КРАТКИЕ СООБЩЕНИЯ

УДК 681.324.067

ОЦЕНКА ЭФФЕКТИВНОСТИ РАСПАРАЛЛЕЛИВАНИЯ КРИПТОАЛГОРИТМОВ

А.С. ПОЛЯКОВ, В.Е. САМСОНОВ

Объединенный институт проблем информатики Национальной академии наук Беларуси, Республика Беларусь

Поступила в редакцию 12 октября 2016

Аннотация. Рассмотрена проблема повышения быстродействия алгоритмов шифрования при их аппаратной реализации с использованием параллельной обработки фрагментов алгоритмов. Приводятся результаты анализа и моделирования аппаратной реализации трех алгоритмов шифрования с различной степенью параллелизма, получены оценки эффективности распараллеливания операций алгоритмов.

Ключевые слова: аппаратная реализация, криптоалгоритм, параллельная обработка.

Abstract. The problem of increasing the speed of the encryption algorithms for their hardware implementation using parallel processing of algorithms fragments is considered. The results of analysis and simulation of hardware implementation of the three encryption algorithms with varying degrees of parallelism are given. The efficiency of parallelization algorithms operations is estimated.

Keywords: hardware implementation, cryptographic algorithm, parallel processing.

Doklady BGUIR. 2017, Vol. 103, No. 1, pp. 77-81
The efficiency of crypt algorithms parallelization
A.S. Poljakov, V.E. Samsonov

Введение

В условиях повышения производительности вычислительных сетей актуальной является проблема защиты передаваемой по коммуникационным каналам информации. Надежным способом защиты является шифрование передаваемых сообщений с помощью криптографических алгоритмов, программная реализация которых не всегда обеспечивает необходимую скорость шифрования. Аппаратная реализация алгоритмов позволяет значительно повысить производительность шифрования, особенно в случае параллельной обработки фрагментов алгоритма. Однако эффективность распараллеливания алгоритмов не исследована. Неизвестно, какие преимущества и недостатки могут быть получены в результате параллельной реализации алгоритмов. А на практике часто требуется более высокая скорость шифрования информации. Именно в таких случаях целесообразным является использование параллельной обработки фрагментов применяемого алгоритма шифрования.

Для оценки эффективности распараллеливания операций были исследованы аппаратные реализации трех известных, широко применяемых криптоалгоритмов:

– алгоритм СТБ34.101.31–2011 [1], изначально имевший название Belt [2], а в 2011 году принятый в качестве стандарта Республики Беларусь;

– алгоритм AES (Advanced Encryption Standard) [3], являющийся стандартом США, и используемый во многих странах мира;

– алгоритм ГОСТ 28147–89 [4], бывший в свое время стандартом СССР, в настоящее время используемый в странах СНГ.

Краткая характеристика исследуемых алгоритмов

Алгоритм блочного шифрования СТБ 34.101.31-2011 рассчитан на работу с блоком данных длиной 128 бит и длиной ключа 256 бит. Алгоритм предусматривает шифрование в режимах простой замены, сцепления блоков, гаммирования с обратной связью и счетчика. Поскольку основным является режим простой замены, то в настоящей работе исследовался только он. В алгоритме предусмотрено выполнение восьми тактов (раундов), на каждом из которых используются 32-битовые ключи шифрования, сформированные из исходного 256-битового ключа. При шифровании блока данных выполняются операции арифметическое сложение, вычитание, сложение по mod 2, циклический сдвиг, подстановка с использованием раундовых ключей шифрования.

В базовом алгоритме шифрования (режим простой замены) предусмотрено последовательное выполнение 12 комплексных операций над блоком данных. В результате анализа алгоритма выявлены те операции, которые информационно независимы и могут выполняться параллельно. Если воспользоваться нумерацией операций, которая принята в п. 4.1.3 стандарта, то одновременно могут выполняться операции 1 и 2, 3 и 4, 5 и 6, 7 и 8.

В алгоритме AES размеры шифруемого блока и ключа шифрования могут изменяться, что допускается используемой в нем архитектурой «квадрат», базирующейся на прямых преобразованиях шифруемого блока, представляемого в виде матрицы байтов. В настоящее время в качестве стандарта AES принят вариант алгоритма с размером шифруемого блока 128 бит, длиной ключа 128 бит и числом раундов 10. Шифрование предусматривает серию однотипных раундов, на каждом из которых блок преобразуется как единое целое. На каждом раунде производится сложение по модулю 2 шифруемого блока и ключевого элемента раунда, за которым следует нелинейное преобразование блока, включающее операции подстановки, циклического сдвига строк и умножения матриц.

С точки зрения возможности распараллеливания операций алгоритм AES предоставляет большие возможности в связи с тем, что ряд сложных и трудоемких операций над шифруемым блоком данных может выполняться одновременно, поскольку информационно они независимы. В частности, параллельно могут выполняться операции сложения блока данных с раундовым ключом, сдвиг строк, подстановка байтов, умножение матриц.

Что касается алгоритма ГОСТ 28147-89, то параллельное выполнение операций невозможно, поскольку на каждом из 32-х циклов алгоритма в каждой из предусмотренных в нем операций используются результаты обработки данных на предыдущем цикле, размещаемые на одних и тех же регистрах.

Результаты экспериментальных исследований

Для сравнения характеристик аппаратной реализации рассматриваемых алгоритмов использовалась следующая методика: для каждого из алгоритмов с помощью системы проектирования XILINX ISE были разработаны проекты в базисе микросхем типа FPGA, производилась имплементация проектов (этапы Synthesize, Translate, Map), в результате чего получены данные о затратах оборудования, необходимого для реализации алгоритмов.

С помощью моделирующей системы ModelSim выполнено логическое моделирование проектов, результаты которого позволили определить количество тактов, необходимых для шифрования одного блока информации, а также для выполнения отдельных этапов алгоритмов. Для проверки корректности разработанных проектов их отладка и моделирование производились на тестовых примерах, в качестве которых были использованы:

– для СТБ34.101.31-2011 – тесты, полученные от разработчиков алгоритма;

– для AES – тесты, приведенные в приложениях к описанию стандарта [3],

– для ГОСТ 28147-89 – тест, представленный в стандарте [5].

Для алгоритмов СТБ34.101.31-2011 и AES было разработано по два проекта, предусматривающие:

1) последовательное выполнение операций (СТБ_seq и AES_seq),

2) выполнение алгоритмов с использованием возможностей параллельной обработки операций (СТБ_par и AES_par).

Для алгоритма ГОСТ 28147–89 был разработан только один проект.

В результате моделирования проектов установлено количество тактов, необходимое для шифрования одного блока информации. Полученные данные представлены в табл. 1. Поскольку в алгоритмах используются блоки различных размеров (128 бит в алгоритмах СТБ и AES, и 64 бита в алгоритме ГОСТ), то для более корректного сравнения производительности исследуемых алгоритмов в последнем столбце табл. 1 представлены результаты, приведенные к блоку данных длиной 64 бита.

Таблица 1. **Производительность алгоритмов шифрования**

Алгоритм	Размер блока данных, бит	Количество тактов на шифрование блока данных	Количество тактов на шифрование блока данных размером 64 бита
СТБ_seq	128	336	168
СТБ_par	128	211	106
AES_seq	128	756	378
AES_par	128	97	49
ГОСТ 28147-89	64	129	129

Результаты моделирования проектов показывают, что при использовании параллельной обработки операций алгоритмов время шифрования для алгоритма СТБ сокращается в 1,6 раза, а для алгоритма AES – в 7,7 раза. Что касается алгоритма ГОСТ 28147–89, то его производительность даже без распараллеливания лишь незначительно уступает распараллеленному алгоритму СТБ_par.

Данные о затратах аппаратуры на реализацию алгоритмов, полученные в результате имплементации соответствующих проектов, представлены в табл. 2.

Таблица 2. **Объемы оборудования, необходимого для реализации алгоритмов**

Алгоритм	Кол-во Slices	Количество триггеров	Количество LUT	Количество BRAMs	Объем памяти, байт
СТБ_seq	750	649	1392	9	288
СТБ_par	1070	302	2050	28	896
AES_seq	777	458	1114	5	704
AES_par	2107	504	3461	35	8384
ГОСТ 28147–89	49	233	479	9	160

Примечание к табл. 2: LUT (look-up table) – логическая таблица, представляющая собой однобитовое ОЗУ на 16 ячеек; Slice – единица оборудования, состоящая из двух триггеров и двух LUT; BRAM – блок памяти размером 256 байтов.

Если привести некоторые элементы табл. 2 (Slices и BRAMs) к более простым элементам, то получим табл. 3, в которой соотношение объемов оборудования, требуемого для реализации алгоритмов с последовательным и параллельным выполнением операций, удобнее для сравнительной оценки.

Таблица 3. **Объемы оборудования в базовых элементах микросхем**

Алгоритм	Количество триггеров	Количество LUT	Объем памяти, байт
СТБ_seq	2150	2442	2592
СТБ_par	3292	4190	8064
AES_seq	2012	4718	1984
AES_par	2696	7675	17344

Основное увеличение оборудования происходит вследствие резкого роста объема количества элементов памяти: для алгоритма СТБ – в 3,1 раза (при увеличении быстродействия в 1,6 раза), для алгоритма AES – в 8,7 раза (при увеличении быстродействия в 7,7 раза). Увеличение количества триггеров и LUT не так велико – в 1,4÷1,8 раза.

Исходя из объемов требуемого оборудования, алгоритмы могут быть аппаратно реализованы, к примеру, на микросхемах семейства Spartan, указанных в табл. 4.

Таблица 4. **Микросхемы семейства Spartan, на которых могут быть реализованы алгоритмы**

Реализация алгоритма	Тип микросхемы	Ориентировочная стоимость микросхемы (у.е.)
СТБ_seq	XC6SL9 или аналог	12 ÷ 30
СТБ_par	XC6SL16 или аналог	25 ÷ 35
AES_seq	XC6SL9 или аналог	30 ÷ 40
AES_par	XC6SL150 или аналог	200
ГОСТ 28147-89	XC6SLX4 или аналог	5

Заключение

Выполненное исследование позволило определить возможности повышения скорости (производительности) рассмотренных криптоалгоритмов в случае распараллеливания операций при их аппаратной реализации и оценить соотношение связанных с этим затрат. Безусловно, распараллеливание операций требует использования большего объема оборудования и применения более мощных и, соответственно, дорогих микросхем.

Сравнение данных табл. 1 и 4 показывает, что увеличение затрат примерно пропорционально повышению производительности рассмотренных алгоритмов.

Поскольку выбор дорогих микросхем обусловлен, главным образом, большим количеством элементов памяти, то затраты на микросхемы можно существенно снизить путем установки внешних элементов памяти, стоимость которых незначительна.

Список литературы

1. СТБ 34.101.31-2011. Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности.
2. Алгоритм шифрования Belt / С.В. Агиевич [и др.] // Управление защитой информации. 2002. № 4. С. 407–412.
3. Announcing the Advanced Encryption Standard (AES) / Federal Information Processing Standards Publication [Электронный ресурс]. – Режим доступа: http://www.nist.gov/CryptoToolkit. – Дата доступа: 12.10.2016.
4. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
5. ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования.

References

1. STB 34.101.31-2011. Informacionnye tehnologii. Zashhita informacii. Kriptograficheskie algoritmy shifrovanija i kontrolja celostnosti. (in Russ.)
2. Algoritm shifrovanija Belt / S.V. Agievich [i dr.] // Upravlenie zashhitoj informacii. 2002. № 4. S. 407–412. (in Russ.)
3. Announcing the Advanced Encryption Standard (AES) / Federal Information Processing Standards Publication [Electronic resource]. – Access mode: http://www.nist.gov/CryptoToolkit. – Date of access: 12.10.2016.
4. GOST 28147-89. Sistemy obrabotki informacii. Zashhita kriptograficheskaja. Algoritm kriptograficheskogo preobrazovanija. (in Russ.)
5. GOST R 34.11-94. Informacionnaja tehnologija. Kriptograficheskaja zashhita informacii. Funkcija hjeshirovanija. (in Russ.)

Сведения об авторах

Поляков А.С., к.т.н., доцент, ведущий научный сотрудник ОИПИ НАН Беларуси.

Самсонов В.Е., заведующий отделом ОИПИ НАН Беларуси.

Information about the authors

Poljakov A.S., Ph.D., associate professor, leading researcher of UIIP NAS Belarus.

Samsonov V.E., head of department of UIIP NAS Belarus.

Адрес для корреспонденции

220012, Республика Беларусь,
г. Минск, ул. Сурганова, д. 6,
ОИПИ НАН Беларуси
тел. +375-29-632-54-46;
e-mail: alexpolja@tut.by;
Поляков Александр Сергеевич

Address for correspondence

220012, Republic of Belarus,
Minsk, Surganova st., 6,
UIIP NAS Belarus
tel. +375-29-632-54-46;
e-mail: alexpolja@tut.by;
Poljakov Aleksandr Sergeevich