УДК 519.2

Адаптивная система трансформации информационных потоков в скоростных каналах связи

Представлены принципы построения адаптивной системы трансформации информационных потоков в высокоскоростных каналах связи. Даны рекомендации по устранению уязвимостей ПЛИС, реализующих адаптивные системы трансформации.

**С. Н. Коянкин, А. П. Мартынов,
Д. Б. Николаев, В. Н. Темненко**

Развитие глобальных информационных сетей позволяет передавать значительные объемы данных на большие расстояния с использованием высокоскоростных каналов связи. При этом задача обеспечения надежной и безопасной передачи данных встает особенно остро. Поскольку основным методом защиты информационных ресурсов с доказуемой степенью защищенности остается криптографическое преобразование данных, то трансформация исходных открытых данных в не имеющую смысла последовательность предполагает наличие некого программного, аппаратного или программно-аппаратного устройства, а зачастую и системы устройств, внедряемой в высокоскоростной канал связи и выполненной в виде «прозрачной», с точки зрения сети, системы. По этой причине к системе трансформации предъявляются требования о конфигурации системы «на лету» при ее включении «в разрыв» соединения защищаемой локальной сети с внешним каналом связи. Исследования различных вариантов построения вычислительных модулей-преобразователей [1] показали, что наиболее оптимальными характеристиками быстродействия обладают аппаратно-реализованные системы. Таким образом, исследование принципов построения адаптивной системы трансформации информационных потоков в скоростных каналах связи является актуальным на сегодняшний день направлением, призванным обеспечить информационную безопасность национальной нанотехнологической сети.

Выбор платформы реализации адаптивной системы трансформации информационных потоков (АСТИП) зависит от многих критических факторов, таких как сложность алгоритма трансформации (преобразования), область его применения, стоимость, скорость, энергопотребление, требуемые аспекты безопасности (безопасность на физическом уровне, побочные каналы утечки и т. д.). Перспективной платформой для решения поставленной задачи являются программируемые логические интегральные схемы (ПЛИС), как правило более предпочтительные, чем специализированные интегральные схемы (СБИС). Немаловажную роль в этом выборе играют такие критерии, как перепрограммируемость, мощность и цена. Внутренние свойства ПЛИС (параллельные операции и выполнение индивидуальных функций) делают их производительность конкурентоспособной с текущими микропроцессорами и микроконтроллерами. Согласно А. Волингеру (Wollinger) и др., А. Волингеру и Г. Пару (Wollinger и Parr) [2] потенциальные преимущества

ПЛИС в криптографических приложениях это быстрое изменение алгоритма, обновление алгоритма, эффективность архитектуры, эффективность использования ресурсов, модификация алгоритма и производительность.

Возможность реализации АСТИП на ПЛИС необходимо рассмотреть с точки зрения уязвимости получаемой системы к внешним угрозам.

Мотивацией любой нападающей стороны, которую принято считать злоумышленником, является стремление разрушить функциональность системы. Возможности взломщика детально разобраны в [2] и объединены по классам:

– класс I – злоумышленники, не имеющие достаточного знания о конкретной системе, но обладающие сведениями в области несанкционированного воздействия на технические системы;

– класс II (осведомленные сотрудники) – злоумышленники, имеющие опыт и специализированное техническое образование и эксперты со сложным оборудованием для анализа частей систем;

– класс III (финансируемые организации) – злоумышленники, являющиеся командой специалистов, способных к разработке и использованию сложного и дорогостоящего аналитического оборудования, без ограничения в ресурсах, с возможностью глубокого анализа систем.

Цель использования злоумышленником аппаратных средств – получение секретной информации и приведение системы в неработоспособное состояние. Для реализации своих целей злоумышленником используются атаки, которые классифицируются по объему аппаратных и программных инструментов, требуемых для их реализации, а также по возможности предотвращения этих атак.

Атака методом «черного ящика»

В этой атаке злоумышленник подает на входы все возможные комбинации для получения соответствующих выходных комбинаций. После формирования необходимого (требуемого) количества различных комбинаций входной и выходной информации может быть подобран искомый алгоритм преобразования. Для реализации этой атаки требуется большая мощность вычислений. Для ПЛИС эта атака будет в меньшей степени осуществима, поскольку ПЛИС обладает большим количеством логических элементов и сложностью взаимосвязей между ними. Стоимость атаки возрастает, если в схеме использованы конечные автоматы, регистры сдвига с обратными связями, а в качестве средств обмена могут быть применены двунаправленные каналы ввода-вывода данных. Следует отметить, что прогресс математических методов, таких как SAT Solvers, может помочь злоумышленнику в запуске атаки «черного ящика».

Атака считыванием записанной информации определенного вида

Цель этой атаки – определить конфигурацию ПЛИС посредством специализированного аппаратного интерфейса на базе стандарта IEEE 1149.1 или программируемого интерфейса для получения секретной информации (ключи преобразования, алгоритм). Для дешифрования защищенной информации может быть использована считанная из ПЛИС конфигурация и структура данных, чтобы избежать этого, необходимо при формировании структуры ПЛИС использовать древовидные алгоритмы с функцией самопроверки. Современное оборудование для отладки, такое как Xilinx JBits, может применяться для реализации атаки методом считывания записанной информации определенного вида. Следует отметить, что эта атака будет затруднена при использовании порта программирования в качестве элемента защиты, тогда после обнаружения вмешательства вся конфигурация ПЛИС будет удалена или она будет выведена из строя.

Клонирование ПЛИС

В этой атаке целью злоумышленника является конфигурационный файл системы. Как показано на рис. 1, битовый поток из флэш-памяти сохраняется в реализованной на ПЛИС статической памяти с произвольным доступом. Этот процесс требует организации передачи данных в виде битового потока из флэш-памяти в ПЛИС при отключении питания.

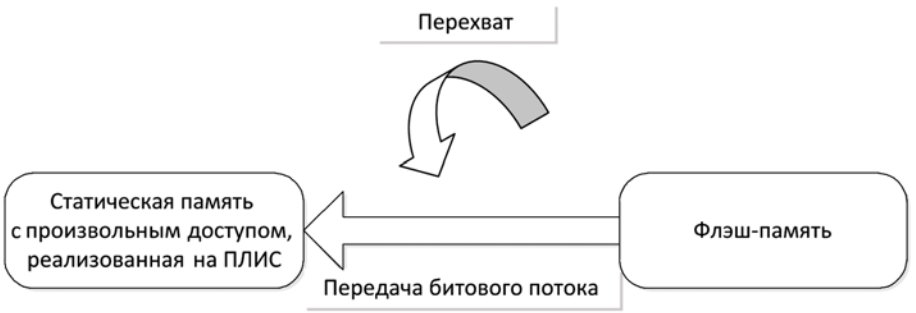

Рис. 1. Конфигурация реализованной на ПЛИС статической памяти с произвольным доступом

Этот битовый поток может быть перехвачен третьим лицом во время передачи для создания его клона. Для выполнения этой атаки требуется расширенный программатор памяти, логический анализатор и регистраторы данных. Использование динамической памяти, реализованной на ПЛИС, поможет устранить данную атаку. Следует отметить, что использование такой флэш-памяти создает ограничения для реализации существующих алгоритмов преобразования данных. Вместе с тем шифрование конфигурационного файла является наиболее эффективной и реальной ответной мерой против клонирования реализованной на ПЛИС статической памяти с произвольным доступом.

Физическое нападение

Целью атаки является исследование ПЛИС для получения информации о структуре его внутреннего пространства. Эта атака может быть выполнена визуальным контролем внешних признаков ПЛИС с использованием такого оборудования, как оптические микроскопы, механические зонды, сфокусированные ионные лучи, электронно-лучевые тестеры. Для предотвращения этой атаки конструкция ПЛИС должна содержать специальные элементы экранирования и использовать технологии, защищающие от сканирования.

Атака по сторонним каналам (анализ потребляемой мощности, исследование характера изменения основных параметров во времени, электромагнитное излучение)

Любая физическая реализация технической системы может предусматривать атаку по сторонним каналам, что допускает утечку информации, которая может быть использована злоумыш-

ленником. Путем простого анализа потребляемой мощности, дифференциальным анализом мощности, простым электромагнитным анализом (ПЭМА), дифференциальным электромагнитным анализом (ДЭМА) стороннего канала может быть получена информация, которая будет использована в интересах злоумышленника (рис. 2).

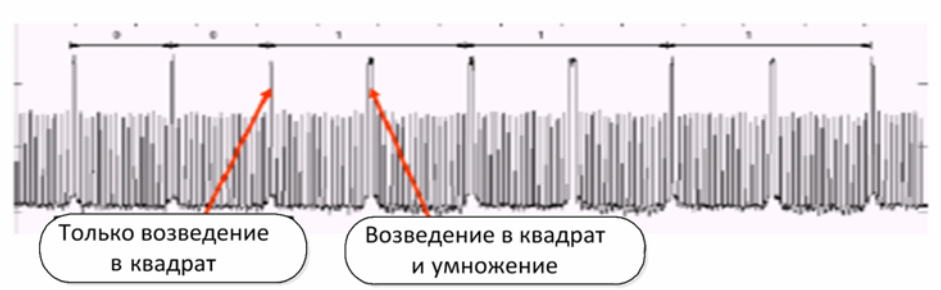

Рис. 2. Анализ потребляемой мощности при реализации алгоритма RSA

Алгоритм RSA реализован в основном с использованием функций возведения в квадрат и перемножения. Как описано в литературе [2], в КМОП вентилях во время переключения происходит выброс тока, что регистрируется с использованием высокочувствительных контрольно-измерительных щупов и высокопроизводительных осциллографов, и позволяет анализировать потребляемую мощность. Меры предотвращения анализа потребляемой мощности по сторонним каналам для рассматриваемой RSA системы для генерации ключа могут быть приняты либо на уровне проектировщика, либо на уровне производителя.

Реинжиниринг битовых потоков

Цель этой атаки – получить алгоритм применяемой криптосистемы или секретные ключи реинжинирингом битового потока двоичных данных. Как показано на рис. 3, типичный технический процесс разработки ПЛИС состоит из различных этапов.

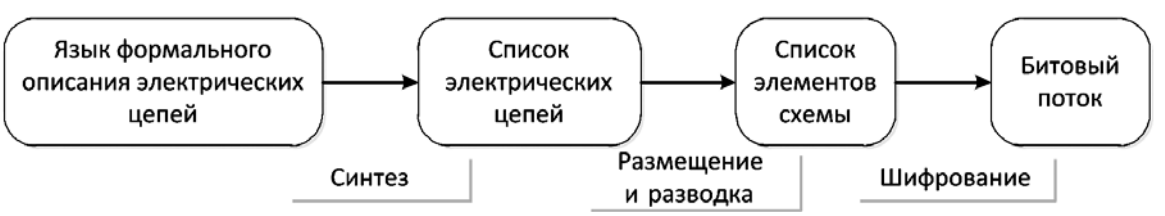

Рис. 3. Алгоритм формирования программного обеспечения для реализации ПЛИС

Злоумышленник может проанализировать коды битового потока, особенно цифровой логики, извлеченные из файла двоичного потока. Современное оборудование для реинжиниринга битового потока, такое как Debit, дает информацию о таблице преобразования. Сокрытие ключевой информации, используемой для преобразования кодов формального описания и таблиц преобразований, может частично предотвратить эту атаку.

Злонамеренное изменение аппаратных и программных настроек в оборудовании

В этой атаке злоумышленник предпринимает действия по изменению конфигурации оборудования с целью получения недекларированных возможностей, позволяющих, например, получить в открытом виде закрытую информацию или осуществить неавторизированный доступ. Оборудование для проверки соответствия топологии электрической схеме (LVS) может быть использовано для определения вмешательства в настройки, как показано на рис. 4, при этом умышленное изменение аппаратных и программных настроек может быть обнаружено сравнением реализованного и первоначального проектов.

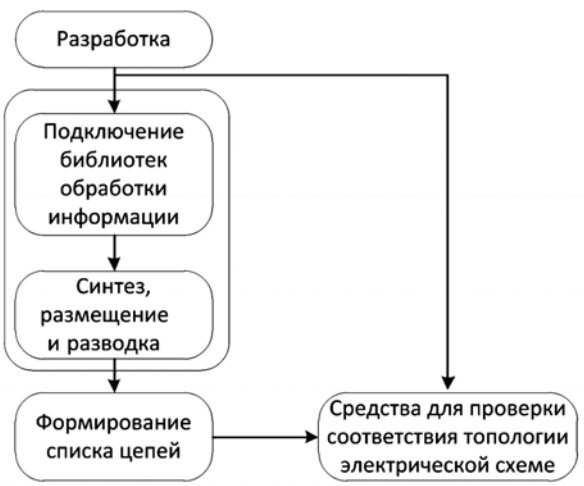

Рис. 4. Проверка достоверности разработки

Атака на ошибки в программно-аппаратной реализации

Атака на ошибки в программно-аппаратной реализации может быть применена там, где аппаратные ошибки (неожиданное условие или дефект) приводят к технологической ошибке, которая может быть полезна для злоумышленника. Для реализации этой атаки необходимы современное оборудование для сравнения временных параметров, логический анализатор и подобные устройства. Однако атака будет менее реализуема при устранении источников шума, некачественного напряжения, чрезмерной температуры, радиационных или высокоэнергетических пучков, таких как ультрафиолет, лазер и т. д.

Атака по косвенным признакам функционирования аппаратных средств

Злоумышленник может использовать аппаратное обеспечение системы, чтобы получить секретную информацию о криптосистеме. Злоумышленник может использовать порты, такие как специализированный аппаратный интерфейс на базе стандарта IEEE 1149.1 и резервное оборудо-

вание, присутствующее в технической системе. Для этой атаки необходимы системы отладки, такие как Quartus, ISE, Visual DSP++, эмуляторы, считыватели памяти и другие подобные устройства. При проектировании устройства могут быть заложены функциональные возможности, предотвращающие эту атаку путем контроля параметров устройства.

Атака с использованием троянских программно-аппаратных воздействий

Троянский вирус – это намеренный вредоносный код, записанный в системный проект, или вредоносная модификация аппаратной схемы, как правило, в пользу злоумышленника. Для реализации троянского вируса необходимы доступ к криптосистеме и знание используемого программного обеспечения. Х. Ванг [2] и другие классифицировали троянский вирус по различным категориям, которые приведены на рис. 5.

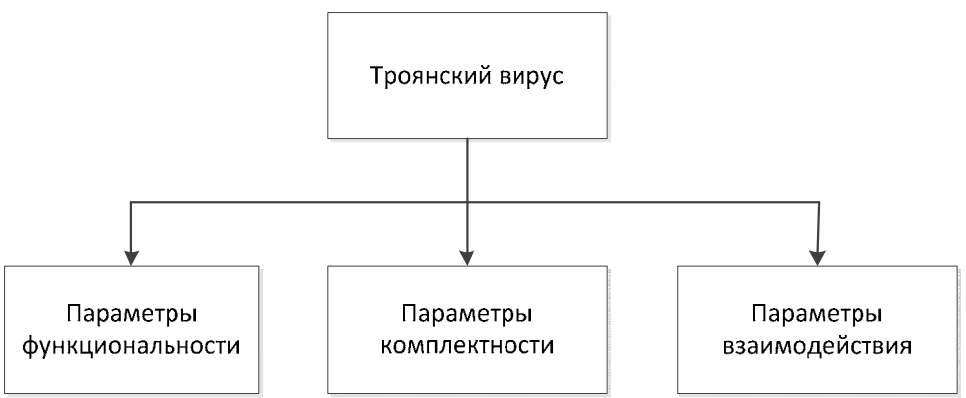

Рис. 5. Классификация областей воздействия троянского вируса

Активация троянского вируса может быть осуществлена как извне, так и изнутри системы. При выполнении статистического анализа активация троянского вируса считается очень редким событием. Кроме того, воздействие троянского вируса направлено на модификацию следующих элементов системы: функциональности, комплектности и взаимосвязи через какое-либо средство, которое может быть проводным или беспроводным.

Кроме того, рассматривая различные технологические разработки в области ПЛИС, можно задать различные уровни сложности, с которыми злоумышленник может столкнуться при осуществлении внешнего воздействия (в таблице приведены основные виды аппаратных атак с определенными уровнями сложности). Коэффициенты уровня сложности для ряда атак получены эмпирическим путем, однако для большинства атак эти коэффициенты заданы на основе теоретических расчетов, поскольку эксперименты невозможны из-за отсутствия вычислительных и временных ресурсов. Кроме того, список классификации уровней сложности может изменяться в зависимости от категории злоумышленника, который собирается выполнить атаку.

Атаки на защищенное аппаратное оборудование

Внешние воздействия на ПЛИС	Уровень сложности для атакующего
Атака на «черный ящик»	5
Атака считыванием только что записанной информации	2
Клонирование ПЛИС	
a. Внутренние ПЗУ/ППЗУ ПЛИС	5
b. ППЗУ ПЛИС	4
c. ПЗУ ПЛИС	4
d. ОЗУ ПЛИС с восстановлением битовых последовательностей	3
e. ОЗУ ПЛИС	1
Реинжиниринг битовых потоков	4
Физическая атака	5
Атака по побочным каналам	4
Несанкционированное изменение аппаратных и программных настроек в оборудовании	3
Атака на ошибки в программно-аппаратной реализации	4
Атака по косвенным признакам функционирования аппаратных средств	5
Атака с использованием троянских программно-аппаратных воздействий	1

Примечание. Выделяют уровни сложности от 1–5, где 5 – максимальной уровень сложности для осуществления атаки.

На основании анализа внешних воздействий и классификации злоумышленников предложен ряд основных подходов, которые учитывались при разработке АСТИП на ПЛИС:

1. Чтобы избежать реинжиниринга и клонирования ПЛИС, в ППЗУ следует хранить только зашифрованный двоичный файл, а также необходимо обеспечивать функциональную возможность восстановления битового потока на кристалле. На сегодняшний день поставщики обеспечивают эту функциональность реализацией криптоалгоритмов с функцией преобразования битового потока [3].

2. Криптографические операции в криптосистеме являются итеративными, что приводит к долговременному хранению результата в ячейках памяти СОЗУ. Разработчику следует добавлять пустые циклы во время криптографических операций.

3. Чтобы избежать искажения в первоначальном варианте проекта ПЛИС средствами проектирования, последний реализованный проект и первоначальный проект должны быть проверены на равенство. Это неотъемлемая часть этапа цикла разработки программного обеспечения.

4. Только ПЛИС, которые имеют уровень безопасности 3 или выше, как показано в таблице, должны использоваться для противодействия реинжинирингу битового потока. Также разработчику следует включить функциональную операцию, такую как удаление битового потока, когда характерный бит является обнаруженным.

5. В случае физической компрометации системы разработчику следует предумотреть функциональную возможность саморазрушения системы. К примеру, при определении неавторизированного вмешательства проект системы должен произвести стирание алгоритма и закрытой ключевой информации из системы.

6. Разработчикам следует уделять должное внимание формированию всех неиспользуемых входных/выходных выводов/портов как выводов с тремя состояниями, чтобы можно было исключить неавторизированный доступ.

7. Проект ПЛИС должен быть таким, чтобы исключить использование пользователем встроенных ключей.

8. Проект следует снабдить программными контрмерами для всех побочных каналов утечки. К примеру, проект должен маскировать секретные ключи по случайным значениям.

9. Разработчику следует использовать подготовленные данные для инициализации алгоритма.

10. Устойчивость криптоалгоритма должна быть высокой в системах, основанных на ПЛИС, для исключения атаки «черного ящика».

11. Разработчику следует использовать специализированные ПЛИС устройства для криптографических приложений, чтобы минимизировать количество аппаратных средств, входящих в систему.

12. Физическое/логическое разделение должно быть встроенным для открытых и закрытых данных на проектном уровне.

Предложенные подходы позволили на базе ПЛИС разработать АСТИП для высокоскоростных каналов, позволяющую:

• адаптировать программно-аппаратные средства АСТИП к высокоскоростным каналам связи;

• использовать модифицируемый набор алгоритмов криптографического преобразования;

• трансформировать информационные потоки в режиме реального времени со скоростями 1–10 Гбит/с;

• применять средства имитозащиты с возможностью использования асимметричной криптографии;

• обеспечивать распределение параметров системы без формирования специальных каналов и специализированных предустановок;

• уничтожить всю конфиденциальную информацию при несанкционированном вскрытии модулей системы.

АСТИП реализует такие преимуществам ПЛИС-архитектуры, как быстрое изменение алгоритма, обновление алгоритма, эффективность архитектуры, эффективность использования ресурсов, модификация алгоритма и производительность.

Список литературы

1. Грибунин В. Г., Мартынов А. П., Николаев Д. Б., Фомченко В. Н. Криптография и безопасность цифровых систем: учебн. пособие / Под ред. А. И. Астайкина. – Саров: РФЯЦ-ВНИИЭФ, 2011.

2. Кузьмин И. В., Кедрус В. А. Основы теории информации и кодирования. – Киев: Вища шк., 1986.

3. Мартынов А. П., Николаев Д. Б., Фомченко В. Н., Похлебаев М. И. Анализ вариантов построения многофункциональной структуры потокового преобразования для высокоскоростных каналов связи // Сб. докл. XIX Международ. науч.-техн. конф. «Информационные системы и технологии» ИСТ-2013. – Нижний Новгород: ННГТУ. 2013.

Adaptive transformation system of information streams in high-speed communication channels

S. N. Koyankin, A. P. Martynov, D. B. Nikolaev, V. N. Temnenko

Construction principles of adaptive transformation system of information streams in high-speed communication channels are carried out. Recommendations on elimination vulnerability FPGA, realizing adaptive systems of transformation are given.