 2015. – № 2 (109) – С. 63-68.

[15] Rührmair U., Devadas S., Koushanfar F. (2012). Security Based on Physical Unclonability and Disorder // Introduction to Hardware Security and Trust / M. Tehranipoor, C. Wang (eds.). – N. Y.: Springer. – 2012. – Ch. 4. – P. 65-102.

[16] Wei Sh., Nahapetian A., Potkonjak M. Robust passive hardware metering // 2011 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). – 2011. – P. 802-809.

[17] Leest V., Tuyls P. Anti-counterfeiting with hardware intrinsic security // 2013 Design, Automation & Test in Europe Conference & Exhibition (DATE). – 2013. – P. 1137-1142.

[18] Guin U., Forte D., Tehranipoor M. Anti-counterfeit Techniques: From Design to Resign // 2013 14th International Workshop on Microprocessor Test and Verification. – 2013. – P. 89-94.

[19] Koushanfar F. Active Hardware Metering by Finite State Machine Obfuscation // Hardware Protection through Obfuscation / D. Forte et al. (eds.). – N. Y.: Springer. – 2017. – Ch. 7. – P. 161-187.

[20] Семенов Ю.А. Коррекция ошибок. – URL: http://book.itep.ru/2/28/corec_28.htm (дата обращения: 15.05.2024).

[21] Заливако С.С., Иванюк А.А. Обзор методов активной идентификации цифровых устройств // Информатика. – 2016. – № 3. – С. 38-48.

[22] Боронников А.С., Деменкова Т.А., Кряхтунов Г.М. Программно-аппаратная система для исследования физически неклонируемых функций в базисе ПЛИС // ИТ-Стандарт. – 2024. – № 1(38). – С. 34-54.

[23] Защита микросхем от реверс-инжиниринга и несанкционированного проникновения. – URL: https://habr.com/ru/articles/436998/ (дата обращения: 20.05.2024).

Methods, algorithms and hardware for protecting integrated circuits from unauthorized access

A.S. Boronnikov

***Abstract* — The paper presents the results of research in the field of trusted design of integrated circuits. The main methods of protection of integrated circuits are considered. A promising direction is highlighted in the using physical unclonable functions' form to use their responses in the unique identifiers' form.**

The work of a physical unclonable function of the arbiter type and the main schemes with this function for generating identifiers are analyzed in detail. The main existing methods and hardware solutions for the identification of integrated circuits are considered and their disadvantages are identified.

A method of data encryption using metastable states of the physical unclonable function of the arbiter type has been developed, which allows generating a unique key value with each new clock cycle. A hardware functional block is proposed designed to automatically set the arbiter of a physical unclonable function to a metastable state for the subsequent operation of this block in the mode of generating truly random numbers. An original method of decoding encrypted data using a functional encryption block based on a physical unclonable function of the arbiter type, based on a change in crystal temperature, is proposed.

A scheme and algorithm for activating the resources of an integrated circuit have been developed, which are maximally protected from reverse engineering.

***Keywords* — integrated circuits, protection, unauthorized access, physical unclonable function, trusted design, hardware cryptography, identification, activation, PUF, FPGA, IC.**

REFERENCES

[1] Grebenshchikov P. Detection of counterfeit products in the field of microelectronics // Electronics: science, technology, business. – 2019. –- № 6 (187). – pp. 172-175 (in Russian).

[2] Kessarinsky L.N., Shirin A.O., Koval K.A., Tayibov F.F., Kameneva A.S. Detection of counterfeit signs in the products of electronic component base in the aspect of industrial cybersecurity // Information technology security. – 2019. – Vol. 26, № 2. – pp. 117-128 (in Russian).

[3] Koushanfar F., Qu G. Hardware metering // Proceedings of the 38th Design Automation Conference. – 2001. – pp. 490-493.

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

[5] Kolomov, D.; Zolotukho, R. Use of the special memory chips for the FPGA copy protection // Components and technologies. – 2008. – № 12. – pp. 24-26 (in Russian).

[6] Herder Ch., Yu M-D., Koushanfar F., Devadas S. Physical Unclonable Functions and Applications: A Tutorial // Proceedings of the IEEE. – 2014. – Vol. 102, № 8. – pp. 1126-1141.

[7] Belsky V., Chizhov I., Chichaeva A., Shishkin V. Physically Unclonable Functions in cryptography // International Journal of Open Information Technologies. – 2020. – Vol. 8, № 10. – pp. 10-26 (in Russian).

[8] Komleva E.R., Nikiforov M.B. Physical unclonable functions. Problems and prospects. // Izvestia Tula State University. Technical Sciences. – 2021. – № 6. – pp. 61-69 (in Russian).

[9] Ivanyuk, A.A., Zalivako, S.S. Physical cryptography and protection of digital devices // Reports of BSUIR. – 2019. – № 2. – pp. 50-58 (in Russian).

[10] Boronnikov A.S., Demenkova T.A. Methodology for designing unique identifiers of integrated circuits on FPGA // Fundamental, search, applied research and innovative projects. Collection of proceedings of the National Scientific and Practical Conference. – 2023. – pp. 6-11 (in Russian).

[11] Lebedev V.R., Pevtsov E.Ph., Demenkova T.A., Maleto M.I., Filimonov V.V. Method for studying the implementation of Physical Unclonable Function in information systems // International Journal of Open Information Technologies. – 2024. – Vol. 12, №1. – pp. 28-36 (in Russian).

[12] Principle of operation of RSLOS [Online]. Available: https://habr.com/ru/articles/534732/

[13] Fedorets V.N., Belov E.N., Balybin S.V. Technologies of protection of microchips from reverse engineering in the context of information security. – Moscow: Advertising and publishing center "Technosphere" – 2019. – 216 pp (in Russian).

[14] Semyonov A. V. V., Kostyuk A. V. Protection of chip keys on physically unclonable functions in the context of distrust in silicon fab // Information Protection Issues. – 2015. – № 2 (109) – pp. 63-68 (in Russian).

[15] Rührmair U., Devadas S., Koushanfar F. (2012). Security Based on Physical Unclonability and Disorder // Introduction to Hardware Security and Trust / M. Tehranipoor, C. Wang (eds.). – N. Y.: Springer. – 2012. – Ch. 4. – pp. 65-102.

[16] Wei Sh., Nahapetian A., Potkonjak M. Robust passive hardware metering // 2011 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). – 2011. – pp. 802-809.

[17] Leest V., Tuyls P. Anti-counterfeiting with hardware intrinsic security // 2013 Design, Automation & Test in Europe Conference & Exhibition (DATE). – 2013. – pp. 1137-1142.

[18] Guin U., Forte D., Tehranipoor M. Anti-counterfeit Techniques: From Design to Resign // 2013 14th International Workshop on Microprocessor Test and Verification. – 2013. – pp. 89-94.

[19] Koushanfar F. Active Hardware Metering by Finite State Machine Obfuscation // Hardware Protection through Obfuscation / D. Forte et al. (eds.). – N. Y.: Springer. – 2017. – Ch. 7. – pp. 161-187.

[20] Semenov Yu.A. Correction of errors [Online]. Available: http://book.itep.ru/2/28/corec_28.htm

[21] Zalivako S.S., Ivanyuk A.A. Review of methods of active identification of digital devices // Informatics. – 2016. – № 3. – pp. 38-48 (in Russian).

[22] Boronnikov A.S., Demenkova T.A., Kryakhtunov G.M. Hardware-software system for investigation of the physically unclonable functions in the FPGA basis // IT-Standard. – 2024. – № 1(38). – pp. 34-54 (in Russian).

[23] Protection of microchips from reverse-engineering and tampering [Online]. Available: https://habr.com/ru/articles/436998/