$$d_H(x_i, x_j) = \sum_{k=1}^{n} (\alpha_{ik} + \alpha_{jk}) .$$

У випадку, коли хромосоми складаються з окремих бітових послідовностей, які описують окремі параметри, останні перетворюються у відповідні фенотипи і між фенотипами обчислюється різниця у відповідності з співвідношенням:

$$d(x_i, x_j) = [x_{ik} + (x'_{ik} - x''_{ik})/(2^{m_k} - 1)] \sum_{j=1}^{m_k} v_{ki} 2^j - [x_{jk} + (x'_{jk} - x''_{jk})/(2^{m_k} - 1)] \sum_{j=1}^{m_k} v_{kj} 2^i] .$$

1. *Батищев Д.А.* Генетические алгоритмы решения экстремальных задач. – Воронеж: Изд-во ВГТУ, 1995.
2. *Олешко Т.І.* Дослідження взаємозв'язку між інформаційною моделлю та базами даних, що входять в склад інформаційної технології. Захист інформації – 2005.Спецвипуск, с.30-35.

Поступила 15.09.2010р.

УДК 004.056.55:004.272.23

А.К. Гиранова, ИПМЭ им. Г.Е.Пухова НАНУ, г. Киев

ОБОБЩЕННАЯ СТРУКТУРА РЕКОНФИГУРИРУЕМОГО ПРОЦЕССОРА, РЕАЛИЗУЮЩЕГО СИММЕТРИЧНЫЕ АЛГОРИТМЫ ЗАКРЫТИЯ ИНФОРМАЦИИ

С развитием информационных технологий все большую актуальность приобретают вопросы обеспечения безопасности информации – предотвращение ее утечки, несанкционированных воздействий на нее. Одним из важнейших направлений деятельности в данной сфере была и остается защита информации криптографическими методами.

Криптоалгоритмы можно поделить на три категории [1-4]:

- безключевые алгоритмы, которые не используют каких-либо ключей в процессе криптографических преобразований;
- одноключевые алгоритмы, использующие в своих вычислениях закрытый ключ;
- двухключевые алгоритмы, в которых на различных этапах вычислений применяются два вида ключей: закрытые и открытые.

На практике широкое применение нашли два последних подхода. К одноключевым алгоритмам относится симметричное шифрование, а к двухключевым – асимметричное.

Главное достоинство асимметричных криптосистем (криптосистем с

открытым ключом) – их потенциально высокая безопасность (нет необходимости сообщать значение секретных ключей и подтверждать их подлинность). Однако, быстродействие таких систем обычно в сотни и более раз ниже быстродействия симметричных криптосистем (криптосистем с закрытым ключом) [5].

В свою очередь, быстродействующие симметричные криптосистемы обладают существенным недостатком: необходимо регулярно передавать обновляемые секретные ключи.

Существует эффективный метод комбинированного использования симметричного и асимметричного шифрования. Данный гибридный метод шифрования позволяет сочетать преимущества высокой секретности, предоставляемые асимметричными криптосистемами, с преимуществами высокой скорости работы, присущими симметричным криптосистемам.

При таком подходе симметричную криптосистему применяют для шифрования исходного открытого текста, а асимметричную – только для шифрования секретного ключа симметричной криптосистемы. В результате асимметричная криптосистема не заменяет, а лишь дополняет симметричную, позволяя повысить в целом защищенность передаваемой информации. Такой подход иногда называют схемой электронного цифрового «конверта».

Наиболее широко используемыми алгоритмами шифрования являются алгоритмы блочного симметричного шифрования (БСШ) [1, 6]. Упомянутые алгоритмы и будут рассмотрены в данной статье.

Для реализации криптографической защиты используются как аппаратные, так и программные средства. Следует заметить, что недостатком аппаратной реализации является жесткая структура, а программной реализации – невысокая производительность [7-9]. Избавиться от недостатков позволяет применение реконфигурируемых унифицированных вычислителей (РУВ) [10].

Анализ последних достижений и публикаций показал, что главная проблема, которая сдерживает широкое применение РУВ – сложность создания конфигураций для ПЛИС. Этот процесс требует от разработчика высокой квалификации, знаний в области синтеза цифровых схем, владения специализированными пакетами. Одним из вариантов решения данной проблемы является разработка методики создания широкого класса решений в конкретной предметной области, которая позволит упростить разработку конфигураций. В области создания процессоров защиты данных такая методика позволит создавать симметричные криптопроцессоры разработчикам, не имеющим навыков программирования ПЛИС. Основой создания данной методики является обобщенная структура создания реконфигурируемого процессора, реализующего алгоритмы БСШ (РП-БСШ).

В настоящей работе проведен анализ существующих алгоритмов блочного симметричного шифрования и на его основе предлагается обобщенная структура реконфигурируемого процессора, реализующего

симметричные алгоритмы закрытия информации.

Целью настоящей статьи является разработка методики создания конфигураций для шифропроцессоров на базе РУВ разработчиками, не имеющим навыков программирования ПЛИС.

Подавляющее большинство современных блочных алгоритмов шифрования работают схожим образом: над шифруемым текстом выполняется некое преобразование с участием ключа шифрования, которое повторяется определенное число раз (раундов). По своей структуре алгоритмы БСШ классифицируются следующим образом [1]:

– алгоритмы на основе сети Фейстеля;
– алгоритмы на основе подстановочно-перестановочных сетей (SP-сети);
– алгоритмы со структурой «квадрат»;
– алгоритмы с нестандартной структурой.

Сеть Фейстеля подразумевает разбиение обрабатываемого блока данных на несколько подблоков (чаще всего на два), один из которых обрабатывается некоторой функцией f и накладывается на один или несколько остальных подблоков. На сети Фейстеля основано большинство современных алгоритмов шифрования (DES, ГОСТ 28147, RC5, Blowfish, TEA, CAST-128 и т.д.).

SP-сети обрабатывают за один раунд целиком шифруемый блок, обработка данных сводится, в основном, к заменам и перестановкам, зависящим от ключа. Данные сети являются гораздо менее распространенными, чем сети Фейстеля. В качестве примера SP-сети можно привести алгоритмы Seprent или SAFER+.

Для структуры «квадрат» (Square) характерно представление шифруемого блока данных в виде двумерного байтового массива. Криптографические преобразования могут выполняться над отдельными байтами массива, а также над его строками или столбцами. В качестве примера можно привести алгоритмы SHARK, Crypron, а также алгоритм Rijndael, который стал в США новым стандартом шифрования AES.

Классифицировать все возможные варианты алгоритмов шифрования достаточно сложно, т.е. существуют такие алгоритмы, которые невозможно причислить ни к одному из перечисленных выше типов. В качестве примера таких алгоритмов можно привести алгоритм FROG (в каждом раунде по достаточно сложным правилам выполняется модификация двух байтов шифруемых данных) и алгоритмы семейства SHACAL, которые основаны на функции компрессии хэш-алгоритма SHA.

Сходство большинства БСШ позволяет создать обобщенную структуру РП-БСШ, в качестве основы для методики разработки широкого класса решений в области создания процессоров защиты данных.

Рассмотрим подробнее обобщенную структурную схему шифропроцессора (рис 1).

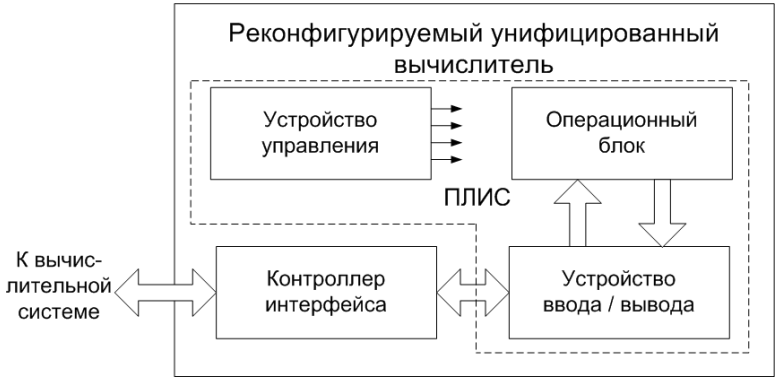

Рис. 1. Обобщенная структурная схема шифропроцессора

Вычислительная система и реконфигурируемый унифицированный вычислитель взаимодействуют между собой посредством интерфейса. Наиболее перспективные интерфейсы обмена данными между вычислительной системой и РУВ приведены в статье [11]. Контроллер интерфейса, входящий в состав РУВ, является средством обмена информацией с вычислительной системой. На этот же контроллер возлагается функция загрузки конфигурации в ПЛИС. Микросхема ПЛИС, входящая в состав реконфигурируемого вычислителя, позволяет синтезировать внутри себя произвольную цифровую схему. В случае универсального блочного шифропроцессора данная схема должна содержать устройство ввода/вывода, операционный блок и устройство управления.

Рассмотрим взаимодействие устройств, которые входят в схему, синтезируемую в ПЛИС. Устройство ввода/вывода передает в операционный блок режимы, ключ, а также исходный блок данных. В качестве результата устройства ввода/вывода принимает зашифрованный блок данных. Обменом между операционным блоком и устройством ввода/вывода руководит устройство управления. Это устройство также управляет работой операционного блока.

Рассмотрим более подробно устройство операционного блока (рис.2).

Как было сказано выше, на вход операционного блока с устройства ввода/вывода поступают режимы, ключ, а также исходный блок данных. Далее эта информация, а также счетчик раундов, который контролируется устройством управления, поступает на вход ядра алгоритма, где и выполняется собственно преобразование. Ядро алгоритма представляет собой комбинационную схему. Преобразованный блок данных помещается в выходной регистр и передается в устройство ввода/вывода.

Основой устройства управления является цифровой автомат, граф функционирования которого изображен на рисунке 3. Данный автомат приведен для алгоритма ГОСТ 28147 [12, 13].

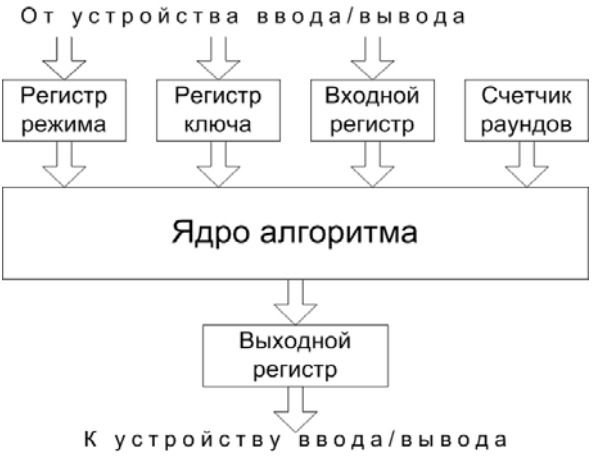

Рис. 2. Структурная схема операционного блока

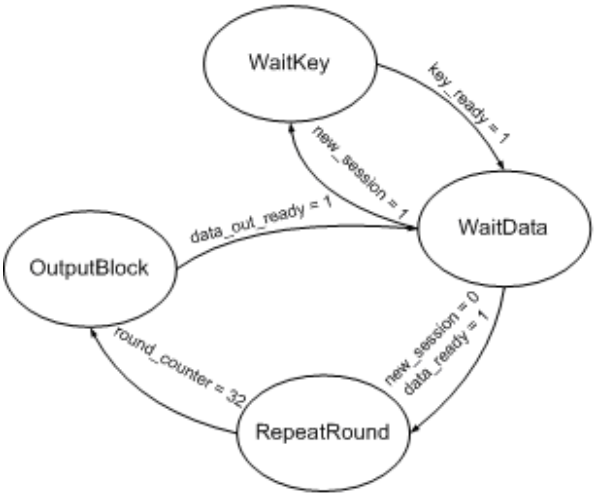

Рис. 3. Граф функционирования цифрового автомата

Данный автомат имеет четыре состояния: WaitKey, WaitData, RepeatRound и OutputBlock. Начальное состояние автомата – WaitKey. В данном состоянии осуществляется формирование ключа. При успешном формировании (key_ready = 1) происходит переход в следующие состояние – WaitData. В данном состоянии формируется блок данных. При успешном формировании (data_ready = 1) происходит переход в следующие состояние – RepeatRound. В данном состоянии автомат остается до тех пор, пока количество раундов не достигнет 32 (round_counter = 32). Далее автомат

переходит в следующее состояние – OutputBlock. В данном состоянии происходит передача преобразованного блока данных через устройство ввода/вывода и интерфейс в вычислительную систему. Подробнее об обмене данными между вычислительной системой и реконфигурируемым вычислителем написано в статье [14]. При успешной передаче данных (data_out_ready = 1), автомат переходит в состояние WaitData. Если в этом состоянии сигнал new_session равен 1, то есть начинается новая сессия с новым ключом, то автомат переходит в начальное состояние WaitKey, а если равен 0, то происходит формирование блока данных.

Выводы. В данной статье проведен анализ существующих алгоримов БСШ с целью создания методики разработки реконфигурируемого процессора, реализующего алгоритмы блочного симметричного шифрования. Структурная схема реконфигурируемого процессора, реализующего алгоритмы БСШ, предложенная в данной статье, позволит упростить разработку конфигураций, что в свою очередь упростит задачу создания симметричных криптопроцессоров разработчикам, не имеющим навыков программирования ПЛИС.

1. *Панасенко С.П.* Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009. – 576 с.
2. *Menezes A., Oorshot P., Vanstone S.* Handbook of applied cryptography. – N.Y.: CRC Press Inc., 1996. – 816 p.
3. *Шаньгин В.Ф.* Информационная безопасность компьютерных систем и сетей: учеб. пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008. – 416 с.
4. *Гиранова А.К.* Анализ подходов к повышению эффективности закрытия информации и вопросы их реализации на унифицированных вычислителях // Зб. наук. праць ІПМЕ НАН України. – Київ, 2009. – Вип. 52. – С.78-83.
5. *Соколов А.В., Шаньгин В.Ф.* Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК Пресс, 2002. – 656 с.
6. *Коркішко Т., Мельник А., Мельник В.* Алгоритми та процесори симетричного блокового шифрування. – Львів: Бак, 2003. – 168 с.
7. *Гиранова А.К.* Сравнительный анализ реализаций алгоритмов шифрования на реконфигурированных вычислителях // Зб. наук. праць ІПМЕ НАН України. – Київ, 2008. – Вип. 48. – С.34-39.
8. *Петров А.А.* Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.
9. *И. Лукашов* Аппаратные шифраторы на отечественной элементной базе // Электроника: НТБ – 2001 – № 6 – с.48-51
10. *Гильгурт С.Я.* Анализ применения унифицированных вычислителей в интеллектуальных системах. // Искусственный интеллект. – Донецк: НАН Украины – институт проблем ИИ. – 2009. – №1. – С. 144–148.
11. *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.
12. ДСТУ ГОСТ 28147:2009 Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.

13. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – М.: Триумф, 2002. – 816 с.
14. *Гильгурт С.Я., Гиранова А.К.* Некоторые вопросы обмена данными между персональным компьютером и реконфигурируемым устройством // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Вип. 43. – Київ: 2007. – С. 86–94.

Поступила 22.09.2010р.

УДК 683.06

Є.Д.Бабинець

ЗАГАЛЬНА ОРГАНІЗАЦІЯ ВИКОРИСТАННЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ АВТОМАТИЗОВАНОГО ПРЕКТУВАННЯ ОБРАЗУ КНИЖКОВОГО ВИДАННЯ

Інформаційна технологія, по своєму визначенню, представляє собою певну сукупність інформаційних засобів, з допомогою яких можна реалізувати необхідні технологічні процеси для створення певних продуктів [1,2]. Це означає, що відповідна технологія представляє собою повну систему окремих компонент, до яких відносяться:

- алгоритми аналізу та перетворення даних,
- бази даних, вміщають дані про предметну область, в якій передбачається розвязувати ті, або інші задачі,
- інформаційні компоненти, які повязують абстрактні представлення окремих компонент інформційної технології з їх описами, які доступні користувачу,
- окремі методики використання інформаційних засобів для розвязування окремих задач, що можуть бути сформульовані в рамках предметної області,
- засоби обслуговування компонент інформаційної технології, які дозволяють модифікувати останні, при необхідності, що обумовлюється розвязком окремих задач,
- засоби аналізу методів розвязку задач, що реалізуються на основі використання інформаційної технології,
- засоби аналізу та формування інтерпретаційних описів даних на природній мові користувача, отриманих в результаті розвязку задач,
- засоби для реалізації сприятливих для користувача інтерфейсів, які дозволяють користувачу отримувати відповіді на питання, що можуть виникнути в процесі використання відповідної інформаційної технології.

