Игорь А. Данилов[1], Павел С. Долотов[2]
[1,2]Акционерное общество «Экспериментальное научно-производственное объединение СПЕЦИАЛИЗИРОВАННЫЕ ЭЛЕКТРОННЫЕ СИСТЕМЫ»,
Каширское ш., 31, Москва, 115409, Россия,
[1,2]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия,
[1]e-mail: IADanilov@mephi.ru, https://orcid.org/0000-0001-7952-5392
[2]e-mail: PSDolotov@mephi.ru, https://orcid.org/0000-0003-4965-4761

ПРИМЕНЕНИЕ АСИНХРОННЫХ СХЕМ ДЛЯ ПОВЫШЕНИЯ ЗАЩИТЫ ОТ АТАК ПО СТОРОННИМ КАНАЛАМ

DOI: http://dx.doi.org/10.26583/bit.2022.2.09

Аннотация. Целью настоящей работы является анализ применения асинхронных схем для повышения защищенности информационных систем от атак по сторонним каналам – методов получения несанкционированного доступа к конфиденциальным данным и выполнения несанкционированных действий в системе. От криптографического анализа и эксплуатации программных ошибок, атаки по сторонним каналам принципиально отличаются нацеленностью на аппаратную часть атакуемой системы. Интегральные схемы во время работы непреднамеренно создают электромагнитные сигналы и обладают рядом эксплуатационных характеристик, которые могут подвергнуться исследованию со стороны злоумышленника и стать источниками утечки информации – сторонними каналами. Безопасность современных информационных систем невозможно в полной мере обеспечить без повышения устойчивости к таким атакам. Одним из методов противодействия атакам по сторонним каналам является использование асинхронных схем, главной отличительной чертой которых является отказ от использования глобального тактового сигнала для синхронизации отдельных элементов интегральной схемы в пользу локальной синхронизации, обеспечиваемой механизмом «рукопожатий». Интегральные схемы, при проектировании которых была применена асинхронная схемотехника, обладают рядом уникальных качеств, позволяющих эффективно противостоять таким атакам по сторонним каналам, как атаки по времени и атаки с применением анализа потребляемой мощности. В настоящей работе представлена классификация атак по сторонним каналам, описаны асинхронные схемы и их свойства, повышающие их устойчивость к некоторым типам атак по сторонним каналам, приведены примеры, наглядно демонстрирующие повышение защиты информационных систем, в которых используются асинхронные схемы.

Ключевые слова: атаки по сторонним каналам, асинхронные схемы, интегральные схемы, безопасность информационных систем.

Для цитирования. ДАНИЛОВ, Игорь А.; ДОЛОТОВ, Павел С. ПРИМЕНЕНИЕ АСИНХРОННЫХ СХЕМ ДЛЯ ПОВЫШЕНИЯ ЗАЩИТЫ ОТ АТАК ПО СТОРОННИМ КАНАЛАМ. Безопасность информационных технологий, [S.l.], т. 29, № 2, с. 112–127, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1422. DOI: http://dx.doi.org/10.26583/bit.2022.2.09.

Igor A. Danilov[1], Pavel S. Dolotov[2]
[1,2] Joint Stock Company "Experimental Research and Production Association SPECIAL ELECTRONIC SYSTEM",
Kashirskoe sh., 31, Moscow, 115409, Russia
[1,2]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe sh., 31, Moscow, 115409, Russia
[1]e-mail: IADanilov@mephi.ru, https://orcid.org/0000-0001-7952-5392
[2]e-mail: PSDolotov@mephi.ru, https://orcid.org/0000-0003-4965-4761

Using of asynchronous circuits to increase protection against side channels attacks

DOI: http://dx.doi.org/10.26583/bit.2022.2.09

Abstract. The aim of this study is to analyze the use of asynchronous circuits to improve the security of information systems against side-channels attacks, which are means of obtaining unauthorized access to confidential data and performing unauthorized actions in the system. Side-channels attacks are fundamentally different as compared with a cryptographic analysis and an exploitation of software errors in their focus on the hardware of the system under attack. Integrated circuits unintentionally create electromagnetic signals during their operation and have a number of performance characteristics that can be investigated by an attacker and therefore become the sources of information leakage, i.e., side-channels. The security of modern information systems cannot be fully ensured without increasing resistance to such attacks. One of the methods to counter side-channel attacks is the use of asynchronous circuits, which main distinguishing feature is the refusal from the use of a global clock signal to synchronize individual elements of an integrated circuit in favour of local synchronization provided by the "handshake" mechanism. Integrated circuits designed using asynchronous circuitry have a number of unique benefits that make it possible to effectively resist side-channel attacks, such as timing attacks and attacks with using power consumption analysis. This paper presents a classification of side-channels attacks, describes asynchronous circuits and their properties that increase their resistance to certain types of side-channels attacks, and provides examples that clearly show the increase in the protection of information systems with the asynchronous circuits.

Keywords: side-channel attacks, asynchronous circuits, integrated circuits, information systems security.
For citation: DANILOV, Igor A.; DOLOTOV, Pavel S. Using of asynchronous circuits to increase protection against side channels attacks. IT Security (Russia), [S.l.], v. 29, no. 2, p. 112–127, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1422. DOI: http://dx.doi.org/10.26583/bit.2022.2.09.

Введение

Атака по стороннему каналу – это любая атака, осуществляемая с использованием информации, полученной в результате взаимодействия с физической, в подавляющем большинстве случаев электронной, вычислительной системой, а не в результате криптографического анализа или эксплуатации программных ошибок. Все электронные устройства в процессе своей работы непреднамеренно создают различные сигналы электромагнитной природы и обладают такими характеристиками, как, например, время выполнения операций, которые можно рассматривать как каналы утечки информации и которые могут быть использованы злоумышленником для получения доступа к конфиденциальным данным, таким как ключи шифрования. Примерами таких сторонних, или побочных, каналов являются меняющееся во времени потребление энергии вычислительной системы и время выполнения операций шифрования.

Первые и основополагающие исследования, посвященные вопросам атак по сторонним каналам относятся к последнему десятилетию прошлого века [1] и к первому десятилетию этого [2]. В этих и более поздних работах рассматривались атаки на криптографические вычислительные машины с помощью анализа электромагнитного излучения электронных устройств, осуществляющих алгоритмы шифрования, их профиля потребления энергии и информации о времени выполнения ими операций шифрования данных. С появлением таких новых и повсеместно распространенных технологий, как персональные мобильные устройства, облачные вычисления, «интернет вещей» и т.п. вопрос защиты от атак по сторонним каналам стал ещё более актуальным, так как теперь злоумышленнику не обязательно находится в прямом физическом контакте с атакуемым устройством – атака может осуществляться удаленно. Примерами таких атак являются: атака по времени кэширования [3] и атака на буфер строк в динамической памяти с произвольным доступом, также известная как «row hummer» [4], которые могут быть проведены с помощью специального программного обеспечения, запущенного на удаленном облачном вычислительном узле. Активно исследуются также атаки по сторонним каналам на смартфоны, которые позволяют узнать текст, вводимый

пользователем на сенсорном экране с помощью штатно встроенных в устройство датчиков [5], установить текущее местоположение смартфона с помощью анализа статистики потребляемой устройством мощности, которая доступна обычным приложениям [6]. В случае [6] для атаки по стороннему каналу применяются алгоритмы машинного обучения, что, вообще говоря, довольно распространено. Более того, в последнее время для атак по сторонним каналам всё чаще стали применяться не классические алгоритмы машинного обучения вроде случайного леса [7] или метода опорных векторов [8], а глубокие нейронные сети [9].

Невозможность достижения абсолютной безопасности информационной системы от атак является очевидным и общеизвестным фактом. Все методы защиты информационных систем, так или иначе, сводятся к повышению сложности проведения атаки с целью сделать её настолько трудоёмкой и затратной по времени, что она станет нецелесообразной для злоумышленника. Методы защиты от атак по сторонним каналам направлены на затруднение анализа сигналов электромагнитной природы, которые создают в процессе своей работы электронные системы, и других характеристик систем, которые также могут служить побочными каналами, доступными для анализа злоумышленником. Одним из хорошо известных методов защиты криптографических систем является выполнение алгоритма шифрования за постоянное время, не зависящее от шифруемых данных и ключа шифрования, что затрудняет или полностью исключает проведение атаки, использующей анализ времени выполнения операций [10]. Другим примером является добавление в интегральную схему (ИС) источника шумов, затрудняющего анализ профиля потребляемой энергии защищаемого устройства [11].

Одним из методов защиты ИС, предназначенных для использования в доверенных системах, является использование асинхронных схем, ключевой особенностью и отличием которых от синхронных схем, является отказ от использования глобальных тактовых сигналов в пользу локальной синхронизации, обеспечиваемой протоколом, называемым «рукопожатия» («handshakes»). Благодаря особенностям асинхронных схем, системы, в которых они применяются, потенциально могут достигать более высокого быстродействия и работоспособности в более широком диапазоне внешних условий, таких как температура окружающей среды и напряжение питания, по сравнению с синхронными схемами, выполненными по тому же технологическому процессу. Побочным эффектом этих особенностей является то, что асинхронные схемы могут эффективно противостоять некоторым видам атак по сторонним каналам. В последнее время данному вопросу посвящено множество исследований, в частности применительно к смарт-картам [12] и криптографическим устройствам [13].

Целью настоящей работы является краткий обзор применения асинхронных схем для повышения защищенности информационных систем от атак по сторонним каналам.

Настоящая работа построена следующим образом. В разделе 1 дано краткое описание основных видов атак по сторонним каналам и приводится их классификация. В разделе 2 кратко описываются асинхронные схемы и их свойства, отличающие их от синхронных схем, которые позволяют повысить защищенность информационных систем от некоторых видов атак по сторонним каналам. В разделе 3 приводятся примеры практической реализации с помощью асинхронных схем ИС, защищенных от атак по сторонним каналам. Выводы приведены в заключении.

1. Классификация и основные виды атак по сторонним каналам

Известны различные подходы к классификации атак по сторонним каналам [14–15], в большинстве из которых используются следующие их характеристики:

- по возможностям атакующего: активные или пассивные;
- по виду утечки информации: преднамеренная или непреднамеренная утечка;
- по используемым свойствам системы: логическим или физическим;
- по уровню доступа злоумышленника к атакуемой системе: программный или физический;
- по необходимости проведения профилирования для осуществления атаки.

Данная классификация представлена на рис. 1 и описана далее.

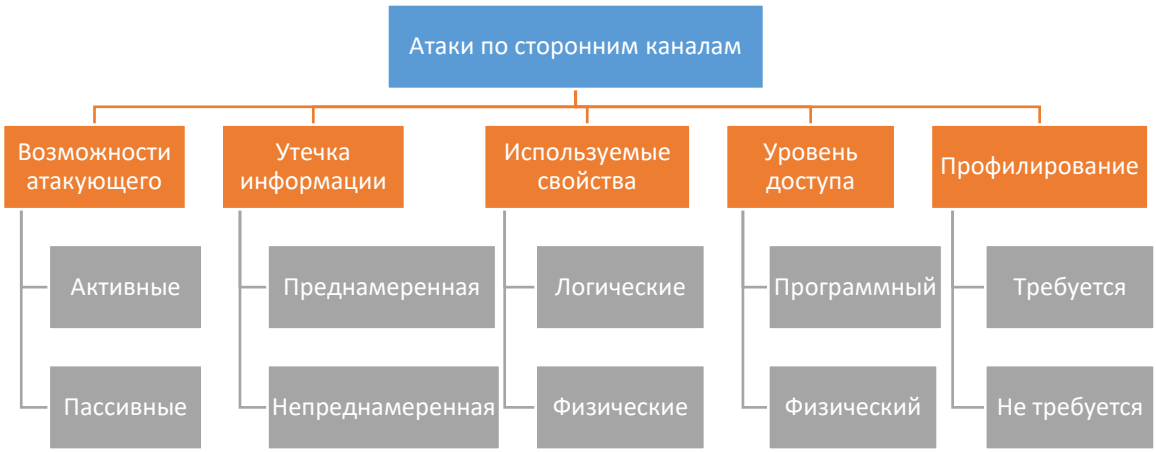

Рис. 1. Классификация атак по сторонним каналам
Fig. 1. Classification of attacks by third-party channels

По возможности атакующего атаки по сторонним каналам подразделяются на активные и пассивные. В случае пассивной атаки злоумышленник только наблюдает за поведением атакуемой информационной системы, использует утечку информации по сторонним каналам и анализирует её. Примером такого типа атак является анализ разницы в потреблении энергии при различных вычислительных операциях. При атаке активного типа злоумышленник может влиять на атакуемое устройство по стороннему каналу, например, изменяя температуру окружающей среды, напряжение питания или даже производя декапсуляцию микросхемы, чтобы вызвать изменения в его функционировании. Надо отметить, что действия злоумышленника, являющиеся штатным использованием атакуемого устройства, например, шифрование им определенных данных, не относятся к атакам по сторонним каналам активного типа.

По виду утечки информации атаки по сторонним каналам принято разделять на атаки с использованием непреднамеренной или преднамеренной утечки данных. Непреднамеренная утечка информации возникает при штатной эксплуатации электронных устройств в виде генерируемых ими сигналов электромагнитной природы, а также особенностями их функционирования, определяемыми их микроархитектурой. В качестве примера непреднамеренной утечки данных можно привести различное энергопотребление устройства при выполнении им разных вычислительных операций или различное время выполнения этих операций. Преднамеренная утечка информации возникает по каналам, заложенным в устройства их разработчиками при проектировании в целях использования во время штатной эксплуатации. Примером таких каналов утечки информации являются данные о потреблении энергии и данные со встроенных сенсоров температуры, предоставляемые с целью оптимизации работы устройства, список доступных Wi-Fi-сетей и другая подобная информация, которая доступна приложениям, запущенным, например, на смартфонах.

По используемым для атаки свойствам системы атаки по сторонним каналам подразделяются на физические и логические. Большинство примеров атак по сторонним каналам, которые приводились в настоящей работе ранее, являются примерами атак физического типа. Менее распространенным и относительно новым типом атак по сторонним каналам являются атаки логического типа, то есть атаки, которые используют только возможности программного обеспечения. Следует отметить, что атаки, которые, например, используют программное обеспечение для получения информации со встроенных в устройство датчиков температуры, не относятся к атакам логического типа. Примерами логических атак являются анализ доступного объёма памяти мобильного телефона с целью получения информации о посещенных веб-сайтах [16].

По уровню доступа злоумышленника к атакуемой системе атаки по сторонним каналам подразделяются на атаки с программным или физическим доступом. Атаки с программным уровнем доступа осуществляются только с помощью программного обеспечения, установленного на целевой информационной системе, которое позволяет проводить анализ способов и времени доступа к общим вычислительным ресурсам, анализировать доступ к кэш-памяти и др. Примерами подобных атак являются хорошо известные Spectre и Meltdown [17], а также описанные выше атаки на смартфоны. При физических атаках злоумышленник имеет непосредственный доступ к атакуемой системе и может анализировать такие сторонние каналы как потребление энергии, воздействовать на систему с помощью изменения температуры окружающей среды.

Также принято разделять атаки по сторонним каналам по необходимости проведения профилирования. Профилирование – это предварительный анализ и сбор характеристик атакуемой системы. Для таких атак необходим полный доступ к системе или её копии, полное знание особенностей её архитектуры и др. Примерами атак, для которых необходимо профилирование, являются уже упомянутые Spectre и Meltdown.

Для дальнейшего рассмотрения применения асинхронных схем для повышения защищенности информационных систем от атак по сторонним каналам необходимо описать распространённые методы атак на ИС. В соответствии с представленной выше классификацией, это активные и пассивные атаки, не требующие профилирования, использующие физические свойства атакуемой системы и непреднамеренные утечки информации, во время которых злоумышленник имеет физический доступ к системе.

Одним из самых известных методов атаки по стороннему каналу является атака с помощью анализа потребления энергии [18], описанная ещё в [19]. В основе данного метода лежит тот факт, что потребление энергии вычислительного устройства зависит от того, какие данные обрабатываются и какие инструкции выполняются. Как правило, во время таких атак измеряется падение напряжения на резисторе в цепи питания микросхемы, который в данном случае выступает сторонним каналом. Различают простой и дифференциальный анализ потребляемой мощности. В первом случае анализируется результат одного измерения, во втором случае проводится сравнение и статистический анализ множества измерений.

Разновидностью атаки с помощью анализа потребления энергии, которую выделяют в отдельный тип, является атака с помощью анализа электромагнитного излучения [20]. Так как злоумышленник не всегда может добавить резистор в цепь питания или осуществить измерение уровня потребления напрямую иным способом, то часто оказывается проще анализировать потребление опосредованно, исследуя электромагнитное излучение ИС.

Атаки по времени [10] основаны на анализе времени, затрачиваемого системой на выполнение команд алгоритма, которое может зависеть от входных данных. Если

злоумышленник может отслеживать время выполнения алгоритмов на атакуемой системе, то он получает доступ к стороннему каналу, анализируя утечку информации по которому, он может скомпрометировать систему. Естественной защитой от подобного рода атак является построение систем, в которых время выполнения алгоритмов, оперирующих конфиденциальными данными, постоянно и не зависит от входных данных.

К менее распространённым типам атак по сторонним каналам относится воздействие на целевую систему с помощью помех по цепям тактового сигнала или питания [21], а также изменение температуры окружающей среды [22].

2. Асинхронные схемы: виды, основные свойства и отличия от синхронных схем

Большинство цифровых ИС, разрабатываемых и выпускаемых в настоящее время, являются синхронными. Доминирование данного подхода к созданию цифровой электроники базируется на двух фундаментальных допущениях, лежащих в их основе, которые существенно упрощают их проектирование и верификацию: все сигналы двоичные, а время дискретно и одинаково для всех элементов [23]. Двоичность сигналов реализуется с помощью представления сигналов в цифровых ИС двумя уровнями напряжения, соответствующими, как правило, потенциалу земли и потенциалу напряжения питания, интерпретируемыми как логический ноль и логическая единица, соответственно. Дискретность времени реализуется с помощью использования тактовых сигналов, обеспечивающих синхронизацию отдельных элементов ИС между собой.

Упрощенное представление синхронной цифровой схемы представлено на рис. 2,а. Данные в схеме распространяются слева направо, тактовый сигнал CLK обеспечивает синхронизацию регистров, отмеченных на рисунке символом «R» и цифрой, построенных с помощью последовательностных элементов (элементов с памятью, триггеров). Регистры осуществляют хранение данных в течение периода тактового сигнала, после чего данные в них обновляются. За это время данные должны быть обработаны комбинационной логикой, отмеченной символом «CL» и цифрой.

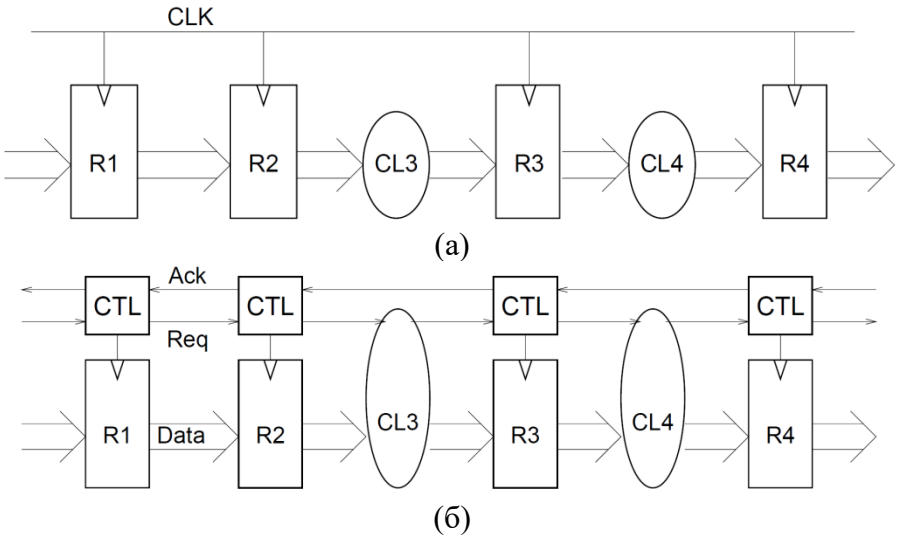

Рис. 2. Упрощенное представление синхронной (а) и асинхронной (б) схемы [23]
Fig. 2. Simplified representation of synchronous (a) and asynchronous (b) circuits [23]

Такая микроархитектура, как было отмечено выше, значительно упрощает проектирование и верификацию данного типа ИС, однако при масштабировании приводит к ряду проблем, которые существенно ограничивают возможности синхронных схем. Так, в современных сверхбольших интегральных схемах (СБИС) цепи распространения

тактовых сигналов становятся предельно сложными [24] и потребляют значительное количество энергии – до 60% от всей потребляемой энергии [25]. Кроме того, в современных ИС обычно используется не один, а множество тактовых сигналов, что усложняет задачу синхронизации и создает проблемы при пересечении доменов тактовых сигналов, которые асинхронны по отношению друг к другу [26].

В основе асинхронных схем лежит только одно из двух вышеописанных фундаментальных предположений – о дискретности (двоичности) сигналов. Время в данном классе устройств рассматривается как непрерывная физическая величина. Поэтому проблем синхронных схем, связанных с глобальной синхронизацией, в них просто нет – вместо общего тактирующего сигнала в асинхронных схемах используется протокол локальной синхронизации, называемый «рукопожатия» («handshakes»). Также очевидно, что к ним неприменимы методы атак по сторонним каналам, основанные на влиянии на тактовые сигналы электронного устройства.

Упрощенное представление асинхронной цифровой схемы представлено на рис. 2,б. Синхронизация здесь осуществляется с помощью специальных управляющих элементов, отмеченных как «CTL», с помощью взаимодействия с соседними CTL-элементами. При этом регистры R и комбинационная логика CL, в общем случае, могут быть такими же, как в синхронных схемах. Синхронизация осуществляется с помощью протокола «рукопожатий», который заключается в использовании сигналов запроса Req (request) и подтверждения Ack (acknowledge). Например, когда данные в регистре R1 готовы для отправки в регистр R2, ассоциированный с регистром R1 управляющий CTL-элемент подаёт на CTL-элемент, ассоциированный с регистром R2, сигнал Req. Когда регистр R2 готов принять эти данные, ассоциированный с ним управляющий CTL-элемент подаёт на CTL-элемент, ассоциированный с регистром R1, сигнал Ack и происходит передача данных из R1 в R2. Так в общем виде устроен протокол «рукопожатий».

Асинхронные схемы известны ещё с середины прошлого века [27], но не получили столь широкого распространения, как синхронные схемы, в силу ряда причин, основными из которых является повышенная, по сравнению с синхронными схемами, сложность их проектирования и верификации, заключающаяся, в частности, в их более сложном описании с помощью математического аппарата. Тем не менее, асинхронные схемы активно исследуются и используются, в том числе в коммерческих микросхемах таких компаний, как IBM, Intel и Sun Microsystems [28]. Более того, последние два десятилетия интерес к ним растёт, что связанно с тем, что синхронные схемы подошли к пределу своего развития, связанного с невозможностью увеличивать частоты тактовых сигналов. В то же время с помощью асинхронных схем можно потенциально создавать ИС, обладающие низким потреблением мощности [29], высоким быстродействием [30], низкими электромагнитными шумами [31], устойчивостью к флуктуациям температуры, напряжения питания и параметрам технологического процесса, по которому они изготовлены [32]. Отечественные учёные ведут активные исследования самосинхронных схем, являющихся одним из классов асинхронных схем [33], уделяя внимание таким вопросам, как использование промышленных САПР для проектирования данного класса устройств [34], повышения их сбоеустойчивости [35] и сбоеустойчивости их базовых элементов [36].

Протокол «рукопожатий» может быть реализован аппаратно различными способами. Каждый из этих способов влияет на такие характеристики устройства, как быстродействие, потребляемая мощность, занимаемая площадь, устойчивость к флуктуациям температуры окружающей среды и др. Протоколы, используемые в асинхронных схемах, классифицируются по двум основным свойствам: по способу кодирования сигналов и по количеству фаз в одной операции.

Сигналы могут кодироваться обычным способом, как в синхронных схемах, и передаваться по однопроводной линии, или кодироваться двумя сигналами, находящимися в противофазе. Последний способ кодирования называется двухпроводным («dual rail»). Теоретически, сигналы могут кодироваться и большим количеством бит, но на практике такие способы кодирования, как правило, не встречаются.

По количеству фаз в одной операции протоколы, используемые в асинхронных схемах, бывают четырехфазные и двухфазные. Как и в случае с кодированием сигналов, возможна реализация большего числа фаз, но на практике это лишено смысла. В четырехфазных протоколах передающее устройство отправляет данные и выставляет сигнал запроса Req, после чего ожидает от приемного устройства сигнала подтверждения Ack; когда принимающее устройство отвечает выставлением сигнала Ack, передающее устройство должно вернуть сигнал Req в исходное логическое состояние, а принимающее устройство после этого должно вернуть в исходное логическое состояние сигнал Ack; после этого транзакция считается законченной. В двухфазных протоколах не происходит возвращения в исходное логическое состояние сигналов Req и Ack, другими словами, в двухфазных протоколах сигналы запроса и подтверждения кодируются не логическим уровнем, а изменением логического состояния. Очевидно, что для построения быстродействующих асинхронных схем предпочтительными являются двухфазные реализации протокола «рукопожатий», хотя они обычно более сложные с точки зрения обеспечения локальной синхронизации.

Одним из распространенных протоколов «рукопожатий» является протокол «объединенные данные» («bundled data»), который бывает двухфазным или четырехфазным [23]. Данный протокол представлен на рис. 3. На рис. 3,а представлена упрощенная логическая схема протокола, из которой видно, что сигналы запроса и подтверждения передаются по отдельным линиям. На рис. 3,б и 3,в представлены упрощенные временные диаграммы сигналов Req, Ack и данных при четырехфазной и двухфазной реализации протокола, соответственно.

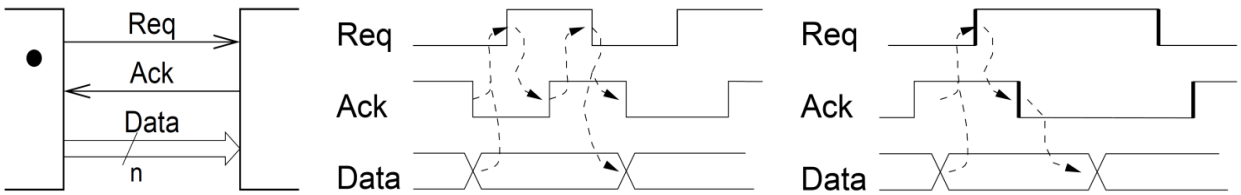

Рис. 3. Протокол локальной синхронизации «объединенные данные»: упрощенная логическая схема (а), упрощенная временная диаграмма при четырехфазной реализации протокола (б), упрощенная временная диаграмма при двухфазной реализации протокола (в) [23]
Fig. 3. Local synchronization protocol «combined data»: simplified logic diagram (a), simplified time diagram for four-phase protocol implementation (b), simplified time diagram for two-phase protocol implementation (c) [23]

Другим распространенным вариантом реализации протокола «рукопожатий» является двухпроводной четырехфазный протокол, упрощенная логическая схема которого представлена на рис. 4,а, а соответствующая ей упрощенная временная диаграмма – на рис. 4,б. В данном протоколе сигнал запроса встроен в данные, что иллюстрируется временной диаграммой на рис. 4,б и соответствующей ей таблицей истинности (табл. 1). Каждый передаваемый бит информации передается по двум

проводам. Передача информации («Valid») с помощью противофазных сигналов обязана перемежаться «пустым» («Empty») состоянием-заполнителем, в котором оба сигнала находятся в одинаковом логическом состоянии, как правило в логическом «0». После того как передающее устройство отправляет принимаемому устройству данные с закодированном в них сигналом запроса, принимающее устройство должно выставить сигнал Ack, передаваемый по отдельной линии; передающее устройство отвечает на это переводом линий, по которым передаются данные в «пустое» состояние-заполнитель, что является эквивалентом возвращения сигнала Req в исходное логическое состояние, как в рассмотренном выше протоколе «объединенные данные»; принимающее устройство в ответ возвращает в исходное логическое состояние сигнал Ack. Очевидно, что обычная шина данных значительно шире одного бита. На практике это означает, что принимающее устройство считает, что поступил сигнал Req только тогда, когда все сигналы, передающиеся по паре линий, примут состояние, соответствующее логическому «0» или логической «1».

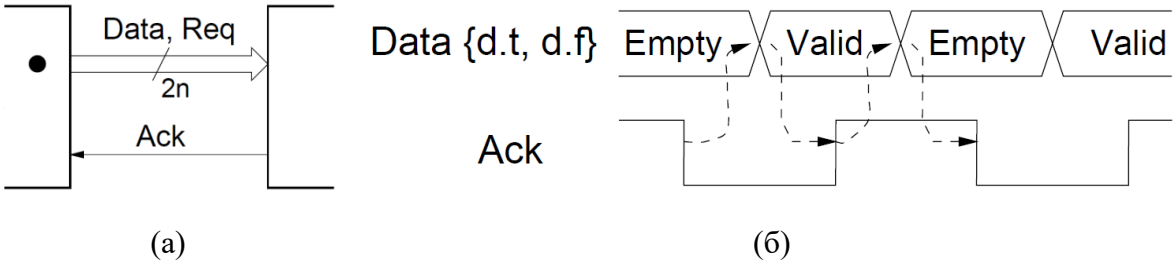

Рис. 4. Двухпроводной четырехфазный протокол локальной синхронизации: упрощенная логическая схема (а), упрощенная временная диаграмма (б) [23]
Fig. 4. Two-wire four-phase local synchronization protocol: simplified logic circuit (a), simplified time diagram (b) [23]

Таблица .1 Таблица истинности двухпроводного четырехфазного протокола локальной синхронизации

Состояние	d.t	d.f
Empty («пустое состояние»)	0	0
Передача логического «0»	0	1
Передача логической «1»	1	0
Запрещенное состояние	1	1

В асинхронных схемах применяются и другие протоколы, например, двухпроводной двухфазный протокол, не рассмотренные в настоящей работе.

Ключевым элементом многих асинхронных схем является С-элемент Маллера, представляющий собой элемент с памятью [37]. Данный элемент хранит предыдущее логическое состояние на своём выходе, если значения на его входах различаются и передает логическое состояние на входах, если они совпадают, на выход. На рис. 5 представлен конвейер Маллера модификации которого используются для синхронизации почти во всех вариантах реализации асинхронных схем. С-элементы отмечены символом «С». Из рис. 5 легко увидеть, что именно с помощью С-элемента осуществляется локальная синхронизация. С-элементы являются предметом научных исследований [38], в частности изучается вопрос повышения их устойчивости к радиационно-индуцированным сбоям [39].

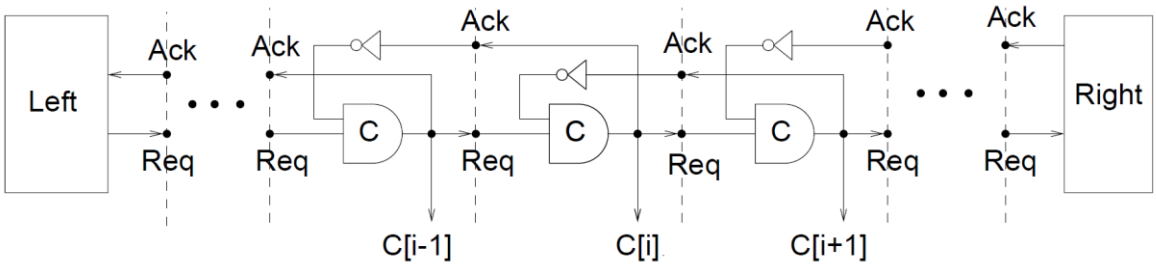

Рис. 5. Конвейер Маллера [23]
Fig. 5. Muller conveyor [23]

Из описанных выше базовых принципов функционирования асинхронных схем очевидно, что переключения регистров, хранящих промежуточные данные, происходит в них по мере готовности этих данных и потому моменты этих переключений оказываются равномерно распределены по времени, в отличие от синхронных схем, в которые переключения происходят в строго определенные моменты времени, определяемые тактовым сигналом. Благодаря этому потребление энергии асинхронных схем оказывается более «сглаженным», по сравнению с синхронными схемами, без явных «пиков» и «провалов». Это делает асинхронные схемы более устойчивыми к атакам по сторонним каналам с помощью анализа потребления энергии устройством. По тем же самым причинам, время распространения сигналов в асинхронных схемах сильно зависит от входных данных, что делает их потенциально менее устойчивыми к такому виду атак по сторонним каналам, как атаки по времени. Однако в виду отсутствия тактового сигнала, а, следовательно, и временной точки отсчёта, при правильном проектировании, асинхронные схемы могут быть сделаны устойчивыми и к атакам по времени.

3. Примеры применения асинхронных схем для защиты от атак по сторонним каналам

В данном разделе представлены примеры практического применения асинхронных схем при проектировании ИС для повышения защиты информационных систем, в которых они применяются.

В [13] показано, что применение двухпроводного кодирования сигналов с двойным «спэйсером» (состояние «Empty», см. рис. 4,б), балансирование путей распространения сигналов, а также использования механизма добавления случайно изменяющихся задержек кардинально повышает защищенность ИС от атак по времени и атак с использованием анализа потребляемой мощности.

Авторы работы [40] анализировали защищенность самосинхронных схем от атак с помощью анализа потребления энергии и от атак по времени. Для этого были разработаны два варианта ARM-совместимого микропроцессора SPA [41]. Результаты исследования показали, что вариант устройства, в котором применялось двухпроводное («dual rail») кодирование сигналов обладает значительно большей защищенностью от атак по сторонним каналам с применением анализа потребляемой мощности. Авторы утверждают, что самосинхронные схемы имеют большой потенциал для создания СБИС, устойчивых к атакам по сторонним каналам такого типа. Авторы отмечают, что отсутствие тактовых сигналов в исследуемых устройствах значительно затрудняют для потенциального злоумышленника проведение статистического анализа, а использование двухпроводного кодирования и техники балансирования логики в совокупности с использованием специальных схем защёлок кардинально снижают различия в диаграммах потребляемой мощности при выполнении ИС вычислительных операций. В заключение авторы делают вывод об

очевидной возможности применения самосинхронных схем для построения ИС с крайне высокой защитой от атак по сторонним каналам, основанных на анализе потребляемой мощности и на анализе временных характеристик устройства, то есть от атак по времени.

В [42] представлен ускоритель AES-алгоритма шифрования, разработанный по технологии с проектной нормой 65 нм. Данное устройство спроектировано с помощью библиотеки асинхронной логики, основанной на стандартных ячейках, предназначенных для проектирования синхронных схем, которые, как правило, входят в комплект средств проектирования, предоставляемой разработчику фабрикой. Для повышения защиты от атак по сторонним каналам, как и в предыдущем случае, используется двухпроводное кодирование сигналов и специальный механизм, вносящий вариации во внутренние задержки схемы при её функционировании, что затрудняет проведение атак по времени. Авторы утверждают, что разработанное ими устройство полностью защищено от атак по сторонним каналам, основанным на анализе временных характеристик и мощности потребления. Их выводы основаны на попытке проведения данного типа атак с помощью 5000 результатов моделирования устройства.

В [43] описана реализация китайского алгоритма блочного шифрования SM4 в виде асинхронной схемы, которая была прототипирована по технологическому процессу с проектными нормами 180 нм. В работе использовалась специальная, так называемая, асинхронная «домино»-логика, описанная в [44]. На рис. 6,а представлена принципиальная электрическая схема логического элемента «И», выполненного в таком стиле проектирования. Входные сигналы схемы обозначены a_t, a_f и b_t, b_f, где постфиксы _t и _f обозначают прямой и противофазный сигналы в схеме двухпроводного кодирования, соответственно, а pc – это сигнал, приходящий с последующей за текущей ступенью асинхронного конвейера. На рис. 6,б представлена схема индикации окончания переходных процессов на основе С-элемента Маллера, служащая для обеспечения локальной синхронизации. Приведенное в [43] устройство занимает небольшую площадь, обладает крайне низким потреблением энергии и повышенной защищенностью от атак по сторонним каналам.

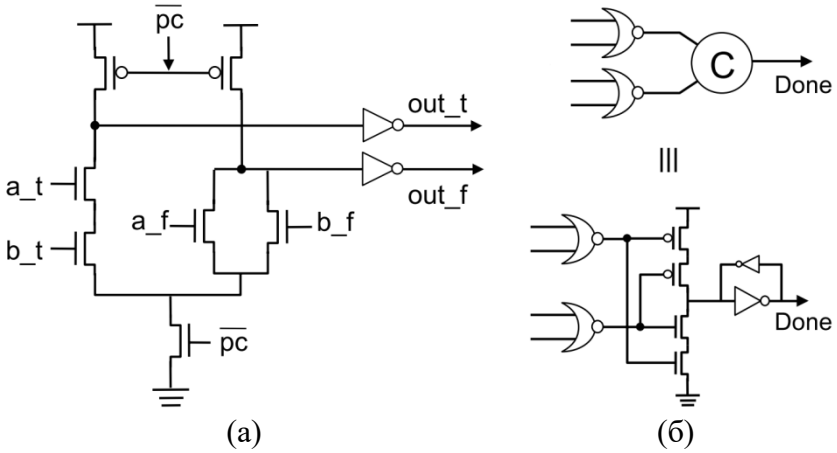

Рис. 6. Асинхронная «домино-логика: логический элемент «И» (а), схема индикации завершения переходных процессов и генерации сигнала «Done» (б) [44]
Fig. 6. Asynchronous «domino» logic: the logic element «AND» (a), the indication circuit for the completion of transients and the generation of the «Done» signal (b) [44]

В [45] представлен асинхронный многопортовый роутер типа Сеть-на-Кристалле, выполненный по технологическому процессу с проектными нормами 65 нм. Данное

устройство обладает значительной защищенностью от атак по сторонним каналам с помощью анализа потребляемой мощности благодаря тому, что в нём реализован механизм варьирования количества задействованных портов и подстройке напряжения питания внутренних блоков.

В большинстве приведенных примеров для проектирования асинхронных схем с повышенной защищенностью от атак по сторонним каналам использовалось двухпроводное («dual rail») кодирование сигналов, затрудняющее для потенциального злоумышленника проведение статистического анализа потребляемой мощности.

Также стоит отметить, что в большинстве примеров были использованы механизмы внесения случайных задержек для повышения защищенности от атак по времени. В целом, приведенные примеры показывают перспективность применения асинхронных схем для повышения безопасности информационных систем в части защиты от некоторых типов атак по сторонним каналам.

Заключение

В настоящей работе проведен обзор основных видов атак по сторонним каналам на современные информационные системы и представлена их классификация, изложены базовые принципы функционирования асинхронных схем и показаны основные протоколы локальной синхронизации и способы кодирования данных, используемые в них. Приведенные примеры позволяют сделать вывод о том, что для проектирования асинхронных схем с повышенной защитой от атак по сторонним каналам оптимально применять двухпроводное кодирование сигналов, четырехфазный протокол локальной синхронизации и балансирование линий передачи данных для защиты от атак с помощью анализа потребляемой мощности, а также использовать механизмы, вносящие случайные, меняющиеся во времени, задержки в элементы асинхронной схемы для повышения защиты от атак по времени. Рассмотренные примеры применения асинхронных схем для повышения защиты от атак по времени и атаки с помощью анализа потребляемой мощности, показывают, что асинхронные схемы являются перспективным направлением исследований для обеспечения безопасности современных информационных систем.

СПИСОК ЛИТЕРАТУРЫ:

1. Kocher P.C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. Advances in Cryptology — CRYPTO ’96, Berlin, Heidelberg. 1996, p. 104–113. DOI: https://doi.org/10.1007/3-540-68697-5_9.
2. Mangard S., Oswald E. and Popp T. Power Analysis Attacks: Revealing the Secrets of Smart Cards, 1st ed. Springer Publishing Company, Incorporated, 2007. DOI: https://doi.org/10.1007/978-0-387-38162-6.
3. Tromer E., Osvik D.A. and Shamir A. Efficient Cache Attacks on AES, and Countermeasures. J Cryptol, vol. 23, no. 1, p. 37–71, Jan. 2010. DOI: http://dx.doi.org/10.1007/s00145-009-9049-y.
4. Pessl P., Gruss D., Maurice C., Schwarz M. and Mangard S. DRAMA: Exploiting DRAM Addressing for Cross-CPU Attacks. 2016. URL:https://www.researchgate.net/publication/285459017_DRAMA_Exploiting_DRAM_Addressing_for_Cross-CPU_Attacks (дата обращения: 18.05.2022).
5. Mehrnezhad M., Toreini E., Shahandashti S.F. and Hao F. TouchSignatures: Identification of User Touch Actions and PINs Based on Mobile Sensor Data via JavaScript. Journal of Information Security and Applications, vol. 26, p. 23–38, Feb. 2016. DOI: http://dx.doi.org/10.1016/j.jisa.2015.11.007.
6. Michalevsky Y., Nakibly G., Schulman A., Veerapandian G.A. and Boneh D. PowerSpy: Location Tracking using Mobile Device Power Analysis, arXiv, arXiv:1502.03182, Aug. 2015. DOI: http://dx.doi.org/10.48550/arXiv.1502.03182.
7. Patel H. and Baldwin R.O. Random Forest profiling attack on advanced encryption standard. International Journal of Applied Cryptography, vol. 3, no. 2, p. 181–194, Jan. 2014. DOI: http://dx.doi.org/10.1504/IJACT.2014.062740.

8. Zeng Z., Gu D., Liu J. and Guo Z. An Improved Side-Channel Attack Based on Support Vector Machine. Tenth International Conference on Computational Intelligence and Security. 2014, p. 676–680. DOI: http://dx.doi.org/10.1109/CIS.2014.80.
9. Shaikh M., Arain Q.A. and Saddar S. Paradigm Shift of Machine Learning to Deep Learning in Side Channel Attacks - A Survey. 6th International Multi-Topic ICT Conference (IMTIC). 2021, p. 1–6. DOI: http://dx.doi.org/10.1109/IMTIC53841.2021.9719689.
10. Biswas K., Ghosal D. and Nagaraja S. A Survey of Timing Channels and Countermeasures. ACM Comput. Surv., vol. 50, no. 1, p. 6:1–6:39, 2017. DOI: http://dx.doi.org/10.1145/3023872.
11. Quisquater J.-J. and Samyde D. ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards. in Smart Card Programming and Security, Berlin, Heidelberg. 2001, p. 200–210.
12. Moore S., Anderson R., Cunningham P., Mullins R. and Taylor G. Improving smart card security using self-timed circuits. In Proceedings Eighth International Symposium on Asynchronous Circuits and Systems, Apr. 2002, p. 211–218. DOI: http://dx.doi.org/10.1109/ASYNC.2002.1000311.
13. Cilio W., Linder M., Porter C., Di J., Smith S. and Thompson D. Side-channel attack mitigation using dual-spacer Dual-rail Delay-insensitive Logic (D3L). In Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon), Mar. 2010, p. 471–474. DOI: http://dx.doi.org/10.1109/SECON.2010.5453826.
14. Spreitzer R., Moonsamy V., Korak T. and Mangard S. Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. IEEE Communications Surveys Tutorials, vol. 20, no. 1, p. 465–488, 2018. DOI: http://dx.doi.org/10.1109/COMST.2017.2779824.
15. Kaur S., Singh B. and Kaur H. Analytical Classifications of Side Channel Attacks, Glitch Attacks and Fault Injection Techniques: Their Countermeasures. In 2020 Indo – Taiwan 2nd International Conference on Computing, Analytics and Networks (Indo-Taiwan ICAN). 2020, p. 144–151. DOI: http://dx.doi.org/10.1109/Indo-TaiwanICAN48429.2020.9181324.
16. Ferrag M.A., Maglaras L., Derhab A. and Janicke H. Authentication schemes for smart mobile devices: threat models, countermeasures, and open research issues. Telecommun Syst, vol. 73, no. 2, p. 317–348, Feb. 2020. DOI: http://dx.doi.org/10.1007/s11235-019-00612-5.
17. Abu-Ghazaleh N., Ponomarev D. and Evtyushkin D. How the spectre and meltdown hacks really worked. IEEE Spectrum, vol. 56, no. 3, p. 42–49, Mar. 2019. DOI: http://dx.doi.org/10.1109/MSPEC.2019.8651934.
18. Yan L., Guo Y., Chen X. and Mei H. A Study on Power Side Channels on Mobile Devices, arXiv, arXiv:1512.07972, Dec. 2015. DOI: http://dx.doi.org/10.48550/arXiv.1512.07972.
19. Kocher P., Jaffe J. and B. Jun. Differential Power Analysis. In Advances in Cryptology — CRYPTO' 99, Berlin, Heidelberg. 1999, p. 388–397.
20. Gebotys C.H., Ho S. and Tiu C.C. EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA. In Cryptographic Hardware and Embedded Systems – CHES 2005, Berlin, Heidelberg. 2005, p. 250–264. DOI: http://dx.doi.org/10.1007/11545262_19.
21. O'Flynn C. Fault Injection using Crowbars on Embedded Systems. IACR Cryptol. ePrint Arch., p. 810, 2016.
22. Hutter M. and Schmidt J.-M. The Temperature Side Channel and Heating Fault Attacks. In Smart Card Research and Advanced Applications, Cham. 2014, p. 219–235. DOI: http://dx.doi.org/10.1007/978-3-319-08302-5_15.
23. Sparsø J. and Furber S. Principles of Asynchronous Circuit Design. Boston, MA: Springer US, 2001. DOI: http://dx.doi.org/10.1007/978-1-4757-3385-3.
24. Liu M., Zhang Z., Wen J. and Jia Y. An Approximate Symmetry Clock Tree Design with Routing Topology Prediction. IEEE International Midwest Symposium on Circuits and Systems (MWSCAS). 2021, p. 92–96. DOI: http://dx.doi.org/10.1109/MWSCAS47672.2021.9531772.
25. Veendrick H. J.M. Nanometer CMOS ICs: From Basics to ASICs. Cham: Springer International Publishing, 2017. DOI: http://dx.doi.org/10.1007/978-3-319-47597-4.
26. Kebaili M., Brignone J. and Morin-Allory K. Clock domain crossing formal verification: a meta-model. IEEE International High Level Design Validation and Test Workshop (HLDVT). 2016, p. 136–141. DOI: http://dx.doi.org/10.1109/HLDVT.2016.7748267.
27. Muller D.E. and Bartky W.C. A theory of asynchronous circuits. Annals of Computing Laboratory of Harvard University, no. 5, p. 204–243, 1959.
28. Nowick S.M. and Singh M. High-performance asynchronous pipelines: An overview. IEEE Design and Test of Computers, vol. 28, no. 5, p. 8–22, 2011. DOI: http://dx.doi.org/10.1109/MDT.2011.71.
29. Weber L. de Oliveira, E. Carara and F.G. Moraes. Reducing NoC Energy Consumption Exploring Asynchronous End-to-end GALS Communication. 33rd Symposium on Integrated Circuits and Systems Design (SBCCI). 2020, p. 1–6. DOI: http://dx.doi.org/10.1109/SBCCI50935.2020.9189896.
30. Densing C.V.J. Asynchronous MOUSETRAP Implementation of AES-128 Encryption Using 65nm Standard Cells. IEEE Region Ten Symposium (Tensymp). Jul. 2018, p. 80–84. DOI: http://dx.doi.org/10.1109/TENCONSpring.2018.8691968.

31. Van Berkel, Burgess R., Kessels J., Roncken M., Schalij F. and Peeters A. Asynchronous circuits for low power: a DCC error corrector. IEEE Design Test of Computers, vol. 11, no. 2, p. 22–32, 1994. DOI: http://dx.doi.org/10.1109/54.282442.
32. Ikeda Asada M., Devlin B.S. and Sogabe T. Self-Synchrounous Circuits with Completion/Error Detection as a Candidate of Future LSI Resilient for PVT Variations and Aging. IEEE 25th International Symposium on Defect and Fault Tolerance in VLSI Systems. 2010, p. 3–3. DOI: http://dx.doi.org/10.1109/DFT.2010.61.
33. Plekhanov L.P., Zakharov V.N. Universal functional method for analyzing large self-timed circuits. Institute of Informatics Problems, Russian Academy of Sciences.2020, vol. 30, no. 2, p. 11-20. DOI: http://dx.doi.org/10.14357/08696527200202. EDN KDUWST.
34. Сурков А.В. Маршрут проектирования самосинхронных конвейерных схем с использованием возможностей сапр. А.В. Сурков, А.О. Власов. Программные продукты и системы. 2015, № 4, с. 110–115. EDN VIDBXD.
35. Каменских А.Н. Особенности обеспечения отказоустойчивости самосинхронных цифровых схем. А.Н. Каменских, С.Ф. Тюрин. Электротехника. 2014, № 11, с. 32–37. EDN STGYHZ.
36. Степченков Ю.А., Дьяченко Ю.Г., Рождественский Ю.В. и др. Повышение сбоеустойчивости индикации самосинхронных схем. Проблемы разработки перспективных микро- и наноэлектронных систем (МЭС). 2020, № 2, с. 66–72. DOI: http://dx.doi.org/10.31114/2078-7707-2020-2-66-72. EDN DQMAKC.
37. Данилов И.А., Шнайдер А.И., Балбеков А.О., Рогаткин Ю.Б. С-элементы на основе DICE-ячейки как элементы сбоеустойчивых самосинхронных схем. Вопросы атомной науки и техники. Серия: Физика радиационного воздействия на радиоэлектронную аппаратуру. 2015, № 3, с. 32–38. EDN UNETJJ.
38. Moreira B. Oliveira, F. Moraes and N. Calazans. Impact of C-elements in asynchronous circuits. In Thirteenth International Symposium on Quality Electronic Design (ISQED), Mar. 2012, p. 437–343. DOI: http://dx.doi.org/10.1109/ISQED.2012.6187530.
39. Danilov A., Gorbunov M.S., Shnaider A.I., Balbekov A.O., Rogatkin Y.B. and Bobkov S.G. On board electronic devices safety provided by DICE-based Muller C-elements. Acta Astronautica, vol. 150, p. 28–32, Sep. 2018. DOI: http://dx.doi.org/10.1016/j.actaastro.2018.01.019.
40. Yu Z.C., Furber S.B. and Plana L.A. An investigation into the security of self-timed circuits. In Ninth International Symposium on Asynchronous Circuits and Systems, Proceedings. 2003, p. 206–215. DOI: http://dx.doi.org/10.1109/ASYNC.2003.1199180.
41. Plana A., Riocreux P.A., Bainbridge W.J., Bardsley A., Garside J.D. and Temple S. SPA - a synthesisable Amulet core for smartcard applications. In Proceedings Eighth International Symposium on Asynchronous Circuits and Systems, Apr. 2002, p. 201–210. DOI: http://dx.doi.org/10.1109/ASYNC.2002.1000310.
42. Chong K.-S. et al. Side-Channel-Attack Resistant Dual-Rail Asynchronous-Logic AES Accelerator Based on Standard Library Cells. Asian Hardware Oriented Security and Trust Symposium (AsianHOST). 2019, p. 1–7. DOI: http://dx.doi.org/10.1109/AsianHOST47458.2019.9006690.
43. Xia Z., Hariyama M. and Kameyama M. Asynchronous Domino Logic Pipeline Design Based on Constructed Critical Data Path. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 23, no. 4, p. 619–630, Apr. 2015. DOI: http://dx.doi.org/10.1109/TVLSI.2014.2314685.
44. Li Y., Wu X. and Bai G. Implementation of SM4 Algorithm based on Asynchronous Dual-Rail Low-power Design.14th IEEE International Conference on Solid-State and Integrated Circuit Technology (ICSICT). 2018, p. 1–3. DOI: http://dx.doi.org/10.1109/ICSICT.2018.8564874.
45. Ho W.-G. et al. A DPA-Resistant Asynchronous-Logic NoC Router with Dual-Supply-Voltage-Scaling for Multicore Cryptographic Applications. IEEE International Symposium on Circuits and Systems (ISCAS). 2020, p. 1–5. DOI: http://dx.doi.org/10.1109/ISCAS45731.2020.9180849.

REFERENCES:

[1] Kocher P.C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. Advances in Cryptology — CRYPTO ’96, Berlin, Heidelberg. 1996, p. 104–113. DOI: https://doi.org/10.1007/3-540-68697-5_9.
[2] Mangard S., Oswald E. and Popp T. Power Analysis Attacks: Revealing the Secrets of Smart Cards, 1st ed. Springer Publishing Company, Incorporated, 2007. DOI: https://doi.org/10.1007/978-0-387-38162-6.
[3] Tromer E., Osvik D.A. and Shamir A. Efficient Cache Attacks on AES, and Countermeasures. J Cryptol, vol. 23, no. 1, p. 37–71, Jan. 2010. DOI: http://dx.doi.org/10.1007/s00145-009-9049-y.
[4] Pessl P., Gruss D., Maurice C., Schwarz M. and Mangard S. DRAMA: Exploiting DRAM Addressing for Cross-CPU Attacks. 2016. URL:https://www.researchgate.net/publication/285459017_DRAMA_Exploiting_DRAM_Addressing_for_Cross-CPU_Attacks (дата обращения: 18.05.2022).

[5] Mehrnezhad M., Toreini E., Shahandashti S.F. and Hao F. TouchSignatures: Identification of User Touch Actions and PINs Based on Mobile Sensor Data via JavaScript. Journal of Information Security and Applications, vol. 26, p. 23–38, Feb. 2016. DOI: http://dx.doi.org/10.1016/j.jisa.2015.11.007.
[6] Michalevsky Y., Nakibly G., Schulman A., Veerapandian G.A. and Boneh D. PowerSpy: Location Tracking using Mobile Device Power Analysis, arXiv, arXiv:1502.03182, Aug. 2015. DOI: http://dx.doi.org/10.48550/arXiv.1502.03182.
[7] Patel H. and Baldwin R.O. Random Forest profiling attack on advanced encryption standard. International Journal of Applied Cryptography, vol. 3, no. 2, p. 181–194, Jan. 2014. DOI: http://dx.doi.org/10.1504/IJACT.2014.062740.
[8] Zeng Z., Gu D., Liu J. and Guo Z. An Improved Side-Channel Attack Based on Support Vector Machine. Tenth International Conference on Computational Intelligence and Security. 2014, p. 676–680. DOI: http://dx.doi.org/10.1109/CIS.2014.80.
[9] Shaikh M., Arain Q.A. and Saddar S. Paradigm Shift of Machine Learning to Deep Learning in Side Channel Attacks - A Survey. 6th International Multi-Topic ICT Conference (IMTIC). 2021, p. 1–6. DOI: http://dx.doi.org/10.1109/IMTIC53841.2021.9719689.
[10] Biswas K., Ghosal D. and Nagaraja S. A Survey of Timing Channels and Countermeasures. ACM Comput. Surv., vol. 50, no. 1, p. 6:1–6:39, 2017. DOI: http://dx.doi.org/10.1145/3023872.
[11] Quisquater J.-J. and Samyde D. ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards. in Smart Card Programming and Security, Berlin, Heidelberg. 2001, p. 200–210.
[12] Moore S., Anderson R., Cunningham P., Mullins R. and Taylor G. Improving smart card security using self-timed circuits. In Proceedings Eighth International Symposium on Asynchronous Circuits and Systems, Apr. 2002, p. 211–218. DOI: http://dx.doi.org/10.1109/ASYNC.2002.1000311.
[13] Cilio W., Linder M., Porter C., Di J., Smith S. and Thompson D. Side-channel attack mitigation using dual-spacer Dual-rail Delay-insensitive Logic (D3L). In Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon), Mar. 2010, p. 471–474. DOI: http://dx.doi.org/10.1109/SECON.2010.5453826.
[14] Spreitzer R., Moonsamy V., Korak T. and Mangard S. Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. IEEE Communications Surveys Tutorials, vol. 20, no. 1, p. 465–488, 2018. DOI: http://dx.doi.org/10.1109/COMST.2017.2779824.
[15] Kaur S., Singh B. and Kaur H. Analytical Classifications of Side Channel Attacks, Glitch Attacks and Fault Injection Techniques: Their Countermeasures. In 2020 Indo – Taiwan 2nd International Conference on Computing, Analytics and Networks (Indo-Taiwan ICAN). 2020, p. 144–151. DOI: http://dx.doi.org/10.1109/Indo-TaiwanICAN48429.2020.9181324.
[16] Ferrag M.A., Maglaras L., Derhab A. and Janicke H. Authentication schemes for smart mobile devices: threat models, countermeasures, and open research issues. Telecommun Syst, vol. 73, no. 2, p. 317–348, Feb. 2020. DOI: http://dx.doi.org/10.1007/s11235-019-00612-5.
[17] Abu-Ghazaleh N., Ponomarev D. and Evtyushkin D. How the spectre and meltdown hacks really worked. IEEE Spectrum, vol. 56, no. 3, p. 42–49, Mar. 2019. DOI: http://dx.doi.org/10.1109/MSPEC.2019.8651934.
[18] Yan L., Guo Y., Chen X. and Mei H. A Study on Power Side Channels on Mobile Devices, arXiv, arXiv:1512.07972, Dec. 2015. DOI: http://dx.doi.org/10.48550/arXiv.1512.07972.
[19] Kocher P., Jaffe J. and B. Jun. Differential Power Analysis. In Advances in Cryptology — CRYPTO' 99, Berlin, Heidelberg. 1999, p. 388–397.
[20] Gebotys C.H., Ho S. and Tiu C.C. EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA. In Cryptographic Hardware and Embedded Systems – CHES 2005, Berlin, Heidelberg. 2005, p. 250–264. DOI: http://dx.doi.org/10.1007/11545262_19.
[21] O'Flynn C. Fault Injection using Crowbars on Embedded Systems. IACR Cryptol. ePrint Arch., p. 810, 2016.
[22] Hutter M. and Schmidt J.-M. The Temperature Side Channel and Heating Fault Attacks. In Smart Card Research and Advanced Applications, Cham. 2014, p. 219–235. DOI: http://dx.doi.org/10.1007/978-3-319-08302-5_15.
[23] Sparsø J. and Furber S. Principles of Asynchronous Circuit Design. Boston, MA: Springer US, 2001. DOI: http://dx.doi.org/10.1007/978-1-4757-3385-3.
[24] Liu M., Zhang Z., Wen J. and Jia Y. An Approximate Symmetry Clock Tree Design with Routing Topology Prediction. IEEE International Midwest Symposium on Circuits and Systems (MWSCAS). 2021, p. 92–96. DOI: http://dx.doi.org/10.1109/MWSCAS47672.2021.9531772.
[25] Veendrick H. J.M. Nanometer CMOS ICs: From Basics to ASICs. Cham: Springer International Publishing, 2017. DOI: http://dx.doi.org/10.1007/978-3-319-47597-4.
[26] Kebaili M., Brignone J. and Morin-Allory K. Clock domain crossing formal verification: a meta-model. IEEE International High Level Design Validation and Test Workshop (HLDVT). 2016, p. 136–141. DOI: http://dx.doi.org/10.1109/HLDVT.2016.7748267.

[27] Muller D.E. and Bartky W.C. A theory of asynchronous circuits. Annals of Computing Laboratory of Harvard University, no. 5, p. 204–243, 1959.
[28] Nowick S.M. and Singh M. High-performance asynchronous pipelines: An overview. IEEE Design and Test of Computers, vol. 28, no. 5, p. 8–22, 2011. DOI: http://dx.doi.org/10.1109/MDT.2011.71.
[29] Weber L. de Oliveira, E. Carara and F.G. Moraes. Reducing NoC Energy Consumption Exploring Asynchronous End-to-end GALS Communication. 33rd Symposium on Integrated Circuits and Systems Design (SBCCI). 2020, p. 1–6. DOI: http://dx.doi.org/10.1109/SBCCI50935.2020.9189896.
[30] Densing C.V.J. Asynchronous MOUSETRAP Implementation of AES-128 Encryption Using 65nm Standard Cells. IEEE Region Ten Symposium (Tensymp). Jul. 2018, p. 80–84. DOI: http://dx.doi.org/10.1109/TENCONSpring.2018.8691968.
[31] Van Berkel, Burgess R., Kessels J., Roncken M., Schalij F. and Peeters A. Asynchronous circuits for low power: a DCC error corrector. IEEE Design Test of Computers, vol. 11, no. 2, p. 22–32, 1994. DOI: http://dx.doi.org/10.1109/54.282442.
[32] Ikeda Asada M., Devlin B.S. and Sogabe T. Self-Synchrounous Circuits with Completion/Error Detection as a Candidate of Future LSI Resilient for PVT Variations and Aging. IEEE 25th International Symposium on Defect and Fault Tolerance in VLSI Systems. 2010, p. 3–3. DOI: http://dx.doi.org/10.1109/DFT.2010.61.
[33] Plekhanov L.P., Zakharov V.N. Universal functional method for analyzing large self-timed circuits. Institute of Informatics Problems, Russian Academy of Sciences. 2020, vol. 30, no. 2, p. 11-20. DOI: http://dx.doi.org/10.14357/08696527200202. EDN KDUWST.
[34] Surkov A.V., Vlasov A.O. Design route of self-synchronous conveyor circuits using CAD capabilities. Programmnye produkty i sistemy. 2015, vol. 4, p. 110–115. EDN VIDBXD (in Russian).
[35] Kamenskikh A.N., Tyurin S.F. Features that provide fault tolerance of self-synchronizing circuits. Elektrotehnika. 2014, no. 11, p. 32–37. EDN STGYHZ (in Russian).
[36] Stepchenkov Y.A., Diachenko Y.G., Rogdestvenski Y.V., Morozov N.V., Stepchenkov D.Y., Diachenko D.Y. Hardening Self-Timed Circuit Indication against Soft Errors. Problemy razrabotki perspektivnyh mikro- i nanojelektronnyh sistem (MES). 2020, no. 2, p. 66–72. DOI: http://dx.doi.org/10.31114/2078-7707-2020-2-66-72. EDN DQMAKC (in Russian).
[37] Danilov I.A., Shnaider A.I., Balbekov A.O., Rogatkin Yu.B. C-elements based on DICE cell as elements of failure tolerance self-timed circuits. Voprosy atomnoj nauki i tehniki. Serija: Fizika radiacionnogo vozdejstvija na radiojelektronnuju apparaturu. 2015, no. 3, p. 32–38. EDN UNETJJ (in Russian).
[38] Moreira B. Oliveira, F. Moraes and N. Calazans. Impact of C-elements in asynchronous circuits. In Thirteenth International Symposium on Quality Electronic Design (ISQED), Mar. 2012, p. 437–343. DOI: http://dx.doi.org/10.1109/ISQED.2012.6187530.
[39] Danilov A., Gorbunov M.S., Shnaider A.I., Balbekov A.O., Rogatkin Y.B. and Bobkov S.G. On board electronic devices safety provided by DICE-based Muller C-elements. Acta Astronautica, vol. 150, p. 28–32, Sep. 2018. DOI: http://dx.doi.org/10.1016/j.actaastro.2018.01.019.
[40] Yu Z.C., Furber S.B. and Plana L.A. An investigation into the security of self-timed circuits. In Ninth International Symposium on Asynchronous Circuits and Systems, Proceedings. 2003, p. 206–215. DOI: http://dx.doi.org/10.1109/ASYNC.2003.1199180.
[41] Plana A., Riocreux P.A., Bainbridge W.J., Bardsley A., Garside J.D. and Temple S. SPA - a synthesisable Amulet core for smartcard applications. In Proceedings Eighth International Symposium on Asynchronous Circuits and Systems, Apr. 2002, p. 201–210. DOI: http://dx.doi.org/10.1109/ASYNC.2002.1000310.
[42] Chong K.-S. et al. Side-Channel-Attack Resistant Dual-Rail Asynchronous-Logic AES Accelerator Based on Standard Library Cells. Asian Hardware Oriented Security and Trust Symposium (AsianHOST). 2019, p. 1–7. DOI: http://dx.doi.org/10.1109/AsianHOST47458.2019.9006690.
[43] Xia Z., Hariyama M. and Kameyama M. Asynchronous Domino Logic Pipeline Design Based on Constructed Critical Data Path. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 23, no. 4, p. 619–630, Apr. 2015. DOI: http://dx.doi.org/10.1109/TVLSI.2014.2314685.
[44] Li Y., Wu X. and Bai G. Implementation of SM4 Algorithm based on Asynchronous Dual-Rail Low-power Design.14th IEEE International Conference on Solid-State and Integrated Circuit Technology (ICSICT). 2018, p. 1–3. DOI: http://dx.doi.org/10.1109/ICSICT.2018.8564874.
[45] Ho W.-G. et al. A DPA-Resistant Asynchronous-Logic NoC Router with Dual-Supply-Voltage-Scaling for Multicore Cryptographic Applications. IEEE International Symposium on Circuits and Systems (ISCAS). 2020, p. 1–5. DOI: http://dx.doi.org/10.1109/ISCAS45731.2020.9180849.

Поступила в редакцию – 17 мая 2022 г. Окончательный вариант – 02 июня 2022 г.
Received – May 17, 2022. The final version – June 02, 2022.