АППАРАТНЫЕ ТРОЯНЫ. ЧАСТЬ 2: ПРИМЕРЫ РЕАЛИЗАЦИИ, СПОСОБЫ ВНЕДРЕНИЯ И АКТИВАЦИИ

HARDWARE TROJANS. PART2: EXAMPLES OF IMPLEMENTATION, METHODS OF INSERTION AND ACTIVATION

УДК 621.382, ВАК 05.27.01, DOI:10.22184/1993-8578.2016.70.8.12.20

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

Во второй части цикла статей, посвященных аппаратным закладкам в интегральных схемах – аппаратным троянам, приведены примеры их реализации и внедрения в интегральные схемы. Рассмотрены различные методы активации аппаратных троянов в электронной системе.
In the second part of a series of articles devoted to hardware Trojan examples of their implementation and insertion into integrated circuits are given. Various methods of hardware Trojan activating in electronic system are considered.

Аппаратные закладки лишь недавно попали в поле зрения исследователей, поэтому пока опубликовано сравнительно мало данных об их фактической реализации, и только в нескольких публикациях предпринято углубленное рассмотрение эффектов от атак с их использованием. Ниже рассматриваются наиболее интересные подходы к реализации аппаратных закладок.

В работе [1] представлены два наиболее общих подхода к созданию вредоносного процессора. Авторы показывают, как электрические схемы аппаратных троянов могут быть встроены в процессор для реализации таких атак, как кража паролей, расширение привилегий доступа и автоматические логины в систему. Представлена общая платформа для поддержки широкого спектра атак с возможностью их динамического обновления. В центральный процессор вносятся две модификации, которые реализуют механизм, обеспечивающий злоумышленнику доступ в защищенные области памяти, и теневой режим, позволяющий взломщику выполнить скрытую "встроенную программу". В работе описывается атака на логин, которая дает злоумышленнику полный высокий уровень доступа к процессору. Атака выполнена с помощью злонамеренной модификации, реализованной на схеме с использованием только 1341 вентилей. Авторами впервые приведена реализация аппаратной закладки, которая может использоваться в качестве общей программируемой платформы для атак. Показано внесение такой модификации на уровне VHDL (языка описания аппаратуры интегральных схем), проведено моделирование и синтез ИС для платформы на базе процессора Leon 3 SPARC 40 МГц. Рассмотрено обнаружение такого аппаратного трояна путем анализа внесенных им возмущений в аналоговые и цифровые сигналы. В частности, отмечается, что операционной системе виден программный компонент механизма доступа к памяти, и могут быть обнаружены задержки сигнала, связанные с внесением модификации. Также в работе [1] показаны общие подходы для обеспечения защиты от подобных вредоносных процессоров.

С целью изучения способов внедрения аппаратных закладок в политехническом институте Нью-Йоркского университета проводятся ежегодные конференции CSAW (Cyber Security Awareness Week – Неделя знаний об информа-

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

ционной безопасности). В рамках этой конференции организуются состязания между командами по внедрению и поиску встроенных аппаратных систем (Embedded System Challenge). В 2008 году было дано задание получить доступ к криптографическому устройству "АЛЬФА" на основе ПЛИС путем внесения набора аппаратных закладок, при этом устройство должно проходить тест на достоверность. Участникам соревнования выдали исходный HDL-код и предоставили один месяц на разработку. Победили две команды, одна из которых разработала механизм утечки информации секретных ключей через канал входа-выхода, другая – организовала DoS-атаку. Если обобщить все участвовавшие в состязании разработки, то аппаратные закладки были в 90% случаев внесены на этапе фазы разработки ИС, 50% из них активировались пользователем и 75% аппаратных троянов были размещены в схемах входа-выхода [2].

В работе [3] анализируется пространство проектных параметров аппаратных закладок и предлагается схема размером менее 50 вентилей, вырабатывающая мощность, которая может служить побочным каналом для скрытой утечки секретной информации. Технология, получившая название MOLES (Malicious Off-chip Leakage Enabled by Side-channels), была реализована в криптографической ИС на основе алгоритма AES, спроектированной по проектным нормам 45 нм. Использование метода расширенного спектра при разработке аппаратного трояна MOLES позволило осуществлять считывание многоразрядной информации на основе анализа потребляемой мощности с чувствительностью ниже уровня собственных шумов ИС, что обеспечивает скрытность. Авторы [3] заявляют, что данная технология обладает максимальной скрытностью и невосприимчивостью к большинству методов обнаружения аппаратных троянов, таких как визуальный контроль, проведение функциональных тестов и обнаружение на основе характерных "дактилоскопических" признаков ИС. Хотя схема задействует малое количество логических вентилей, вычислительные затраты для восстановления считанных данных, имеющих малое отношение сигнал / шум, с учетом вариабельности характеристик технологии, могут иметь критическое значение. Авторы [3] предложили обобщенную методологию проектирования и реализации MOLES-схем, опираясь на математический аппарат теории обнаружения для анализа дифференциальной мощности, которая необходима для экстракции многоразрядных ключей. Полученные результаты основаны на модели-

Hardware Trojans have only recently come in view of researchers, therefore, there is relatively little published data on their actual implementation, and only a few publications have undertaken an in-depth examination of the effects of their attacks. The following are considering the most interesting approaches to the implementation of hardware Trojans.

Paper [1] gives two of the most common approaches to creating malicious processors. The authors show how the electric circuits of hardware Trojans can be embedded in the processor to carry out such attacks as the theft of passwords, access privileges extension and automatic logins to the system. It presents a common platform to support a wide range of attacks with the possibility of their dynamic update. Two modifications are installed into the central processor to implement a mechanism that provides an attacker access to the protected memory area, and the shadow mode allowing an attacker to perform a silent embedded software. The Paper describes the attack on the login which allows the attacker a complete high level access to the processor. The attack is fulfilled with the help of a malicious modification based on the circuit by using only 1341 gates. For the first time the authors show the way of the implementation of hardware Trojan that can be used as a common programmed platform for the attacks. They show embedding of such a modification on the VHDL level (Hardware Description Language) and IC modelling and synthesis for the platform based on the 3 Leon SPARC 40 MHz processor have been conducted. Detection of this hardware Trojan by analysing the perturbations introduced by it into analogue and digital signals has been considered. In particular, it is noted that the operating system determines the software component of the memory access mechanism and it can detect a signal delay associated with the introduction of a modification. Also paper [1] shows common approaches to ensure the protection against these malicious processors.

In order to study how to embed hardware Trojans annual CSAW (Cyber Security Awareness Week)

рования экстракции только коротких ключей (8-бит), весьма далеких от реальной разрядности используемых ключей. При этом авторы указывают, какие вопросы необходимо решить для практического надежного восстановления многоразрядных ключей на основе анализа потребляемой мощности крипто-процессора.

В работе [4] проведены эксперименты с двумя упрощенными аппаратными закладками, встроенными в схемы шифрования на основе RSA – алгоритма для анализа эффектов, связанных с побочными каналами. В аппаратных закладках использовался простой счетчик, отключавший ИС после определенной пороговой величины, и компаратор, который сравнивал данные на системной шине или регистре с фиксированной величиной и вносил изменения в вычислительный процесс при превышении соответствия. Указывается, что такие аппаратные закладки достаточно трудно обнаружить, и они могут использоваться для отключения электрических схем, кражи информации, сбоев в системе, нарушения целостности и безопасности всей системы, в которую включена "зараженная" ИС.

В работе [5] рассматривается пример аппаратного трояна, действие которого приводит к утечке информации из ядра DES-шифрования. За такт схема извлекает один бит 56-разрядного ключа. Вскрывая один бит в каждом 64-разрядном блоке предаваемых данных, троян обеспечивает утечку информации. После накопления всех 56-ти блоков зашифрованного текста, полный ключ передается по радиоканалу, компрометируя шифрование. Извлеченный ключ спрятан в допустимом диапазоне амплитуды или частоты, обусловленном вариацией параметров технологического процесса, что обеспечивает соблюдение разработанных функциональных спецификаций ИС.

В работе [6] описан новый тип аппаратных закладок, основанных на надежностных характеристиках ИС. Этот тип троянов –достаточно простые модификации технологического процесса, которые приводят к ускорению деградации КМОП ИС. Изменения в технологии могут не затрагивать внутренние характеристики схемы, однако влияют на увеличение вариабельности технологических параметров, поэтому выявляются в ходе технологических тестов. Такие аппаратные трояны могут основываться на следующих деградационных физических явлениях: эффекте горячих электронов (эффект HCI), электрическом пробое затворного диэлектрика, эффекте температурной нестабильности при обратном смещении в p-МОП транзисторе (NBTI эффект), эффекте электромиграции. По классификации их можно отнести к постоянно действующим аппаратным троянам типа DoS (отказ в обслуживании), которые приводят к постепенной деградации рабочих характеристик, либо к ранним отказам отдельных частей ИС.

conferences are held at the Polytechnic Institute of New York University. As part of this conference, competitions between the teams for embedding and searching embedded hardware systems (Embedded System Challenge) are organized. In 2008 the task was given to gain access to the FPGA-based ALPHA cryptographic unit by introducing a set of hardware Trojans, while the device must be tested for validity. The participants of the competition received the source HDL-code and were given one month for development. Two teams won, one of which developed a mechanism for leaks of secret keys via the input-output channel but the other team organized of DoS attack. To synthesize all the projects considered in the competition, the hardware Trojans were embedded at the stage of IC development phase in 90% of cases, 50% of them were activated by the user, and 75% of hardware Trojans were embedded in the input-output circuits [2].

Paper [3] analyses the space of design objectives of hardware Trojans and a scheme of fewer than 50 gates is offered generating power output which can serve as a side channel for clandestine leakage of confidential information. The technology called MOLES (Malicious Off-chip Leakage Enabled by Side-channels) has been implemented in the cryptographic 45 nm IC based on the AES algorithm. The use of the spread-spectrum technique in the development of the MOLES hardware Trojan allowed to carry out reading out a multi-bit data on the basis of power consumption analysis with the sensitivity of below the level of IC own noises that ensure clandestine activity. The authors of paper [3] claim that this technology has the highest secrecy and immunity to most methods of detection of hardware Trojans, such as visual

МЕХАНИЗМЫ АКТИВАЦИИ ЗАКЛАДОК

Как правило, после внедрения в систему аппаратная закладка находится в состоянии покоя, пока не будет активирована (запущена) для выполнения своей вредоносной функции. Механизмы активации могут иметь разнообразный характер, явный или скрытый, случайный, непосредственный, или заранее определенный, в результате которых аппаратный троян может изменять свое состояние и поведение. Знания об этих механизмах важны, поскольку процесс активации может нести информацию, позволяющую выявить и противодействовать аппаратной закладке. Следует пытаться активировать аппаратные трояны на этапах верификации ИС. Обычно это выполняется при аттестационном и функциональном тестировании ИС или при исследовании пространства состояний проекта, включая состояния входов-выходов и внутренней логики. Активация аппаратной закладки во время тестирования может помочь идентифицировать ее наличие в ИС. Различные механизмы активации и их классификация коротко рассмотрены ниже.

АППАРАТНЫЕ ТРОЯНЫ С ВНУТРЕННЕЙ АКТИВАЦИЕЙ

Внутренняя активация основывается на некоторых специфических состояниях, при достижении которых в целевом устройстве происходит активация аппаратной закладки. В большинстве случаев она строится на схемах секвенциальной (последовательностной) или комбинационной логики.

АКТИВАЦИЯ НА ОСНОВЕ КОМБИНАЦИОННОЙ ЛОГИКИ

Аппаратный троян с активацией на основе комбинационной логики запускается при достижении так называемого триггерного состояния, когда определенные значения (векторы) обнаруживаются на определенных узлах внутренней схемы ИС. Этот тип активационного механизма может быть реализован только с использованием комбинационной логики (комбинационный триггер). В работе [7] авторы приводят пример так называемого "однотактного чит-кода" – специфического адреса на шине, который активизирует аппаратный троян. На практике комбинационная активация может потребовать большего набора определенных одновременных состояний на некоторых узлах, например на внутренних регистрах, совмещенных со специфическим словом на шине данных и определенным словом на адресной шине. В работе [8] приводится пример, в котором для активации аппаратной закладки используются определенные комбинированные наборы на входах ИС. В частности, это может быть определенный входной набор, объединяющий данные, управляющие команды, адреса и команды самотестирования.

inspection, conducting functional tests and the detection based on the characteristic "dactylographic" IC features. Although the scheme uses a small amount of logic gates, the computational cost for restoring the read data having a low S/N ratio may be critical taking the technology characteristics variability into account. The authors of paper [3] proposed a generalized design methodology and implementation of MOLES-schemes basing on the mathematical apparatus of the theory of detection for the analysis of differential power which is necessary for the extraction of multi-bit keys. The received results are based on modelling the extraction of only short keys (8-bit), which are very far from the real bit keys used. At the same time the authors point out what issues are needed to be solved for practical reliable restoring multi-bit keys basing on an analysis of crypto-processor power consumption.

Paper [4] displays experiments with two simplified hardware Trojans embedded in encryption schemes based on RSA, an algorithm for the analysis of the effects associated with the side channels. The hardware Trojans used a simple counter disabling the IC after a certain threshold value and a comparator comparing the data on the system bus or a register with a fixed value and made changes in the computational process in case of threshold crossing. It is stated that it is rather difficult to detect such hardware Trojans and they can be used for turning off the electrical circuits, information theft, introducing errors, destroying the integrity and security of the entire system into which the "contaminated" IC has been embedded.

Paper [5] describes an example of a hardware Trojan the effect of which leads to the leakage of information from the kernel DES-encryption. The circuit

АКТИВАЦИЯ НА ОСНОВЕ ПОСЛЕДОВАТЕЛЬНОСТНОЙ ЛОГИКИ

Аппаратный троян с активацией на основе последовательностной логики запускается определенной последовательностью событий. Если сравнивать с комбинационной активацией, то активация на последовательностной логике имеет намного большее пространство состояний, так как триггерный механизм здесь может реализовываться с использованием конечного автомата. В работе [9] отмечается, что поскольку конечный автомат обеспечивает логическую глубину, последовательность событий обычно описывается маловероятными логическими величинами, и обнаружить их во время тестирования и верификации ИС намного труднее.

Простейшим последовательностным триггером является схема синхронного счетчика, которая активируется после определенного количества циклов синхронизации. В работе [7] такие трояны названы "бомбами замедленного действия". В работе [9] обсуждаются счетчики асинхронных последовательностей, в которых при определенных событиях осуществляется приращение, например, увеличение фронта импульса на выходе вентиля. Эти же авторы предлагают использование гибридного механизма активации, комбинируя синхронные и асинхронные триггеры.

Также в работе [9] рассматриваются так называемые последовательные чит-коды. Например, к активации аппаратного трояна приводит последовательность байт 0xd, 0xe, 0xc, 0xa, 0xf, 0xb, 0xa, 0xd в течение различных восьми циклов синхронизации. При этом нет необходимости, чтобы данные байты приходили последовательно, они могут быть разнесены по времени. Таким образом, активация аппаратного трояна достигается гораздо более сложной последовательностью событий.

Задать сложность последовательностного триггера не представляет труда для разработчика аппаратной закладки. Единственная проблема, связанная с увеличением сложности – потребляемая трояном мощность и количество логических вентилей, необходимых для его реализации. В связи с этим были предложены внутренние последовательностные механизмы активации, которые используют физические и аналоговые эффекты в ИС. Например, мониторинг температуры чипа или потребляемой мощности могут быть включены в механизм пусковой схемы. Более того, в работе [9] приводится конкретный пример схемы, состоящей из электрической емкости, заряжающейся через резистор. Заряд и напряжение на емкости определяются активностью окружающей логики, которая в свою очередь может отражать активность ИС. Аппаратная закладка запускается при достижении на емкости определенного значения порогового напряжения.

Активационный триггер может быть как цифровым, так и аналоговым. Аналоговая активация используется с целью увеличения

extracts one bit of a 56-bit key in one phase. Exposing one bit in each 64-bit transmission data block, the Trojan provides the information leakage. After accumulating all 56 blocks of an encrypted text the full key is transmitted over the air compromising the encryption. The extracted key is hidden within the allowable range of the amplitude or frequency specified by a variation of the technological process parameters, which ensures compliance with the designed functional IP specifications.

Paper [6] describes a new type of hardware Trojans based on the IC reliability characteristics. This type of Trojan is easily embedded into the technological process and leads to the faster degradation of CMOS IC. It is possible that modifications will not affect the characteristics of the internal circuits but they affect the increase in variability of process parameters, therefore they are identified in the course of technological tests. Such hardware Trojans may be based on the following degradation physical phenomena: the hot electron effect (HCI effect), electrical breakdown of the gate dielectric, the temperature instability effect at a reverse bias in the p-channel MOS transistor (NBTI effect), and the electromigration effect. According to the classification they can be attributed to a permanent type of DoS (Denial of Service) hardware Trojans which lead to a gradual degradation of performance or to the early failures of separate parts of IC.

MECHANISMS OF ACTIVATION OF TROJANS

As a rule, a hardware Trojan is dormant after embedding into the system until it is activated (started) to perform its malicious function. Activation mechanisms can be diverse in nature, explicit or hidden, incidental, direct, or

скрытности и сложности его обнаружения. Злоумышленник может использовать несколько индивидуальных триггеров последовательностного типа для активации различных троянов в ИС.

Активация на основе последовательностной логики может предусматривать как контентные, так и временные события. В работе [10] исследовались такие триггеры, когда активация трояна происходит при определенных контентных данных в определенное время. Для простого активационного триггера было показано, что время тестирования, за которое можно с большой вероятностью активировать такой троян, составляет $3 \cdot 10^{35}$ лет: рассматривалась вероятность определения комбинации определенных числовых кодов, вводимых с клавиатуры за определенный интервал времени.

Авторы [10] предложили также "температурный триггер". Принцип его действия заключается в следующем. Активность определенных участков ИС на кристалле модулирует частоту кольцевого генератора, выполненного на инверторах. Частота кольцевого генератора определяет тепловыделение, которое влияет на задержку в другом подобном кольцевом генераторе. При достижении определенной величины задержки происходит активация аппаратной закладки. Похожие механизмы могут быть построены на использовании в качестве сигнала для активации электромагнитных или радиочастотных помех, частоты или потребляемой мощности логической схемы, а также временной характеристики потребляемой мощности определенных участков ИС.

АППАРАТНЫЕ ТРОЯНЫ С ВНЕШНЕЙ АКТИВАЦИЕЙ

Внешняя активация подразумевает некое взаимодействие аппаратного трояна с внешней средой, отличной от системы, в которую внедрен троян. Преимущества использования внешних триггеров для атакующего заключается в том, что активация инициируется источником, расположенным вне системы и поэтому не зависящим от нее [11]. В этой же работе приводятся примеры приемников или антенн внешнего сигнала, внедренных в "зараженный" прибор.

В работе [8] рассматриваются встроенные в чип сенсоры, которые могут осуществлять мониторинг физических параметров: температуры, электрического напряжения, электромагнитных помех, влажности и высоты над уровнем моря. Активационные механизмы с подобными сенсорами на чипе часто называют триггерами побочного канала по аналогии с технологиями получения информации в электронных приборах без непосредственного влияния на них [12]. Другие внешние механизмы активации аппаратных троянов основаны на непосредственном взаимодействии с целевым прибором. Также активация может быть инициализирована прикрепленным компонентом системы, например дополнительной памятью.

predetermined, as a result of which a hardware Trojan can change its state and behaviour. Knowledge of these mechanisms is important because the activation process may carry the information that enables to identify and counteract the hardware Trojan. It is necessary to try to activate the hardware Trojans at the stages of IC verification. This is usually carried out during the conformance and functional testing of ICs or space research of project conditions including the status of inputs, outputs and internal logic. Activation of a hardware Trojan during testing can help to identify its presence in the IC. Various mechanisms of activation and their classification are briefly discussed below.

HARDWARE TROJANS WITH INTERNAL ACTIVATION

Internal activation is based on some specific conditions at which activation of hardware Trojans in the target device takes place. In most cases it is based on the circuits of the sequential or combinational logic.

ACTIVATION BASED ON THE COMBINATIONAL LOGIC

The hardware Trojan with activation based on the combinational logic is embedded when the so-called flip-flop state is achieved and when certain values (vectors) are found on certain sites of the internal IC schemes. This type of an activation mechanism can be implemented only by using the combinational logic (combinational flip-flop). In their paper [7] the authors give the example of the so-called "single-cycle cheat code", a specific address on the bus, which activates a hardware Trojan. In practice the combinational activation may require a larger set of definite simultaneous states at certain nodes, such as internal registers combined with a

ПОСТОЯННО АКТИВНЫЕ АППАРАТНЫЕ ЗАКЛАДКИ

Существуют аппаратные закладки, которые всегда активны и не могут быть активированы или дезактивированы специальным триггерным механизмом. Возможны также аппаратные трояны, которые вносят незаметные изменения в спецификацию, функциональность или синхронизацию системы и не нуждаются в триггерном механизме. В качестве примера таких постоянно действующих троянов можно привести аппаратную закладку, производящую утечку данных через побочный канал, который отражает активность специфической ИС.

Постоянно активные аппаратные закладки могут иметь и более тонкие триггерные механизмы. В работе [11] обсуждается такая модификация топологии, при которой отдельные узлы или части ИС имеют большую вероятность отказа, то есть можно говорить, что триггерный механизм постоянно действует и приводит к непрерывной деградации рабочих характеристик ИС. В работе [6] рассматриваются модификации в ИС, в результате которых она выходит из строя после определенного периода эксплуатации длительностью от нескольких месяцев до года. Примеры таких аппаратных троянов – преднамеренные изменения в технологическом процессе, приводящие к ухудшению надежности ИС. Трудность их обнаружения связана с тем, что вносимые изменения не влияют на параметры ИС, которые находятся в допустимых пределах, характерных для технологического процесса. Поскольку такие трояны постоянно активны, они не имеют побочных активационных эффектов, таких как изменения шумовых характеристик ИС, изменения характера потребляемой мощности или температуры.

ОСОБЕННОСТИ РАЗРАБОТКИ ТРИГГЕРНЫХ МЕХАНИЗМОВ АКТИВАЦИИ

Разработчику аппаратного трояна достаточно просто создать триггерный механизм активации, который будет трудно обнаружить, поскольку он может использовать огромное пространство состояний системы, в которую внедряется троян. Это пространство состояний включает все внутренние узлы логических схем, входов и выходов ИС, модификацию топологии ИС, вариации технологических процессов, аналоговые эффекты электроники в ИС. Гибридные механизмы, совмещающие некоторые или все известные триггерные принципы, делают работу по обнаружению аппаратных закладок все более трудной. Общее мнение исследователей сводится к тому, что постоянно действующие аппаратные закладки намного более трудны для обнаружения по сравнению со сложными конструкциями триггерных механизмов для предотвращения случайной активации или активации во время тестирования.

ЗАКЛЮЧЕНИЕ

Внести и активировать аппаратные трояны становится проще с увеличением пространства состояний, повышением параллельности вычислений,

specific word on the data bus and a certain word on the address bus. In Paper [8] there is an example in which certain combination sets at IC inputs are used to activate the hardware Trojan. In particular, it may be a certain input set combining the data, control commands, addresses and self-testing commands.

ACTIVATION BASED ON THE SEQUENTIAL LOGIC

Hardware Trojan with activation on the basis of the sequential logic is embedded with the help of a specific sequence of events. In comparison with the combinational activation, the activation based on the sequential logic has a much larger state space as a flip-flop mechanism in this case can be implemented using finite state automation. It is stated in paper [9] that since finite state automation provides a logical depth, the sequence of events is usually described with the help of unlikely logical values; as a result, it is much more difficult to detect it during testing and verifying IC.

The simplest sequential flip-flop is a synchronous counter circuit which is activated after a certain number of timing loops. In paper [7], these Trojans are called "delayed-action bombs". In paper [9] asynchronous sequence counters are considered in which at certain events increments, for example, an increase in pulse edge at the exit gate, are carried out. These authors offer the use of a hybrid activation mechanism combining synchronous and asynchronous flip-flops.

Paper [9] also considers the so-called sequential cheat codes. For example, the sequence of bytes 0xd, 0xe, 0xc, 0xa, 0xf, 0xb, 0xa, 0xd during eight different timing loops leads to activation of a hardware Trojan. Besides, it is not necessary for the data bytes to come

усложнением внутренней разводки и возрастанием числа входов-выходов современных ИС. В таких условиях аппаратная закладка может быть глубоко скрыта внутри конструкции ИС и очень трудно поддаваться обнаружению. Необходимо отметить, что разработки, направленные на предотвращение внесения аппаратных троянов на этапе проекта или изготовления ИС, все еще находятся в зачаточном состоянии.

Статья подготовлена при финансовой поддержке Минобрнауки России в рамках выполнения государственного задания 8.527.2016/БЧ.

ЛИТЕРАТУРА

1. **Baumgarten A. et al.** A case study in hardware Trojan design and implementation // International Journal of Information Security. 2011. Т. 10. №. 1. С. 1–14.
2. **Rajendran J. et al.** Towards a comprehensive and systematic classification of hardware trojans // Circuits and Systems (ISCAS), Proceedings of 2010 IEEE International Symposium on. IEEE, 2010. С. 1871–1874.
3. **Lin L., Burleson W., Paar C.** MOLES: malicious off-chip leakage enabled by side-channels // Proceedings of the 2009 International Conference on Computer-Aided Design. ACM, 2009. С. 117–122.
4. Agrawal D. et al. Trojan detection using IC fingerprinting // Security and Privacy, 2007. SP'07. IEEE Symposium on. IEEE, 2007. С. 296–310.
5. **Jin Y., Makris Y.** Hardware Trojans in Wireless Cryptographic ICs // IEEE Design & Test of Computers. 2010. Т. 27. №1.С. 26–35.
6. **Shiyanovskii Y. et al.** Exploiting semiconductor properties for hardware trojans // arXiv preprint arXiv:0906.3834. 2009.
7. **Waksman A., Sethumadhavan S.** Silencing hardware backdoors // Security and Privacy (SP), 2011. IEEE Symposium on. IEEE, 2011. С. 49–63.
8. **Tehranipoor M., Koushanfar F.** A survey of hardware trojan taxonomy and detection // IEEE Design and Test of Computers. 2010. №1. Т. 27. С. 10–25.
9. **Chakraborty R.S., Narasimhan S., Bhunia S.** Hardware Trojan: Threats and emerging solutions // High Level Design Validation and Test Workshop, 2009. HLDVT 2009. IEEE International. IEEE, 2009. С. 166–171.
10. **Chen Z. et al.** Hardware trojan designs on basys fpga board // Embedded System Challenge Contest in Cyber Security Awareness Week-CSAW. 2008. Т. 2008.
11. **Wang X., Tehranipoor M., Plusquellic J.** Detecting malicious inclusions in secure hardware: Challenges and solutions // Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on. IEEE, 2008. С. 15–19.
12. **Potkonjak M.** Synthesis of trustable ICs using untrusted CAD tools // Proceedings of the 47th Design Automation Conference. ACM. 2010. С. 633–634.

sequentially; they can be separated in time. Thus, the activation of a hardware Trojan is achieved by much more complex sequence of events.

To develop the complexity of a sequential flip-flop is not difficult for a developer of hardware Trojans. The only problem associated with increasing complexity is the power consumed by the Trojan and the number of logic gates required for its embedding. In this regard internal sequential activation mechanisms that use physical and analogue effects in ICs have been offered. For example, chip temperature or power consumption monitoring may be included in the flip-flop mechanism of the circuit. Furthermore, Paper [9] gives a specific example of a circuit consisting of capacitance charged through a resistor. The charge and voltage on the capacitance are determined by the surrounding logic activity, which in turn may reflect IC activity. A hardware Trojan starts when the capacitance achieves a certain value of the threshold voltage.

The activating flip-flop can be either digital or analogue. The analogue activation is used to increase the secrecy and complexity of its detection. An intruder can use several types of sequential individual flip-flops to activate various IC Trojans.

Activation based on the sequential logic can include both content- and time-related events. Paper [10] studies such flip-flops when activation of a Trojan comes with certain content data at a specific time. For activating a simple flip-flop, it is shown that the testing time, for which you are likely to activate such a Trojan, is $3 \cdot 10^{35}$ years, the likelihood of determining the combination of specific numerical codes entered from the keyboard for a certain period of time is considered.

The authors [10] also proposed a "temperature flip-flop". Its operating principle is as follows. The activity of specific IC sections on a crystal modulates the frequency of the ring oscillator performed on the inverters. The ring oscillator frequency determines the heat release which affects the delay in the other similar ring oscillator. When you reach a certain amount of delay, the activation of the hardware Trojan takes place. Similar mechanisms may be constructed for use as a signal to activate the electromagnetic or radio frequency interference, frequency or power consumption of a logic circuit as well as the time characteristics of the power consumption of certain sections of the IC.

HARDWARE TROJANS WITH EXTERNAL ACTIVATION

External activation involves an interaction of a hardware Trojan with an external environment that is different from the system in which the Trojan is embedded. The advantages of using external flip-flops for the intruder is that activation is initiated by a source located outside the system and therefore not depending on it. [11] The same paper gives the examples of receivers or external signal antenna embedded in the 'infected' device.

The paper [8] discusses the sensors built in chip, they can monitor physical parameters, e.g. temperature, voltage, electromagnetic interference, humidity and altitude. The activation mechanisms with similar sensors on the chip are often referred to as side-channel flip-flops similar to the technology of obtaining the information in electronic devices without producing any direct effect on them [12]. Other external mechanisms of activation of hardware Trojans are based on the direct interaction with the targeted device. Activation may also be initialised by the system's attached component, such as additional memory.

CONSTANTLY ACTIVE HARDWARE TROJANS

There are hardware Trojans that are always active, and they cannot be activated or deactivated by a special flip-flop mechanism. There are also hardware Trojans that make subtle changes to the system specification, functionality or synchronization without the need of any flip-flop mechanism. Such permanent Trojans can be illustrated by the example of the hardware Trojan generating data leakage through a side channel that reflects the activity of a specific IC.

Constantly active hardware Trojans can have flip-flop mechanisms that are more subtle. Paper [11] discusses a modification topology in which the individual components or parts of ICs have a greater probability of failure, in other words, you can say that the flip-flop mechanism operates continuously and leads to continuous degradation of operating characteristics of the IC. Paper [6] considers modifications in IP as a result of which it breaks down after a certain period of operation lasting from several months to a year.

Examples of such hardware Trojans include intentional changes in the process leading to a deterioration in the reliability of ICs. The difficulty of detecting them is due to the fact that the modifications made do not affect the change in IC parameters that are within acceptable limits typical for a process. Because these Trojans are always active, they have no side activation effects, such as changes in the noise characteristics of IC, a change in the nature of power consumption and temperature.

FLIP-FLOP ACTIVATION MECHANISM DEVELOPMENT FEATURES

It is quite easy for the developer of a hardware Trojan to create a flip-flop activation mechanism which will be difficult to detect because it can use the huge space of system states in which a Trojan is introduced. This space of states includes all the internal components of logic circuits, the IC inputs and outputs, the IC topology modification, variation of manufacturing processes and the effects of analogue electronics in IC. Hybrid mechanisms combining some or all of the known flip-flop principles make the detection of hardware Trojans increasingly difficult. The general opinion of researchers is that the permanent hardware Trojans are much more difficult to detect than the complex designs of flip-flop mechanisms to prevent accidental activation or activation during testing.

CONCLUSION

It becomes easier to introduce and activate hardware Trojans with the increase in the state of states, an increase in parallel computing, complexity of internal wiring and increasing the number of modern IC outputs/inputs. In such circumstances, hardware Trojans can be hidden deep inside the IC design and are very difficult to be detectable. It should be noted that developments designed to prevent the introduction of hardware Trojans at the stage of designing or manufacturing ICs, are still in their infancy. ■

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 8.527.2016/БЧ.