АППАРАТНЫЕ ТРОЯНЫ. ЧАСТЬ 3: СПОСОБЫ ПРЕДУПРЕЖДЕНИЯ И ОБНАРУЖЕНИЯ

HARDWARE TROJANS. PART 3: METHODS FOR PREVENTION AND DETECTION

УДК 621.382, ВАК 05.27.01, DOI:10.22184/1993-8578.2017.71.1.30.40

Е.Кузнецов, А.Сауров**
E.Kuznetsov, A.Saurov**

В третьей части цикла обзорных статей рассмотрены наиболее действенные способы предупреждения аппаратных закладок в интегральных схемах – аппаратных троянов. Однако и они не дают гарантию отсутствия аппаратного трояна в системе. Поэтому противодействие должно быть комплексным, включая способы обнаружения.

In the third part of a series of articles devoted to Hardware Trojans the most effective methods to prevent them are considered. However, they does not give a guarantee of absence Hardware Trojan in the system. Therefore, counteraction should be comprehensive, including detection methods.

Наличие аппаратных троянов представляет значительную угрозу безопасности, поэтому самая действенная мера борьбы с ними – предотвращение их внедрения в процессе разработки ИС. Предупреждение является первым уровнем защиты от аппаратных троянов и важным звеном в стратегии многоуровневой защиты. Исходя из традиционных правил, процедур и практического опыта, для сохранения контроля над процессом разработки ИС следует задействовать доверенные команды разработчиков, средства проектирования и доверенные производства. Однако существуют и специальные исследования, посвященные новым методам предупреждения внедрения аппаратных троянов на различных этапах проектирования и изготовления ИС.

ПРЕДУПРЕЖДЕНИЕ АППАРАТНЫХ ЗАКЛАДОК НА ЭТАПЕ ПРОЕКТИРОВАНИЯ

На этапе проектирования аппаратная закладка может быть внедрена в проект членом группы разработчиков, занесена непроверенным программным обеспечением для разработки ИС или через включение в проект непроверенных сторонних сложно-функциональных модулей (IP-блоков). Создание проверенных схем (без аппаратных закладок) с использованием непроверенных инструментов САПР ИС рассмотрено в работе [1]. Предложенное решение основано на использовании инструментов САПР для сложных синтезов и очень простой проверенной программы, созданной разработчиком для контроля результата и выявления возможных привнесенных в проект модификаций. Основная идея заключается в создании такой спецификации проекта, при которой не остается места для добавления злонамеренной схемы непроверенными инструментами САПР. Полная спецификация должна предполагать, что аппаратные ресурсы проекта должны быть полностью задействованы во все такты. Метод базируется на том, что достаточно легко проверить, используются ли в проекте полностью все ресурсы (NP-полная задача), по аналогии с тем, что найти решение NP-полной задачи сложно, но проверить, удовлетворяет ли ей решение, относительно просто.

Основная проблема такого подхода состоит в том, что вполне возможно [2] построить аппаратный троян, используя только логику, которая уже задействована в проекте. Относительно просто разработать программу для проверки того, что проект использует все доступные аппаратные ресурсы, но определить, отсутствуют ли злонамеренные изменения достаточно сложно.

* НПК "Технологический центр"/ SMC "Technological Centre".

Похожий подход, но с использованием методов обфускации (запутывания), подробно рассмотрен в работе [3]. Правильная функциональность ("нормальный режим") спрятана за секретную инициализирующую последовательность, любое отклонение от которой переводит ИС в невозвратимый "режим обфускации" в графе состояний. Отличие между этим подходом и изложенным выше заключается в том, что метод обфускации использует тупиковые состояния, а не стремление задействовать все доступные логические вентили. Это упрощает его реализацию, но и позволяет внести более простые изменения в проект вне последовательности. Такой подход не защищает от возможных изменений исходника, причем они не выявляются специальным анализом проекта методами обратного проектирования после изготовления ИС.

ПРЕДУПРЕЖДЕНИЕ НА ЭТАПЕ ИЗГОТОВЛЕНИЯ

Вопросы изготовления ИС на непроверенном производстве рассмотрены в работе [4]. Авторы предложили систему, которая обеспечивает разработчика – потребителя СФ-блоков (IP-блоков), спецификацией используемых в нем аппаратных средств, а также списком так называемых "свойств, имеющих отношение к секретности". И поставщик, и потребитель СФ-блоков соглашаются транслировать эти свойства в формальный математический код на языке "автоматического доказательства". Поскольку разработчик СФ-блока пишет HDL-код, он проводит формальное доказательство того, что специфицированные аппаратные средства выполняют все требуемые свойства. Они могут быть проверены через программу автоматического доказательства, когда СФ-блок будет доставлен потребителю. Эта идея подобна процессу программной верификации на основе PCC-кода (кода носителя доказательства) [5]. Связывание формальной модели проекта со спецификацией проекта может привести к более корректной реализации ИС. Однако, как отмечают авторы, создание формальной модели остается за поставщиком СФ-блока, и необходимо быть полностью уверенным в его надежности, что он не добавит аппаратную закладку в проект или в доказательный код. В противном случае такую закладку будет достаточно трудно обнаружить.

ПРЕДУПРЕДИТЕЛЬНЫЕ МЕРЫ ПОСЛЕ ИЗГОТОВЛЕНИЯ ИС

В работе [2] рассматривается подход к реализации ИС с применением реконфигурируемой логики (специфицируется после изготовления ИС), которую располагают между выходами одной схемы и входами другой. Таким образом, достигается скрытность проекта от злоумышленника, который имеет доступ к описанию на уровне регистровых передач. Этот подход можно рассматривать как превентивную меру и как метод противодействия при эксплуатации ИС в присутствии аппаратного

Hardware Trojans pose a significant security risk, so the most effective measure to combat them is to prevent introducing them in the IC design. Prevention is the first level of protection against hardware Trojans and an important link in the multi-layered security strategy. According to the traditional rules, procedures and practical experience, in order to maintain control over the IC development, trusted teams of developers, design tools and trusted productions should be involved. However, special research on new methods of prevention of the introduction of hardware Trojans is undertaken at various stages of IC design and manufacture.

PREVENTION OF HARDWARE TROJANS AT DESIGN STAGE

At the design stage the hardAt the design stage, a hardware backdoor can be introduced in a project by a development team member, untested software for the IC development, or through inclusion in the project of some unverified third-party intellectual property modules (IP modules). The creation of the checked schemes (without hardware Trojans) using untested IC CAD tools is discussed in [1]. The proposed solution is based on the use of CAD tools for the complex synthesis and very simple proven programme created by the developer to control the results and identify possible modifications introduced in the project. The key idea is to create such project specifications which would exclude adding any malicious scheme by unverified CAD tools. Full specification should assume that the hardware resources of the project should be fully involved in all strokes. The method is based on the fact that it is easy enough to check whether a project uses all the resources (NP-complete problem), similar to that it is difficult to find a solution for a NP-complete problem but it is relatively easy to verify whether the solution will be suitable.

The main problem with this approach is that it is quite possible [2] to build a hardware Trojan using only logic already involved

трояна. С точки зрения превентивных качеств, этот метод оставляет злоумышленнику неопределенность в работе без знания схемы реконфигурируемой логики, что сужает область возможных атак.

Даже прилагая большие усилия, достаточно трудно полностью предотвратить внедрение аппаратной закладки в ИС. Однако наилучших результатов в комплексном противодействии аппаратным троянам можно достичь, не допустив его наличия в ИС.

ОБНАРУЖЕНИЕ АППАРАТНЫХ ЗАКЛАДОК

Наряду с превентивными мерами защиты от проникновения троянов в проект или в ИС, существуют и методы их обнаружения. При выявлении аппаратный троян может быть удален из проекта (если обнаружен в описании на уровне регистровых передач), либо ИС с трояном может не использоваться, или же может эксплуатироваться и с присутствием аппаратной закладки. В зависимости от механизма обнаружения, закладка может быть идентифицирована, или же может быть выполнена статистическая оценка вероятности наличия изменений в проекте.

Традиционное тестирование и верификация ИС направлены на проверку соответствия техническим условиям и спецификации. Наличие дополнительных функциональных возможностей ИС, как правило, не проверяется. Учитывая все пространство состояний, в котором могут быть спрятаны эти дополнительные функции, такая проверка выполнима только для небольших логических проектов.

В настоящее время не существует общего подхода, гарантирующего обнаружение всех аппаратных троянов. Большинство исследований сфокусированы на поиске аппаратных троянов после изготовления ИС, поскольку этот этап рассматривается как самое слабое звено в полном цикле разработки и производства ИС. Малая часть исследований посвящена обнаружению аппаратных троянов в исходном RTL-коде (RTL – язык уровня регистровых передач) до синтеза проекта (преобразования проекта, написанного на уровне регистровых передач в двоичный код нет-листа для шаблонов), или непосредственно во время изготовления ИС. Предполагается, что к персоналу, осуществляющему поиска троянов, существует полное доверие, а поиск аппаратных троянов – доверенная экспертная процедура, которая должна включать анализ проекта на уровне регистровых передач, а также исследование его имитационного поведения (имитационное моделирование).

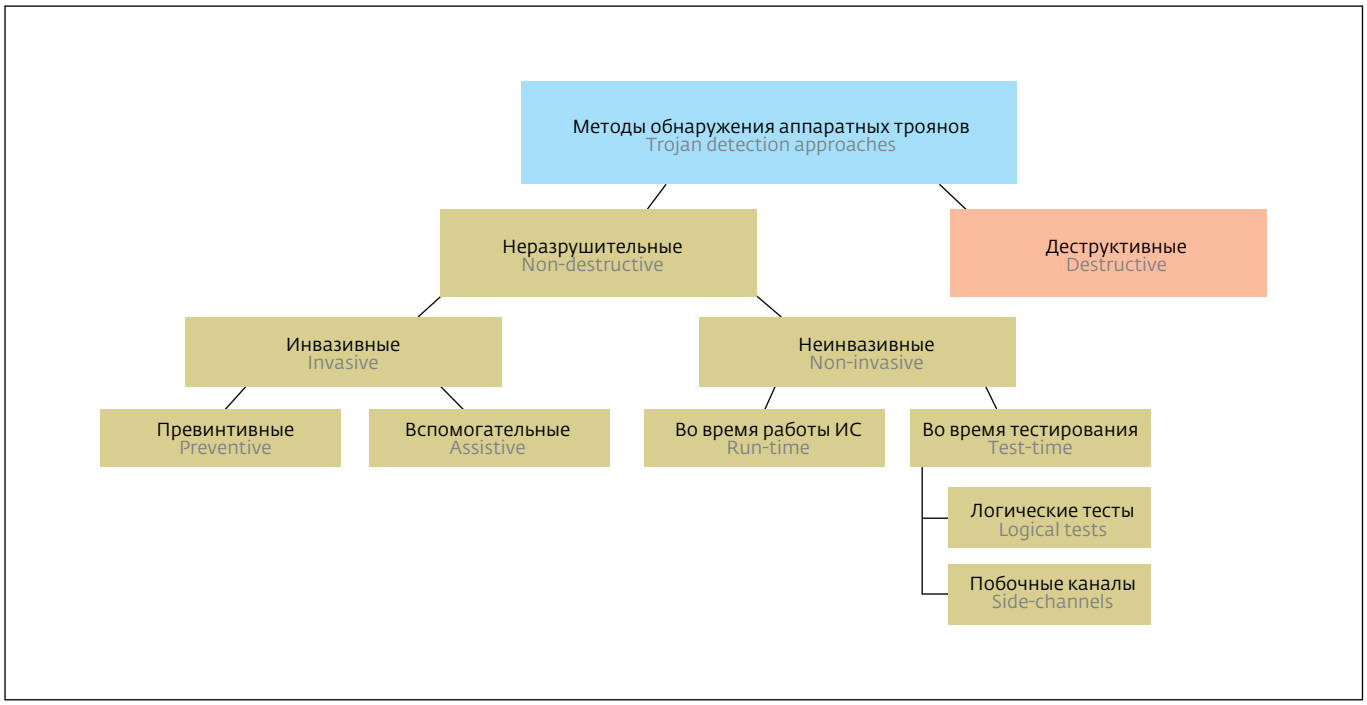
При индивидуальном проектировании аппаратной закладки будет сделана попытка обойти существующие и появляющиеся по мере исследований и разработок новые методы обнаружения троянов. Это своего рода гонка вооружений, подобная той, которую мы наблюдаем в антивирусной индустрии программного обеспечения. На рисунке приведена классификация современных методов обнаружения аппаратных троянов [3].

in the project. It is relatively easy to develop a programme to check that a project is using all available hardware resources, but it is quite difficult to determine whether there are no malicious changes.

A similar approach, although using obfuscation methods, is discussed in detail in [3]. The correct functionality (normal mode) is hidden behind a secret initiating sequence, any deviation from which switches IC to the irrecoverable "obfuscation mode" in the status column. The difference between this approach and the one described above is that the obfuscation technique uses dead states but not the desire to use all available logic gates. This simplifies its implementation and also allows you to make a simple change in the project out of sequence. This approach does not protect against possible changes to the source code, and they cannot be detected by a special analysis of the design through reverse engineering after producing IC.

PREVENTION AT STAGE OF MANUFACTURE

Some issues concerning the IC manufacture at untested production are considered in [4]. The authors have proposed a system that provides the developer consuming IP modules with the specification on hardware used in it as well as a list of so-called "properties relating to confidentiality". Both the supplier and consumer of IP modules agree to translate these properties into a formal mathematical code in the "automatic proof" language. Since the developer of an IP module writes an HDL code, it carries out a formal proof that the specified hardware performs all the required properties. They can be checked through the automatic proof programme when an IP



Классификация методов обнаружения аппаратных троянов [3]
Trojan detection techniques [3]

ДЕСТРУКТИВНЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ

Под деструктивными подразумевают методы обнаружения аппаратных троянов, которые приводят к полному разрушению ИС. Полное разрушение в значительной степени ограничивает их применение. Чтобы быть уверенным, что данная ИС не содержит аппаратного трояна, ее исследуют методами обратного проектирования. Однако, обратное проектирование современной сложной ИС достаточно трудоемкий и дорогостоящий процесс. Как правило, оно осуществляется методами химико-механической полировки с последующей реконструкцией и анализом топологии ИС с использованием сканирующего электронного микроскопа. В большинстве случаев

module will be delivered to the consumer. This idea is similar to the programme verification based on the PCC code (proof-carrying code) [5]. Linking the formal project model with the project specification can lead to some more correct implementation of IC. However, as the authors note, it is the supplier of an IP module who is to create a formal model, and you should be fully confident in its reliability and that it does not add any hardware backdoor in the project or in a proof code. Otherwise, it will be quite difficult to detect such a hardware backdoor.

PREVENTIVE MEASURES AFTER IC MANUFACTURE

In [2] considered is a concept of implementing IC using reconfigurable logic (it is specified after IC manufacture) which is located between the outputs of a pattern and the inputs of another one. By doing so, a project can be protected against an intruder that has access to the description at the register transfer level. This approach can be considered as a countermeasure and as a method of prevention during the IP operation with a hardware Trojan. In terms of preventive qualities, this method leaves an intruder in the uncertainty without the knowledge of the reconfigurable logic circuit thus narrowing the scope of possible attacks.

Even making great efforts, it is difficult to completely prevent the implementation of a hardware Trojan in IC. However, the best results in the complex countermeasures to hardware Trojans can be achieved by excluding it in IC.

DETECTING HARDWARE TROJANS

Along with preventive measures against the Trojans in any project or in IC, there are methods for detecting them. In identifying a

"корректность" чипа устанавливается путем визуального сравнения с известным примером или эталонной ИС. Однако, если аппаратный троян был внесен непосредственно перед изготовлением (следовательно, он будет присутствовать во всех изготовленных ИС), визуальное сравнение ничего не даст.

Аппаратной модификации могут быть подвергнута лишь часть ИС. В этом случае метод обратного проектирования может только с некоторой вероятностью дать основания утверждать, что ИС не содержит аппаратного трояна. В связи с этим в работе [6] предложено использовать деструктивное обратное проектирование для выявления "хороших" ИС. Перед проведением обратного проектирования исследуются косвенные характеристики случайной выборки ИС, такие как профили потребляемой мощности, температуры, электромагнитного излучения, токов утечек. В итоге для каждой ИС получают набор характеристик – "отпечаток пальцев". Если наблюдается определенное выделенное распределение характеристик, то все образцы из этой выборки подвергаются обратному проектированию для проверки наличия аппаратных троянов. В дальнейшем принадлежность "отпечатка пальцев" ИС к характерному распределению (как для "хороших", так и "зараженных" ИС) может использоваться для неразрушающей сортировки ИС в партии.

Описанный подход не решает ряда проблем. Так, аппаратный троян может быть реализован путем добавления, удаления или модификации всего двух логических вентилей [7], в то время как современная ИС состоит из миллиарда вентилей. Поиск такой "иголки в стоге сена" требует проведения полного обратного проектирования ИС на уровне вентилей, что может быть намного дороже разработки и изготовления ИС. С другой стороны, нет гарантии того, что "отпечаток пальцев" ИС с аппаратным трояном будет отличаться от "незараженной" ИС на фоне возрастающих дисперсий характеристик ИС, что обусловлено уменьшением характеристического линейного размера.

НЕРАЗРУШАЮЩИЕ МЕТОДЫ ОБНАРУЖЕНИЯ

Неразрушающие методы обнаружения аппаратных троянов не приводят к нарушению целостности ИС и классифицируются на инвазивные и неинвазивные. Неинвазивные методы не изменяют проект ИС, в то время как инвазивные характеризуются внесением изменений в проект с целью придания функций, способствующих обнаружению трояна.

Инвазивные методы делятся на два класса: превентивные и вспомогательные. Вспомогательные методы используются для того, чтобы было легче обнаружить троян в тестах после изготовления ИС. В работе [3] предложена схема, которая позволяет выявить наличие аппаратного трояна в мульти-модальном проекте. Это достигается путем использования дополнительных входов и выходов, которые добавляются к каждому модулю. Дополнительные входы обеспечивают "ключ", который переводит модуль в "прозрачный

hardware Trojan can be removed from the project (if found in the description at the register transfer level) or ICs with Trojan may not be used or may be used also with the hardware Trojan. Depending on the detection mechanism, a hardware Trojan can be identified, or the likelihood of changes in the project may be statistically estimated.

Traditional testing and verification of IC are aimed at checking compliance with technical requirements and specifications. Some additional functional features of IC are usually not checked. Talking into account all the space of states, in which the extra functions may be hidden, such testing is feasible only for smaller logic projects.

Currently, there is no common approach to guarantee detection of all hardware Trojans. Most studies have focused on finding the hardware Trojans after manufacturing IC since this stage is seen as the weakest link in the full cycle of IC development and production. A small part of research is dedicated to the detection of hardware Trojans in the original RTL (Register Transfer Language) code to design the project synthesis (translation of a project written at the register transfer level into the binary no-sheet code for templates), or directly in the manufacture of IC. It is expected that there is complete trust to the personnel in charge of the search for Trojans, and the search for hardware Trojans is a trusted expert procedure which should include a project assessment at the register transfer level as well as the project simulation behaviour study.

During the individual design of hardware Trojans, attempt to circumvent any existing and emerging R&D methods for detecting Trojans will be made.

режим". В этом режиме модуль выполняет самотестирование схемы, разработанное таким образом, чтобы проверить редкие события и маловероятные состояния. По окончании самотестирования на выход модуля поступает подпись, которая состоит из установленного входного ключа и результата самотестирования. Эта подпись затем последовательно поступает на вход следующего модуля, как входной "ключ". Таким образом, простой "специальный" входной ключ, введенный на основной вход, тестирует всю систему, и результат этого тестирования выводится однозначной величиной на основном выходе. Авторы утверждают, что этот метод действенен против злоумышленника, который располагает информацией о функциональной и логической структуре ИС.

Использование логики, позволяющей проверять расширенное пространство состояний, в которых может проявиться аппаратный троян, на практике обеспечивает очень слабую защиту от целевой закладки. Как уже говорилось в данном разделе, вероятность обнаружения профессионально спроектированной закладки достаточно мала. К тому же, этот метод предполагает, что аппаратная закладка будет внедрена на конкретной стадии проектирования. Однако злоумышленник может вставить троян после разработки функционального проекта модуля, но перед разработкой логики определения "отпечатков пальцев".

В работе [8] предложен метод, основанный на добавлении в проект нерабочей триггерной схемы, которая приводит к увеличению активности аппаратного трояна при его включении. Это упрощает его обнаружение через побочные каналы. В работе [9], для обнаружения закладки через побочные каналы предлагается дополнительная схема, характеризующая время задержки ИС, которое изменяется в случае наличия трояна.

Неинвазивные методы обнаружения аппаратных закладок основаны на сравнении рабочих характеристик ИС с характеристиками заведомо исправной эталонной ИС. Обнаружение неинвазийным методом может быть проведено или во время работы ИС или во время ее тестирования. Механизмы обнаружения во время работы ИС во многом пересекаются с методами противодействия аппаратным троянам. Если закладка обнаружена, то можно попытаться продолжить эксплуатацию ИС и в ее присутствии. Обнаружение во время проведения теста основывается на улучшении традиционного тестирования или анализе побочных характеристик ИС (побочного канала).

В работе [10] подробно рассмотрен подход к обнаружению аппаратных троянов с использованием аппаратного и программного обеспечения. Стратегия позволяет обнаруживать только два типа атаки. Атака типа DoS (отказ в обслуживании), обнаруживается с использованием небольшой заказной схемы защиты на шине памяти, которая запрограммирована реагировать на периодические пинги "живучести". Отсутствие ответа в установленное время рассматривается как успешное обнаружение попытки DoS атаки.

It is a kind of arms race, like the one we are witnessing in the antivirus software industry. Fig. shows the classification of modern hardware Trojans detection methods [3].

DESTRUCTIVE DETECTION METHODS

The destructive methods involve the detection of hardware Trojans that lead to the complete destruction of IC. Complete destruction greatly limits their application. To be sure that the IC does not contain any hardware Trojan, it is examined by reverse engineering. However, reverse engineering of our today's complex ICs is quite a time-consuming and expensive process. Usually, it is carried out by the chemical and mechanical polishing methods with the subsequent reconstruction and analysis of the IC topology using a scanning electron microscope. In most cases, the chip "correctness" is set by visual comparison with the reference or a benchmark IC. However, if a hardware Trojan was introduced just before the manufacture (hence, it will be found in all the manufactured ICs), visual comparison will not be helpful.

Only some IC may be subjected to the hardware modifications. In this case, a reverse engineering method can only give limited grounds to assert that IC does not contain a hardware Trojan. In this regard, in [6] it is proposed to use destructive reverse engineering to determine "good" IC. Before performing any reverse engineering, indirect IC sampling characteristics are randomly examined, e.g. the profiles of power consumption, temperature, electromagnetic radiation and leakage currents. As a result, for each IC, a set of characteristics, fingerprint can be obtained. If there is some distribution of the selected characteristics, then all samples

Комбинированные атаки с применением аппаратных и программных средств, когда аппаратный троян отключает защиту памяти, а программный троян может расширить свои привилегии, обнаруживаются тестированием того, могут или нет непривилегированные программы получить доступ к закрытым для них разделам памяти. Этот подход требует также внесения изменений в операционную систему для работы с защитной схемой.

АНАЛИЗ КОСВЕННЫХ ХАРАКТЕРИСТИК

Анализ косвенных характеристик ИС (анализ побочных каналов), в отличие от непосредственной активации аппаратного трояна с целью его обнаружения, использует тот факт, что внедренный активационный триггерный механизм изменяет некоторые характеристики ИС независимо от того, активирована закладка или нет. Величина потребляемой мощности отдельными частями ИС, количество выделяемого тепла в определенных участках или время, необходимое определенным блокам для выполнения операций (задержка) – типичные примеры вторичных характеристик ИС, которые можно использовать для проведения такого анализа. Этот тип анализа, по всей видимости, обеспечивает наилучшую вероятность обнаружения аппаратного трояна, поскольку не требует его активации.

В работе [11] представлен характерный пример рассматриваемого механизма обнаружения закладок. Вначале исследуются образцы ИС без аппаратных троянов – эталонные ИС, снимаются одна или несколько характерных вторичных характеристик – так называемые "отпечатки пальцев". Далее тестируются другие чипы, и проводится сравнение их "отпечатков пальцев" с эталонными. Для того чтобы выбрать статистически значимые (но хорошо спрятанные) различия, могут быть использованы различные статистические методы. Авторы, в частности, использовали характеристику энергопотребления ИС в качестве основной косвенной характеристики. Очевидный недостаток метода заключается в том, что необходимо полностью быть уверенным, что эталонные ИС не "заражены".

Другая косвенная характеристика ИС – переходная характеристика потребляемой мощности – анализировалась в работе [12]. Цель работы – определение наименьшего размера аппаратного трояна, который можно обнаружить с помощью предлагаемого метода. Проведенные тесты, имитирующие работу конкретной экспериментальной ИС, показали, что этим методом можно обнаружить минимальную аппаратную закладку, состоящую из трех вентилей.

В работе [13] предложен метод, позволяющий усилить различие косвенных характеристик ИС, в которой отсутствовали аппаратные трояны, и такой же ИС, но "зараженной" закладкой. В качестве косвенной характеристики анализировалось энергопотребление. Использовался так называемый метод "устойчивого вектора", периодически подаваемого на отдельные входы ИС. Через некоторое время с момента подачи ИС входит в стабильное состояние. Эта процедура

from the sample are subjected to reverse engineering to check for hardware Trojans. In the future, belonging of the IC fingerprint to a typical distribution (for both "good" and "infested" IC) can be used for non-destructive IC sorting in a lot.

The described approach does not solve a number of problems. For example, hardware Trojans can be implemented by adding, removing or modifying only two logic gates [7], while modern IC consists of one billion gates. Search for a "needle in a haystack" requires complete reverse engineering of IC at the gate level, and it can be much more expensive than the IC development and production. On the other hand, there is no guarantee that the IC fingerprint with the hardware Trojan will be different from any non-infested IC against the background of increasing dispersion of IC performances, which is due to a decrease in the typical linear dimension.

NON-DESTRUCTIVE DETECTION METHODS

Non-destructive methods for the detection of hardware Trojans do not lead to a violation of the IC integrity, and are classified as invasive and non-invasive. The non-invasive methods do not change the IC project while the invasive ones can be characterised by making changes to the project in order to add functions that contribute to the Trojan detection.

Invasive methods are divided into two classes, preventive and auxiliary. Auxiliary methods are used in order to make it easier to detect the Trojan in the tests after IC manufacturing. In [3] a scheme is proposed that allows you to detect a hardware Trojan in a multi-modal project. This is achieved by using additional inputs and outputs which are added to each module.

названа авторами "переключательной минимизацией". Изменяя входной вектор, можно задействовать различные участки ИС. Изменения разницы потребляемой мощности с эталонным образцом свидетельствует о посторонних аппаратных устройствах в исследуемом участке ИС, то есть идентифицируются цепи, которые активны, но не должны быть таковыми.

Анализ и использование в качестве косвенной характеристики ИС и ее "отпечатков пальцев" задержки прохождения сигнала исследовалось в работе [14]. Авторы рассматривали две категории аппаратных троянов, имеющих явную и неявную нагрузки. Трояны с явной полезной нагрузкой напрямую влияют на схему, к которой они присоединены (например, изменяют значение управляющего или информационного сигнала). Аппаратные закладки с неявной полезной нагрузкой не вносят непосредственных изменений в цепь, но могут, например, считывать информацию через побочные каналы или исполнить DoS-атаку при инициализации. Авторы утверждают, что могут обнаружить 100% явных и 36% неявных аппаратных троянов, однако эксперименты проводились на симуляторах (моделирующих программах), а трояны представляли собой несложные модификации, специально разработанные и влияющие на энергопотребление и задержку прохождения сигнала. В аналогичной работе [15] в качестве косвенных характеристик и побочного канала рассматривались ток утечки и задержка прохождения сигнала.

Другой подход изложен в работе [3]. Авторы измеряли интеграционный ток – временные зависимости электрического заряда в узлах ИС, и использовали данные, полученные с различных участков схемы, для анализа и поиска троянской цепи. При анализе учитывались также данные, снятые с эталонной ИС, не содержащей закладок. Авторы заявили, что способны обнаружить внесенные аппаратные закладки, размером в "несколько вентилей", занимающие до 0,1% от площади всей ИС.

Основная проблема метода анализа косвенных характеристик для обнаружения аппаратных закладок заключается в том, что он полностью зависит от наличия подлинной эталонной ИС, которую можно использовать для сравнения и оценки. Если же аппаратная закладка была добавлена где-либо до стадии изготовления и, следовательно, содержится в каждой ИС, рассматриваемый метод неприменим. Кроме того, пространство поиска с использованием этого метода может быть очень большим. Несмотря на интересные разработки и использование современных статистических методов определения различий характеристик модифицированной и подлинной ИС, вероятность обнаружения такого отличия очень мала, особенно, если аппаратная закладка хорошо спроектирована и имеет целевое назначение.

ЗАКЛЮЧЕНИЕ

Таким образом, исследовательские работы, направленные на выявление аппаратных троянов, преимущественно посвящены разрушающим методам,

Additional inputs provide a "key" which translates a module into the "transparent mode". In this mode, the module performs self-testing of a circuit designed in such a way as to check the rare and unlikely event status. After the end of self-testing, at the module output there is a signature that includes the input key and self-testing results. This signature is then successively supplied to the input of the next module as input "key". Thus, a simple special input key entered at the main entrance will test the entire system, and the test result shows a single value at the main output. The authors argue that this method is effective against an attacker who has the information about the functional and logical structure of IC.

In practice, the logic allowing you to check the expanded space of states, which can manifest a hardware Trojan, provides very little protection from the targeted instrument bug. As discussed in this section, the likelihood of finding a professionally designed hardware Trojan is quite low. In addition, this method assumes that the hardware Trojan will be brought at a specific design stage. However, an attacker can insert Trojans after the development of a functional design of the module but before the development of the logic of the fingerprint definition.

In [8] a method based on the addition to the design of the dead trigger circuit, which results in an increased hardware Trojan activity during activation, is proposed. This makes its detection through the side channels easier. In [9], for the detection of a hardware backdoor through the side channels an additional circuit, which characterises the IC delay time changing in the event of a Trojan, is proposed.

Non-invasive methods for the detection of hardware Trojans are based on a comparison of IC

а также подходам с использованием побочных каналов и вспомогательных методов на этапе тестирования ИС. Механизмы обнаружения часто сосредоточены на конкретном классе аппаратных троянов, не существует единого метода или комбинации методов, которые могли бы обеспечить широкий охват при выявлении несанкционированных закладок.

Самый эффективный путь предупреждения внесения аппаратных закладок в ИС – тщательный контроль всего цикла разработки и изготовления. Небольшая проверенная команда разработчиков, использующих собственные программные средства и библиотеки, могут создать проект ИС, гарантированно свободный от аппаратных закладок. Изготовление такого проекта на проверенном кристальном производстве (управляемого небольшой группой поверенных лиц) обеспечит получение верных и надежных изделий. Заключительная сборка микросхем в корпуса и последующее их использование только лицами, которым полностью доверяет заказчик, обеспечит полную уверенность, что оригинальный проект реализован без вредоносных изменений.

Для такой страны, как Россия, которая не является лидером в полупроводниковой промышленности, замкнуть процесс от проектирования до изготовления возможно только для малых проектов специализированных ИС, поэтому доля ИС, изготовленных в кооперации с иностранными партнерами, будет увеличиваться. В связи с этим будет повышаться вероятность внесения аппаратных закладок. Для обеспечения безопасной работы электронной аппаратуры становится крайне важной разработка способов контроля, которые смогут надежно гарантировать аутентичность используемых ИС.

Возможен и другой подход, основанный на использовании сертифицированных коммерческих электронных компонентов, находящихся в свободной продаже (COTS – Commercial Off The Shelf – компонентов). Коммерческий сектор использует обширные библиотеки СФ-блоков, что обеспечивает быстрое развитие новых, более функциональных приборов (например, смартфонов). Если бы оборонные сектора разрабатывали и использовали только собственные СФ-блоки, то связанные с электроникой военные разработки находились бы далеко позади коммерческих гражданских продуктов. Поэтому имеет смысл создавать только некоторые ИС, такие как крипточипы, где полностью возможен проверенный цикл разработка/изготовление, особенно для чипов с малым количеством логических вентилей. Однако и в этом случае возможны кража, проведение обратного проектирования, изготовление ИС с модификацией и подмена оригинальных ИС через ненадежную цепь поставщиков и посредников.

Статья подготовлена при финансовой поддержке Минобрнауки России в рамках выполнения государственного задания 16.9021.2017/БЧ.

operating performances with the characteristics of the knowingly operational benchmark IC. Detection with the non-invasive method can be carried out during the IC operation or during IC testing. The detection mechanisms of during the IC operation largely overlap with the methods of counteracting hardware Trojans. If a hardware Trojan is found, you can try to continue the IC operation with it. Detection during the test is based on the improvement of traditional testing or an analysis of the side characteristics of the IC (side channel).

In [10] it details the approach to detect hardware Trojans using hardware and software. The strategy can detect only two types of attacks. DoS (Denial of Service) attacks are detected using a small customised protection circuit on the memory bus, which is programmed to respond to the episodic "survivability" pings. Failure to respond within the specified time is seen as a successful attempt to detect DoS attacks. Combined attacks using hardware and software when a hardware Trojan disables memory protection, and the software Trojan can extend its privileges can be found by testing whether or not non-privileged programmes can get access to the memory sections close for them. This approach also requires changes to the operating system to work with a protection circuit.

ANALYSIS OF INDIRECT CHARACTERISTICS

An analysis of the indirect IC characteristics (an analysis of side channels) in contrast to the immediate activation of the hardware Trojan, for the purpose of detecting it, exploits the fact that the injected activation trigger mechanism changes some characteristic of IC irrespective of whether or not the Trojan is activated. The amount of power consumed by different

ЛИТЕРАТУРА

1. **Potkonjak M.** Synthesis of trustable ICs using untrusted CAD tools // Proceedings of the 47th Design Automation Conference. – ACM, 2010. С. 633–634.
2. **Baumgarten A. et al.** A case study in hardware Trojan design and implementation // International Journal of Information Security. 2011. Vol. 10. №. 1. P. 1–14.
3. **Chakraborty R.S., Narasimhan S., Bhunia S.** Hardware trojan: Threats and emerging solutions. – http://www.trust-hub.org/resources/113, 2010.
4. **Love E., Jin Y., Makris Y.** Enhancing security via provably trustworthy hardware intellectual property // Hardware-Oriented Security and Trust (HOST), 2011. – IEEE International Symposium on. IEEE, 2011. С. 12–17.
5. **Necula G. C., Lee P.** Safe, untrusted agents using proof-carrying code // Mobile Agents and Security. Springer Berlin Heidelberg, 1998. С. 61–91.
6. **Agrawal D. et al.** Trojan detection using IC fingerprinting // Security and Privacy, 2007. SP'07. IEEE Symposium on. – IEEE, 2007. С. 296–310.
7. **Sturton C. et al.** Defeating UCI: Building stealthy and malicious hardware // Security and Privacy (SP), 2011 IEEE Symposium on. – IEEE, 2011. С. 64–77.
8. **Salmani H., Tehranipoor M., Plusquellic J.** New design strategy for improving hardware trojan detection and reducing trojan activation time // Hardware-Oriented Security and Trust, 2009. HOST›09. IEEE International Workshop on. – IEEE, 2009. С. 66–73.
9. **Li J., Lach J.** At-speed delay characterization for IC authentication and Trojan horse detection // Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on. – IEEE, 2008. С. 8–14.
10. **Bloom G., Narahari B., Simha R.** OS support for detecting Trojan circuit attacks // Hardware-Oriented Security and Trust, 2009. HOST'09. IEEE International Workshop on. – IEEE, 2009. С. 100–103.
11. **Abramovici M., Bradley P.** Integrated circuit security: new threats and solutions // Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies. – ACM, 2009. С. 55.
12. **Rad R., Plusquellic J., Tehranipoor M.** Sensitivity analysis to hardware Trojans using power supply transient signals // Hardware-Oriented Security and Trust, 2008. HOST 2008. – IEEE International Workshop on. IEEE, 2008. С. 3–7.
13. **Banga M., Hsiao M.S.** A novel sustained vector technique for the detection of hardware Trojans // VLSI Design, 2009 22nd International Conference on. IEEE, 2009. С. 327–332.
14. **Jin Y., Makris Y.** Hardware Trojans in Wireless Cryptographic ICs // IEEE Design&Test of Computers. – 2010. Т. 27. № 1. С. 26–35.
15. **Potkonjak M. et al.** Hardware Trojan horse detection using gate-level characterization // Design Automation Conference, 2009. DAC›09. 46th ACM/IEEE. IEEE, 2009. С. 688–693.

parts of the IC, the amount of heat generated in certain areas, or the time required by certain modules to perform operations (delay) are typical examples of the secondary characteristics of IC that can be used for the analysis. This kind of analysis appears to provide the best probability of hardware Trojan detection since it does not require any activation.

In [11] it shows a typical example of the considered Trojan detection mechanism. Initially IC samples are researched without hardware Trojans, the benchmark IC, and one or more characteristic of the secondary characteristics, the so-called "fingerprints" are taken. Then, other chips are tested, and their fingerprint are compared with the benchmark ones. In order to select statistically significant (but well hidden) differences, various statistical methods can be used. The authors, in particular, used the IC power consumption used as the main indirect characteristic. The obvious drawback of the method is that you should be completely sure that the benchmark IC is not infected.

Another indirect IC feature, the transient power consumption feature was analysed in [12]. The objective is to determine the smallest hardware Trojan which can be detected by the proposed method. The tests that emulate the work of a particular experimental IC have shown that this method can be used to detect the minimum hardware Trojan consisting of three gates.

In [13] a method to enhance the difference between the indirect characteristics of IC, which has no hardware Trojans, and the same IC but infected with a Trojan, was proposed. Power consumption was examined as an indirect feature. The so-called method of a sustainable vector periodically applied to individual IC inputs was used.

After some time of supplying, IC reaches the stable state. This procedure is called by the authors "switching minimisation". By changing the input vector, you can use different IC sections. Changing the difference of the consumed power with the benchmark sample indicates foreign hardware devices in the tested section of the IC, that is identified are chains which are active but they should not be active.

The analysis and use as an indirect characteristic of IC and its fingerprint of the signal delay were studied in [14]. The authors looked at two categories of hardware Trojans with explicit and implicit loads. Trojans with obvious useful load directly influence the circuit to which they are attached (e.g. change the value of the control or data signals). Hardware Trojans with implicit useful load do not make immediate changes to the circuit but may, for example, read information through side channels or perform DoS-attack when initialising. The authors argue that they can detect 100% explicit and 36% of implicit hardware Trojans but the experiments were conducted on simulators (simulation programmes), and the Trojans were simple modifications specially designed and affecting power consumption and path delay. In a similar paper [15] leakage current and path delay were considered as indirect characteristics and a side channel.

Another approach is described in [3]. The authors measured the integration current, time dependence of the electric charge in the IP nodes and used the data obtained from different parts of the circuit to make an analysis and search for the Trojan chain. The analysis also took into account the data taken from the benchmark IC not containing any Trojans. The authors have stated that they can detect the added hardware Trojans with the size of "a few gates" occupying 0.1% of the area of the entire IC.

The main problem of the method for analysing the indirect characteristics for the detection of the hardware Trojans is that it is totally dependent on the presence of a true benchmark IC which can be used for comparison and evaluation. If a hardware Trojan was added anywhere before the manufacturing stage and is therefore contained in each IC, the method in question is not applicable. Furthermore, the search space using this method can be very large. Despite the challenging developments and the use of modern statistical methods for determining differences in the characteristics of the modified and true IC, the likelihood of detecting this difference is very low, especially if the hardware Trojan is well designed and has a purpose.

CONCLUSION

Thus, studies aimed at the detection of hardware Trojans, are mainly devoted to destructive methods and approaches that use side channels and auxiliary methods in the testing phase of IC. Detection mechanisms are often focused on a particular class of hardware Trojans, there is no common method or combination of methods, which could ensure a wide coverage in identifying unauthorized bookmarks.

The most effective way to prevent any hardware Trojans in the IC is careful control of the whole cycle of development and manufacture. Small trusted team of developers using in-house software tools and libraries can create the IC project that is guaranteed free from hardware bookmarks. The implementation of this project on the proven crystal production (managed by a small group of trusted persons) will provide right and reliable products. Final assembly and packaging of microchips and their subsequent use only by persons who are completely trusted by the customer, will provide complete confidence that the original project was implemented without the malicious changes.

For a country like Russia, which is not a leader in the semiconductor industry, it is possible to close the cycle from design to manufacturing only for small projects of specialized IC, so the share of ICs made in cooperation with foreign partners, will increase. In this regard, the probability of insertion of hardware Trojans will increase. To ensure safe operation of electronic equipment it is extremely important to develop methods of control that will be able to securely guarantee the authenticity of the used ICs.

Also other approach based on use of the certified commercial electronic components (COTS – Commercial Off The Shelf) is possible. The commercial sector uses the vast libraries of IP cores for quick development of new and more functional devices (e.g., smartphones). If defensive sector will develop and use only their own IP cores, then the military developments related to electronics would be far behind commercial civil products. So it makes sense to develop only some ICs, such as the crypto chips with a small number of logical gates, where the completely proven cycle of development/manufacturing is possible. However, in this case theft, reverse engineering, modification during manufacturing and substitution of original IC through an unreliable chain of suppliers and intermediaries are also possible. ■

This paper was created with the financial support of the Ministry of Education and Science of the Russian Federation within the framework of the state order 16.9021.2017/БЧ.