- в некоторых случаях – дополнительную информацию о местонахождении ошибки, а также возможную причину ее возникновения.

Применение описанного алгоритма позволяет сократить время регрессионного тестирования без потери качества тестирования. Практическая ценность работы состоит в том, что использование предлагаемого алгоритма позволяет получить новый инструмент, который может быть применен для тестирования программных продуктов различного уровня сложности и в различных предметных областях.

1. *Дідковська М.В., Тимошенко Ю.О.* Тестування: Основні визначення, аксіоми та принципи, 2010, 58 с. [Электронный ресурс]. – Режим доступа: CD-ROM.
2. *Котляров В.П.* Основы тестирования программного обеспечения / *Котляров В.П., Коликова Т.В.* – М.: БИНОМ, 2006. – 286 с.
3. *Boehm B.* Software Engineering Economic – N.J. Prentice-Hall, Inc, 1981. – 767 pp.
4. *Майерс Г.* Искусство тестирования программ / Майерс. Г., пер с англ. под ред. Б.А. Позина – М.: Финансы и статистика, 1982. – 172 с.

Поступила 3.03.2011р.

УДК 004.056.55:004.272.23:004.274

С.Я. Гильгурт, канд.техн.наук, ИПМЭ им. Г.Е.Пухова НАНУ, г. Киев
А.К. Гиранова, ИПМЭ им. Г.Е.Пухова НАНУ, г. Киев

РЕКОНФИГУРИРУЕМЫЙ ПРОЦЕССОР, РЕАЛИЗУЮЩИЙ УСИЛЕННЫЕ АЛГОРИТМЫ ЗАКРЫТИЯ ИНФОРМАЦИИ

*Аннотация***.** В статье предложена обобщенная структура реконфигурируемого процессора, реализующего усиленные алгоритмы блочного симметричного шифрования. Разработаны структурные схемы для различных методов усиления.

Библиогр.**:** 6 наим.

Ключевые слова: закрытие информации, блочное симметричное шифрование, реконфигурируемый вычислитель.

Стремительный рост производительности вычислительной техники помимо положительных сторон приводит в качестве побочного эффекта к ослаблению защиты информации, в частности, к снижению стойкости криптографических средств. Алгоритмы шифрования, которые еще несколько лет назад считались безопасными, в настоящее время уже не являются таковыми [1]. С другой стороны, создание совершенно новых алгоритмов закрытия информации представляется весьма непростой задачей. Этим обусловлена актуальность направления, связанного с развитием

методов усиления криптографической защиты, основанных на использовании известных, проверенных временем алгоритмов.

Вопрос вскрытия зашифрованной информации злоумышленником сводится, в конечном итоге, к наличию у него двух видов ресурсов – вычислительных и временных. Из чего следует два направления, позволяющих усилить существующие методы криптозащиты: комбинирование (повторное применение) криптографических алгоритмов; динамическая модификация (смена алгоритма во времени) [2].

Очевидно, что практическая реализация данных подходов приводит к усложнению и повышению ресурсоемкости создаваемых технических средств закрытия информации. В этой связи вызывает интерес такой класс цифровых устройств, как реконфигурируемые унифицированные вычислители (РУВ) на базе микросхем программируемой логики типа FPGA (Field Programmable Gate Array) [3]. В настоящее время РУВ наряду с унифицированными вычислителями (УВ) других типов [4] начинают активного использоваться для решения различных задач, в том числе, в области информационной безопасности.

В настоящей работе на основе анализа методов усиления криптозащиты, проведенного в работе [2], предлагается обобщенная вычислительная структура, реализующая ряд усиленных алгоритмов блочного симметричного шифрования (БСШ) [5] на базе программируемой логики, учитывающая специфические особенности применения РУВ.

Анализ последних достижений и публикаций показал, что в литературе встречаются отдельные работы по реализации на ПЛИС некоторых алгоритмов усиления криптозащиты. В то же время, отсутствует информация о более полных и систематизированных исследованиях по данной проблеме.

Целью настоящей статьи является разработка и исследование обобщенных структур реконфигурируемых процессоров, реализующих все методы усиления алгоритмов блочного симметричного шифрования, рассмотренных в работе [2].

В работе [6] на основе выявленного сходства большинства БСШ предложена обобщенная структура реконфигурируемого процессора блочного симметричного шифрования (РП-БСШ), ориентированная на использование реконфигурируемых вычислителей. Помимо устройств управления и ввода-вывода в данную структуру входит операционный блок, в котором реализуются различные алгоритмы БСШ.

Достоинством схемы является то, что, независимо от конкретного алгоритма, основные компоненты операционного блока остаются неизменными, заранее разработанными, отлаженными и проверенными. Изменяется лишь небольшой модуль, названный ядром алгоритма (ЯА), который описывает для каждого конкретного случая порядок преобразования данных внутри раунда.

В терминах цифровой техники ЯА представляет собой комбинационную схему, не содержащую триггеров, регистров и других элементов памяти.

Следовательно, при его синтезе разработчику не приходится решать вопросы тактирования, синхронизации, временного планирования и т.п., что существенно облегчает задачу. Именно данное свойство предложенной обобщенной структуры РП-БСШ позволяет создать на ее основе методику разработки широкого класса решений в области создания процессоров защиты данных, ориентированную на пользователей, не являющихся специалистами в области создания аппаратных цифровых устройств. Другими словами, методика позволяет существенно снизить требования к разработчикам и ускорить процесс создания реконфигурируемых решений на базе РУВ для различных прикладных областей, в частности, при разработке криптографических средств информационной защиты.

В настоящей работе данная идея получила дальнейшее развитие и расширена применительно к реализации методов усиления криптографических алгоритмов, рассмотренных в работе [2].

Суть комбинированного метода усиления защиты информации заключается в том, что исходный текст зашифровывается несколько раз. Другими словами, выполняется несколько последовательных шагов, на каждом из которых осуществляется процедура криптографического преобразования. При этом результаты предыдущего шага являются входными данными для последующего шага.

Одним из вариантов комбинирования является многократное шифрование. В этом случае на каждом шаге используется один и тот же алгоритм с различными ключами. Для произвольного числа шагов n такую процедуру можно описать следующим образом:

$$C = E_{kn}\left(\ldots\left(E_{ki}\left(\ldots\left(E_{k1}\left(M\right)\right)\right)\right)\right),$$

где M – исходный текст;

C – зашифрованный текст;

E_{ki} – операция зашифрования по ключу ki;

ki – i-й ключ.

Расшифрование является обратным процессом:

$$M = D_{kn}\left(\ldots\left(D_{ki}\left(\ldots\left(D_{k1}\left(C\right)\right)\right)\right)\right),$$

где D_{ki} – операция расшифрования по ключу ki.

В целях повышения стойкости многократного шифрования к вскрытию методом «встреча посередине» целесообразно использовать чередование операций зашифрования и расшифрования. В этом случае на тех шагах, где в процедуре прямого преобразования выполняется зашифрование, в процедуре обратного преобразования выполняется расшифрование, и наоборот.

Структурные схемы реконфигурируемых процессоров, реализующих усиленные алгоритмы блочного симметричного шифрования (РПУ-БСШ) на

верхнем уровне иерархии имеют одинаковый состав модулей: устройство управления, устройство ввода-вывода и операционный блок (рис. 1).

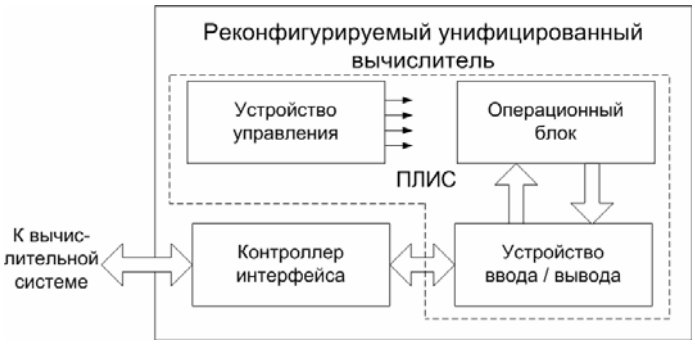

Рис. 1. Обобщенная структурная схема РПУ-БСШ

Функции устройств управления и ввода-вывода остаются такими же, что и для упомянутого выше криптопроцессора РП-БСШ.

Структура операционного блока для случая многократного шифрования приведена на рис. 2. Схема включает в себя входной и выходной регистры данных, память ключей, память режимов, счетчик шагов, а также модуль алгоритма, аналогичный по своей структуре операционному блоку, описанному в работе [6].

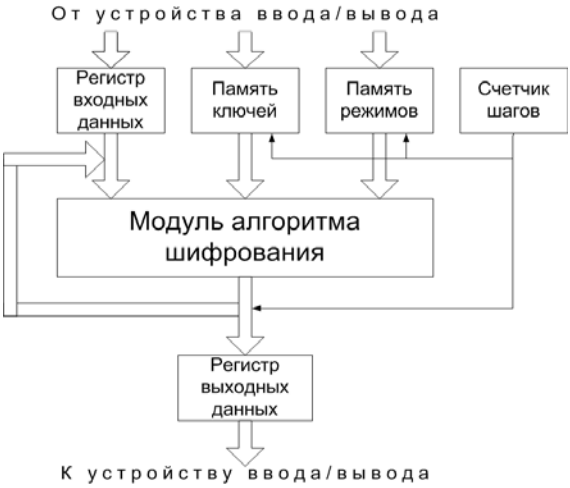

Рис. 2. Структурная схема операционного блока
для случая многократного шифрования

Входной и выходной регистры предназначены для хранения блоков исходного текста и текста, зашифрованного усиленным алгоритмом, соответственно. Для разных алгоритмов БСШ длина блока различна.

В памяти ключей хранится ключевая информация для каждого шага. В простейшем случае допустимо использование всего двух ключей, применяемых на различных шагах поочередно.

Память режимов содержит специфическую информацию, необходимую для выполнения выбранного алгоритма шифрования. В простейшем случае это могут быть биты, указывающие режим использования алгоритма для текущего шага: зашифрование либо расшифрование.

Счетчик шагов содержит номер текущего шага, управляет выборкой нужного ключа и режима, а также перенаправляет выдачу информации на выходной регистр после завершения процедуры шифрования.

Более высокую степень усиления по сравнению с многократным подходом обеспечивает следующий метод комбинирования – каскадное шифрование. При данном подходе на каждом шаге используются различные алгоритмы шифрования с различными ключами:

$$C = E_{kn}^{n}\left(\ldots\left(E_{ki}^{i}\left(\ldots\left(E_{k1}^{1}(M)\right)\right)\right)\right), \quad M = D_{k1}^{1}\left(\ldots\left(D_{ki}^{i}\left(\ldots\left(D_{kn}^{n}(C)\right)\right)\right)\right),$$

где E_{ki}^{i} – операция зашифрования i-м алгоритмом по ключу ki;

D_{ki}^{i} – операция расшифрования i-м алгоритмом по ключу ki.

Операционный блок для каскадного шифрования (рис. 3) отличается от рассмотренной выше схемы наличием нескольких модулей, реализующих различные алгоритмы БСШ.

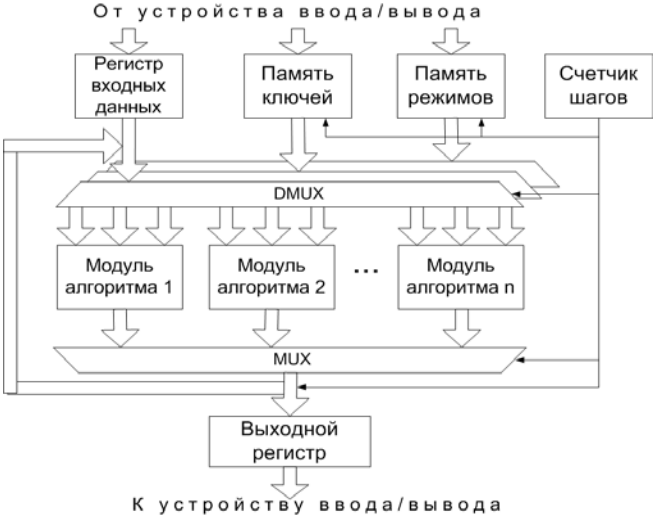

Рис. 3. Структурная схема операционного блока для случая каскадного шифрования

Счетчик шагов в данном случае помимо функций, описанных для предыдущей схемы, управляет также процедурой мультиплексирования, обеспечивающей подачу на вход требуемого алгоритма исходных данных и выдачу с него результатов на каждом шаге преобразования.

Второе направление усиления криптографических методов закрытия информации ориентировано на сокращение временного ресурса, имеющегося в распоряжении злоумышленника. Называется оно динамической модификацией и подразумевает смену алгоритма шифрования во времени. Чем чаще производится смена алгоритма, тем меньше времени остается злоумышленнику для вскрытия закрытой информации в реальном масштабе времени. Вопросы синхронизации процессов зашифрования у отправителя и расшифрования у получателя, возникающие при реализации данного подхода, также рассмотрены в упоминавшейся выше работе [2].

Операционный блок для динамической модификации различными алгоритмами (рис. 4) включает в себя, подобно предыдущей схеме, несколько модулей, реализующих различные алгоритмы БСШ. Отличие состоит в отсутствии канала обратной связи, а также в том, что место счетчика шагов теперь занимает блок смены алгоритма.

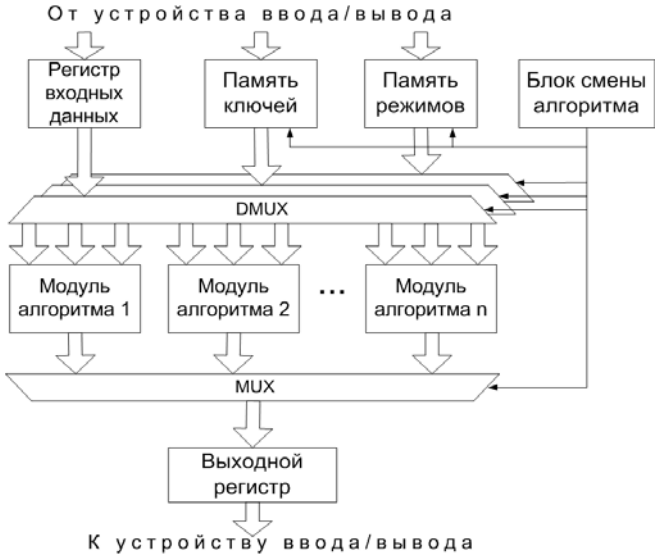

Рис. 4. Структурная схема операционного блока
для случая динамической модификации различными алгоритмами

Известным недостатком динамического подхода является потребность в большом количестве алгоритмов шифрования. Причем, чем большее число различных алгоритмов имеется в распоряжении криптосистемы, тем чаще

может производиться смена алгоритма, и тем выше эффект от использования данного метода усиления. В качестве решения данного противоречия можно использовать некоторые разновидности одного и того же алгоритма шифрования. Такой подход называется динамической модификацией разновидностями. Более подробно он рассмотрен в вышеупомянутой работе [2].

Операционный блок для динамической модификации разновидностями (рис. 5) отличается от предыдущей схемы наличием единственного модуля алгоритма и отсутствием соответствующих схем мультиплексирования. Блок смены алгоритма в данном случае управляет подачей на вход модуля алгоритма некоей параметрической информации, специфическим образом влияющей на алгоритм шифрования.

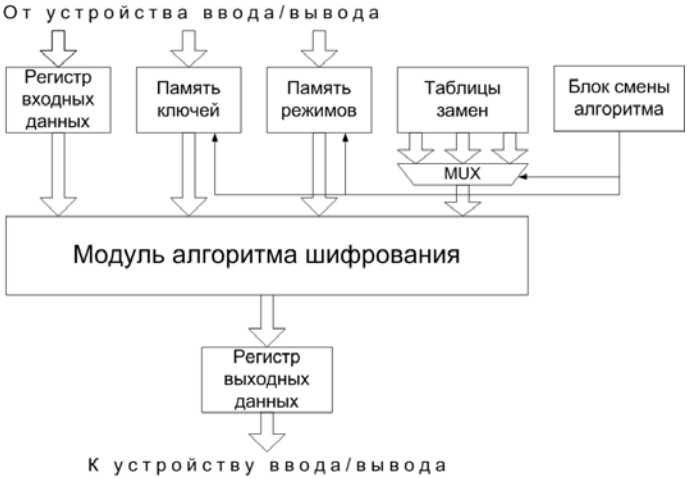

Рис. 5. Структурная схема операционного блока
для случая динамической модификации разновидностями

Рассмотренные выше два подхода – комбинирование и динамическая модификация сами по себе обеспечивают существенное улучшение показателей надежности закрытия информации, однако, наибольший эффект позволяет достичь гибридный подход – так называемое динамическое комбинирование.

Известны три способа такого совмещения подходов: динамическое многократное усиление, динамическое каскадное усиление и динамическое каскадное усиление разновидностями [2]. Схемы реализации операционных блоков для перечисленных способов почти полностью повторяют схемы,

представленные на рис. 2, рис. 3 и рис. 5 соответственно. Отличие состоит лишь в работе устройства управления.

Выводы. Прогресс в области вычислительной техники увеличивает возможности злоумышленников по вскрытию защищенной информации, что приводит к повышению требований к стойкости криптоалгоритмов. С другой стороны, этот же прогресс позволяет разрабатывать усиленные средства информационной защиты.

Преимущества использования РУВ для реализации методов усиления по сравнению с традиционными вычислительными средствами тем существеннее, чем сложнее метод усиления.

Предложенные обобщенные структуры РПУ-БСШ могут служить основой для методики создания реконфигурируемых криптопроцессоров, реализующих усиленные алгоритмы защиты информации, которая позволит снизить требования к разработчикам и ускорить процесс разработки.

Основные принципы организации построения РПУ-БСШ, изложенные в настоящей работе, были опробованы на экспериментальных схемах криптопроцессоров, синтезированных для РУВ типа XC2S_EVAL фирмы Cesys на базе ПЛИС Xilinx Spartan-II (200000 эквивалентных логических элементов) и Nexys-2 фирмы Digilent на базе ПЛИС Xilinx Spartan3E-500 и Spartan3E-1200 (500000 и 1200000 эквивалентных логических элементов соответственно).

1. *Соколов А.В., Шаньгин В.Ф.* Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК Пресс, 2002. – 656 с.

2. *Гиранова А.К.* Анализ подходов к повышению эффективности закрытия информации и вопросы их реализации на унифицированных вычислителях // Зб. наук. пр. ІПМЕ НАН України. – Київ, 2009. – Вип. 52. – С. 78-83.

3. *Гильгурт С.Я.* Обзор современных реконфигурируемых унифицированных вычислителей // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Вип. 49. – Київ: 2008. – С. 17-24.

4. *Гильгурт С.Я.* Анализ существующих унифицированных вычислителей для выполнения ресурсоемких расчетов // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Вип. 48. – Київ: 2008. – С. 115-120.

5. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – М.: Триумф, 2002. – 816 с.

6. *Гиранова А.К.* Обобщенная структура реконфигурируемого процессора, реализующего симметричные алгоритмы закрытия информации // Зб. наук. пр. ІПМЕ НАН України. – Київ, 2010. –Вип. 57.

Поступила 10.02.2011р.