ЗАЩИТА ИНФОРМАЦИИ

УДК 681.324.067

А.С. Поляков, В.Е. Самсонов

ХАРАКТЕРИСТИКИ АППАРАТНОЙ РЕАЛИЗАЦИИ НЕКОТОРЫХ СИММЕТРИЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

Анализируются возможности аппаратной реализации трех современных симметричных алгоритмов шифрования (ГОСТ 28147-89, AES, Belt). Приводятся основные характеристики аппаратной реализации указанных алгоритмов, полученные путем логического моделирования проектов этих алгоритмов, которые были разработаны с помощью системы проектирования XILINX в базисе микросхем типа FPGA.

Введение

Защита информации является важной и актуальной проблемой в области информационного взаимодействия. Шифрование относится к одному из способов решения этой проблемы, приобретающему все большее значение по мере развития информационных систем. В настоящее время известно значительное количество блочных алгоритмов шифрования, часть из которых являются государственными стандартами.

Тем не менее во всем мире постоянно ведутся исследования по разработке новых алгоритмов шифрования. В частности, после появления фактов взлома алгоритма DES (Data Encription Standard [1]) в США был объявлен конкурс на новый алгоритм симметричного шифрования, в результате которого в декабре 2001 г. был отобран алгоритм Rijendal, утвержденный в качестве государственного стандарта США и получивший название AES (Advanced Encryption Standard) [2].

В Республике Беларусь был разработан и в 2007 г. принят в качестве предстандарта алгоритм Belt [3]. Аналогичная ситуация и в других странах.

В связи с появлением новых алгоритмов шифрования возникает необходимость их сравнения с существующими алгоритмами для оценки возможности эффективного применения соответствующего алгоритма в конкретных условиях. Учитывая, что все более высокие требования предъявляются к производительности (быстродействию) алгоритмов, а наиболее эффективным способом повышения производительности является аппаратная реализация, в настоящей работе проведено сравнение показателей аппаратной реализации трех блочных симметричных алгоритмов шифрования:

1) применяемого в Республике Беларусь и во многих странах СНГ алгоритма ГОСТ 28147–89 [4], являющегося, по оценке специалистов [5], одним из наиболее криптографически устойчивых симметричных блочных алгоритмов шифрования с возможностью надежного использования его еще в течение нескольких десятилетий;

2) предстандарта Belt [3], представляемого в настоящее время к внедрению в качестве национального стандарта;

3) алгоритма AES [2], имеющего большой потенциал для распараллеливания операций при аппаратной реализации и, следовательно, достижения высокой производительности.

В настоящее время данные по этому вопросу в литературе отсутствуют.

1. Краткая характеристика исследуемых алгоритмов

Алгоритм криптографического преобразования ГОСТ 28147–89, успешно используемый до настоящего времени в странах СНГ, в том числе и в Республике Беларусь, аналогичен ранее использовавшемуся в США криптоалгоритму DES [1], но отличается от него большим размером ключа (256 битов) и введением некоторых дополнительных функций. Одновременно обрабатываемый блок данных имеет размер 64 бита. Алгоритм построен на архитектуре «сбалансированная

сеть Файстеля» [6], основным принципом которой является то, что процесс шифрования состоит из 32 однотипных раундов, на каждом их которых шифруемый блок (64 бита) делится на две равные части. Одна часть модифицируется путем сложения по модулю 2 со значением, вырабатываемым из другой части с помощью операций сложения по модулю 2^{32} со значением раундового ключа, подстановки и циклического сдвига. Между раундами части блока меняются местами, таким образом, на следующем раунде текущий измененный блок становится неизменяемым и наоборот. Для выработки 32-битовых ключевых элементов из 256-битового ключа применен простой подход: ключ интерпретируется как массив, состоящий из восьми ключевых элементов. Эти элементы используются на раундах шифрования три раза в прямом порядке и один раз в обратном, в итоге каждый ключевой элемент используется четыре раза.

Алгоритм блочного шифрования Belt 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, в настоящей работе исследовался только он. Алгоритм Belt предусматривает выполнение восьми тактов (раундов), в которых используются 32-битовые ключи шифрования, сформированные из исходного ключа. При шифровании применяются базовые операции: сложение, вычитание, сложение по модулю 2, циклический сдвиг 32-разрядого слова на фиксированное число разрядов, подстановка.

В алгоритме AES, в отличие от ГОСТ 28147–89, размеры шифруемого блока и ключа могут изменяться, что допускается используемой в нем архитектурой «квадрат», которая базируется на прямых преобразованиях шифруемого блока, представляемого в форме матрицы байтов. Зашифрование состоит из серии однотипных раундов (10, 12 или 14 в зависимости от размеров шифруемого блока и ключа шифрования), на каждом из которых блок преобразуется как единое целое. Таким образом, за раунд шифруется полный блок. Каждый раунд заключается в побитовом сложении по модулю 2 состояния шифруемого блока и ключевого элемента раунда, за которым следует сложное нелинейное преобразование блока, состоящее из трех операций: подстановка, сдвиг и умножение матриц. В качестве стандарта AES принят вариант алгоритма с размером шифруемого блока 128 бит, длиной ключа 128 бит и числом раундов 10 (AES-128). Стандарт AES предусматривает три режима: зашифрование, расшифрование и эквивалентное расшифрование, отличающееся от режима расшифрования порядком выполнения операций и правилами формирования раундовых ключей.

2. Результаты экспериментальных исследований

Для сравнения показателей аппаратной реализации рассматриваемых алгоритмов была использована следующая методика: для каждого из алгоритмов с помощью системы проектирования фирмы XILINX были разработаны реализующие их проекты в базисе микросхем типа FPGA и произведено логическое моделирование проектов, результаты которого позволили определить количество тактов, необходимых как для шифрования одного блока информации каждым из алгоритмов, так и для выполнения отдельных операций алгоритмов. Выполнение этапов синтеза и имплементации проектов позволило определить объемы оборудования, необходимого для реализации рассматриваемых вариантов каждого из алгоритмов.

С целью проверки корректности разработанных проектов их отладка и моделирование производились на тестовых примерах, в качестве которых были использованы:

для ГОСТ 28147–89 – пример, приведенный в описании стандарта [7];

для Belt – тест, полученный от разработчиков алгоритма;

для AES – тесты, приведенные в описании стандарта [2].

Чтобы оценить эффективность распараллеливания операций для алгоритмов Belt и AES, были разработаны несколько проектов, отличающихся степенью параллелизма выполняемых операций:

для алгоритма Belt:

проект Belt_seq – последовательное выполнение всех операций;

проект Belt_par – параллельное выполнение операций подстановки и шагов алгоритма 1÷2, 3÷4, 7÷8;

для алгоритма AES:

проект AES_st – последовательное выполнение операций;

проект AES_par – параллельное выполнение всех основных операций алгоритма (сложение с раундовым ключом, сдвиг строк, подстановка байтов, умножение матриц).

Проекты разрабатывались с использованием языка VHDL (для управляющего автомата) и схемотехнических решений (для выполнения операций алгоритмов) на основе как типовых элементов системы проектирования XILINX, так и элементов, создаваемых с помощью синтезирующего блока Core Generator.

Для анализа и сравнения производительности алгоритмов использовалась следующая методика: каждый из разработанных проектов был промоделирован с помощью системы ModelSim 6.2f SE, которая позволяет получать значения всех внутренних и выходных сигналов проекта на каждом такте его работы. При этом производилась проверка правильности производимых вычислений сигналов, а также определялось количество тактов, необходимое как для выполнения отдельных операций алгоритма, так и для шифрования блока данных в целом.

В табл. 1 представлены сведения о производительности вариантов исследуемых алгоритмов, выраженные в количестве тактов, затрачиваемых на шифрование одного блока данных:

для ГОСТ 28147–89 – в режиме простой замены, длина ключа 256 бит;

для Belt – в режиме простой замены, длина ключа 256 бит;

для AES – в режимах зашифрования, расшифрования, эквивалентного расшифрования, длина ключа 128 бит.

Таблица 1

Производительность алгоритмов шифрования

Алгоритм	Размер блока данных, бит	Количество тактов на один блок данных	Количество тактов на блок данных в 64 бита
ГОСТ 28147–89	64	129	129
Belt_seq	128	336	168
Belt_par	128	211	106
AES_seq	128	756	378
AES_par	128	97	49

В табл. 1 не указаны единовременные (на каждый сеанс) затраты на подготовку раундовых ключей, которые составляют:

для проекта AES_seq – 251 такт во всех режимах и дополнительно 146 тактов в режиме эквивалентного расшифрования;

для проекта AES_par – 210 и 127 тактов соответственно. Разница в значениях затрат для проектов AES_seq и AES_par обусловлена тем, что в AES_par на этапе подготовки раундовых ключей некоторые операции выполняются параллельно, благодаря чему и затраты времени меньше.

Поскольку в алгоритме Belt ключи для тактов 2÷8 формируются путем выбора в определенном порядке ключей из множества ключей такта 1, предварительная подготовка ключей для всех тактов не производилась, а необходимый ключ выбирался в процессе шифрования путем параметрического задания соответствующего номера ключа из множества ключей такта 1 в зависимости от номера текущего такта в соответствии с правилами формирования тактовых ключей, предусмотренных алгоритмом Belt. Это позволило избежать дополнительных затрат времени и элементов памяти.

Если за единицу принять производительность алгоритма AES_par, значения относительной производительности других алгоритмов составят: ГОСТ 28147–89 – 0,38; Belt_seq – 0,29; Belt_par – 0,46; AES_seq – 0,13.

Если за единицу принять производительность алгоритма ГОСТ 28147–89, значения относительной производительности других алгоритмов составят: Belt_seq – 0,70; Belt_par – 1,21; AES_seq – 0,34; AES_par – 2,63.

Данные табл. 1 показывают, насколько существенно увеличивается быстродействие алгоритмов при организации параллельного вычисления:

– некоторых ветвей алгоритма (в случае с Belt_par – на 58 %);
– всех основных операций алгоритма (в случае с AES_par – на 770 %).

Сложность аппаратной реализации рассматриваемых алгоритмов, определяемая количеством используемых в проекте схемотехнических элементов, в значительной степени зависит не только от алгоритмической сложности рассматриваемых алгоритмов, но и от типа используемых в них операций, выполняемых над данными и ключами шифрования. Обобщенные сведения об объеме оборудования, требуемого для реализации проектов, представлены в табл. 2.

Таблица 2

Объем оборудования, требуемый для реализации алгоритмов

Алгоритм	Число Slices	Число триггеров	Число четырехвход. LUTs	Число BRAMs	Объем памяти, байт
ГОСТ 28147–89	349	233	479	9	160
Belt_seq	750	649	1392	9	288
Belt_par	1070	302	2050	28	896
AES_seq	777	458	1114	5	704
AES_par	2107	504	3461	35	8384

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

Для дополнительной оценки сложности аппаратной реализации алгоритмов в табл. 3 представлены сведения о количестве шин, соединяющих элементы различных типов: мультиплексоры, регистры, арифметические и логические элементы, элементы памяти.

Таблица 3

Количество шин на элементах оборудования

Алгоритм	Мультиплексоры	Регистры	Арифметические элементы	Логические элементы	Элементы памяти
ГОСТ 28147–89	450	288	224	384	99
Belt_seq	2432	900	644	192	83
Belt_par	3030	446	708	480	288
AES_seq	1384	512	0	932	114
AES_par	2518	1060	0	2028	584

В отличие от алгоритмов ГОСТ 28147–89 и Belt, использующих ключи длиной 256 бит, для алгоритма AES рассматривался вариант AES-128 с длиной ключа 128 бит, имеющий в описании стандарта контрольный пример, который позволяет проверить правильность аппаратной реализации алгоритма. При оценке характеристик аппаратной реализации алгоритма AES-256 необходимо принять во внимание следующее: поскольку все операции над элементами ключа шифрования в проекте AES-par выполняются параллельно, производительность алгоритма AES-256 по отношению к алгоритму AES-128 уменьшится пропорционально увеличению числа раундов, т. е. в 14 : 10 = 1,4 раза; время на подготовку раундовых ключей (единовременные затраты при шифровании одного сообщения) увеличится в два раза. Что касается необходимого для реализации алгоритма оборудования, то оно увеличивается в соответствии с увеличением размера ключа и долей операций с участием элементов ключа в общем объеме операций, а именно: объем элементов памяти – на 128 бит, а объем остальных элементов схемы – примерно на 20 %.

3. Анализ результатов

В табл. 1 для алгоритмов ГОСТ 28147–89 и Belt приведены сведения о затратах времени на шифрование одного блока данных в режиме простой замены. Шифрование в режимах гаммирования и гаммирования с обратной связью в алгоритме ГОСТ 28147–89 требует 133 такта на

подготовку первой гаммы шифра, получаемой путем зашифрования специально создаваемой 64-битной синхропосылки, а шифрование самого блока информации удлиняется лишь на шесть тактов в сравнении с режимом простой замены. Аналогичная ситуация для режимов сцепления блоков и гаммирования с обратной связью в алгоритме Belt.

В алгоритмах AES_seq и AES_par шифрование во всех режимах производится с одинаковыми затратами времени, но перед выполнением операции шифрования необходимо выполнить операцию предварительной подготовки раундовых ключей, которая применительно к алгоритму AES в режимах зашифрования и расшифрования занимает 210 тактов, а в режиме эквивалентного расшифрования – 356 тактов. Выполнение основных операций алгоритма AES_par требует: подстановка и сдвиг – 40 тактов, умножение матриц – 27 тактов, сложение с раундовым ключом – 30 тактов.

Если принять во внимание, что микросхема xc3s200 серии Spartan имеет 1920 доступных Slices, 3840 триггеров, 3840 четырехвходовых LUTs и 12 BRAMs, то первые пять из приведенных в табл. 1–3 алгоритмов могут быть реализованы на этой микросхеме и лишь для AES_par потребуется микросхема xc3s400. При этом следует учесть, что для алгоритмов Belt_par и AES_par необходимы установка дополнительной внешней памяти и создание соответствующего интерфейса, что не представляет особой сложности.

Используя данные табл. 1, легко вычислить производительность аппаратной реализации приведенных алгоритмов, основываясь на значении тактовой частоты применяемой микросхемы. Например, если выбрать микросхему с тактовой частотой 500 МГц, производительность рассматриваемых алгоритмов составит:

ГОСТ 28147–89 – $(5 \times 10^8 / 129) \times 64$ бит/с $= 248{,}1 \times 10^6$ бит/с $= 31{,}0$ Мбайт/с;

Belt_seq – $(5 \times 10^8 / 168) \times 64$ бит/с $= 190{,}5 \times 10^6$ бит/с $= 23{,}8$ Мбайт/с;

Belt_par – $(5 \times 10^8 / 106) \times 64$ бит/с $= 301{,}9 \times 10^6$ бит/с $= 37{,}7$ Мбайт/с;

AES_seq – $(5 \times 10^8 / 378) \times 64$ бит/с $= 84{,}7 \times 10^6$ бит/с $= 10{,}6$ Мбайт/с;

AES_par – $(5 \times 10^8 / 49) \times 64$ бит/с $= 652{,}8 \times 10^6$ бит/с $= 81{,}6$ Мбайт/с.

Заключение

В результате проведенных исследований определены объемно-временные характеристики рассматриваемых алгоритмов, что позволяет установить приоритетность алгоритмов по различным показателям, провести анализ, сравнение и выбор лучшего алгоритма в соответствии с требованиями конкретной ситуации. Установлено, что по объему требуемого для реализации оборудования алгоритмы располагаются следующим образом (в порядке возрастания): ГОСТ 28147–89, Belt_par, AES_par. Алгоритм Belt несколько превосходит ГОСТ 28147–89, но разница невелика и фактически для реализации этих алгоритмов может быть использована микросхема одного типа.

По производительности алгоритм Belt_par на 21 %, а алгоритм AES_par на 263 % превышают ГОСТ 28147–89. Эти результаты хорошо согласуются с оценками, сделанными в работе [8].

Учитывая, что стоимость микросхем и элементов памяти в настоящее время невелика, в тех случаях, когда требуется высокая скорость шифрования, приоритет имеет алгоритм AES_par, обеспечивающий наибольшую производительность.

Список литературы

1. Data Encryption Standard. National Bureau of Standards (U.S.) / Federal Information Processing Standards Publication 46 // National Technical Information Service. – Springfield, VA, 1977.

2. Advanced Encryption Standard (AES) // National Institute of Standarts and Technology [Electronic resource]. – 2001. – Mode of access : http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. – Date of access : 20.10.2010.

3. Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности : Предварительный государственный стандарт Республики Беларусь СТБ П 34.101.31–2007. – Минск : Госстандарт, 2007. – 10 с.

4. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования : ГОСТ 28147–89. – М. : Изд-во стандартов, 1989. – 23 с.

5. Пудовченко, Ю.Е. Когда наступит время подбирать ключи / Ю.Е. Пудовченко // Конфидент. Защита информации. – 1998. – № 3. – С. 65–71.

6. Файстель, Х. Криптография и компьютерная безопасность / Х. Файстель ; пер с англ. А. Винокурова // Страничка классических блочных шифров [Электронный ресурс]. – Режим доступа : http://www.enlight.ru/crypto/. – Дата доступа : 22.09.2010.

7. Информационная технология. Криптографическая защита информации. Функция хэширования : ГОСТ Р 34.11–94. – М. : Изд-во стандартов, 1994. – 14 с.

8. Винокуров, А. Сравнение стандарта шифрования РФ и нового стандарта шифрования США / А. Винокуров, Э. Применко [Электронный ресурс]. – 2002. – Режим доступа : http://www.enlight.ru/crypto. – Дата доступа : 20.05.2010.

Поступила 28.07.10

Объединенный институт проблем
информатики НАН Беларуси,
Минск, Сурганова, 6
e-mail: labnet@newman.bas-net.by

A.S. Poljakov, V.E. Samsonov

HARDWARE IMPLEMENTATION PERFORMANCES OF SOME SYMMETRIC ENCRYPTION ALGORITHMS

Hardware implementation capabilities of three up-to-date symmetric encryption algorithms including All-Union standard 28147-89, AES, and Belt are analyzed. The basic performance characteristics of the algorithms obtained as a result of logic simulation of their draft versions developed in a XILINX ISE 8i design system with FPGA microchip basis are given.