УДК 681.324 .067

А.С. Поляков, В.Е. Самсонов

ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК АППАРАТНОЙ РЕАЛИЗАЦИИ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ СТБ 34.101.31–2011

Приводятся данные о быстродействии и требуемых объемах оборудования при аппаратной реализации в базисе микросхем типа FPGA криптографических алгоритмов национального стандарта Республики Беларусь СТБ 34.101.31–2011. Рассматриваются результаты реализации алгоритмов на платформе микросхем семейств Spartan 3 и Virtex 4.

Введение

Защита информации от несанкционированного доступа является одной из важнейших проблем информационного взаимодействия пользователей вычислительных сетей. Применяемые для ее решения современные открытые симметричные алгоритмы шифрования, к которым относятся и алгоритмы СТБ 34.101.31–2011 [1], требуют выполнения большого количества вычислительных операций, поэтому их реализация на ЭВМ с помощью программ занимает длительное время. Во многих приложениях такие временные характеристики алгоритмов шифрования неприемлемы, поэтому имеется потребность в поиске скоростных вариантов их выполнения.

В настоящее время общепризнано, что эффективным способом повышения быстродействия алгоритмов является их аппаратная реализация на базе современных информационных технологий. Наиболее перспективным направлением аппаратной реализации, по мнению авторов, является применение современных СБИС типа FPGA (Field Programmable Gate Array, в русском наименовании СБИС этого класса часто называют *программируемыми пользователями вентильными матрицами*), позволяющих использовать одну и ту же микросхему для выполнения различных алгоритмов, последовательно загружая «программу» (специально сгенерированный битовый файл) очередного алгоритма на место предыдущего. Таким образом, на одной и той же микросхеме можно выполнять несколько алгоритмов шифрования, выбирая из них наиболее подходящий по характеристикам для требуемых условий обеспечения конфиденциальности передаваемых сообщений. Для исследования характеристик аппаратных реализаций алгоритмов шифрования выбраны микросхемы типа FPGA серий Spartan 3 и Virtex 4 [2–4].

1. Краткие описания исследуемых криптографических алгоритмов

Криптографические алгоритмы СТБ 34.101.31–2011 относятся к разряду блочных симметричных алгоритмов. Они рассчитаны на шифрование блоков данных размером 128 бит с помощью ключей длиной 256 бит. Стандарт предусматривает шифрование в нескольких режимах. Базовым для всех режимов является алгоритм шифрования 128-битового блока, предусматривающий выполнение восьми раундов шифрования, на каждом из которых используются 32-битовые ключи, сформированные из исходного 256-битового ключа. При шифровании производятся базовые операции: арифметическое сложение и вычитание, сложение по модулю два, сдвиг, циклический сдвиг, подстановка, конкатенация.

В настоящей работе проводилось исследование криптографических алгоритмов:

1 – шифрование блока, Belt;
2 – шифрование в режиме простой замены, Belt_pz;
3 – шифрование в режиме сцепления блоков, Belt_s_bl;
4 – шифрование в режиме гаммирования с обратной связью, Belt_gam;
5 – шифрование в режиме счетчика, Belt_s;
6 – выработка имитовставки, Belt_imit;
7 – шифрование и имитозащита данных, Belt_e_im;
8 – шифрование и имитозащита ключа, Belt_ed_imkey.

Алгоритмы 1–5 необходимы для обеспечения конфиденциальности сообщений. В каждом из них предусмотрены процедуры как зашифрования, так и расшифрования сообщений. Абоненты сети, располагающие общим ключом, могут организовать конфиденциальный обмен сообщениями путем их зашифрования перед отправкой и расшифрования после получения.

Алгоритм 6 предназначен для контроля целостности сообщений с помощью имитовставок – контрольных слов, которые определяются по исходному тексту сообщения с использованием ключа. Абоненты, располагающие общим ключом, могут организовать контроль целостности при обмене сообщениями путем добавления к ним имитовставок при отправке и проверке имитовставок при получении. Проверка имитовставок позволяет получателю сообщения дополнительно убедиться в том, что отправитель сообщения знает ключ, т. е. позволяет проверить подлинность сообщений.

Алгоритм 7 рекомендуется применять для защиты ключей шифрования. При установке защиты ключ зашифровывается вместе со своим заголовком и формируется слово, которое является одновременно защищенным ключом и имитовставкой ключа.

Алгоритм 8 предназначен для вычисления хэш-функций – контрольных слов, которые определяются без использования ключа шифрования.

2. Цель и метод исследования криптографических алгоритмов

Целью исследования являлось определение основных характеристик (временных – быстродействия и объемных – требуемого количества оборудования) указанных выше криптографических алгоритмов при их аппаратной реализации на микросхемах типа FPGA.

В качестве метода исследования использовалось моделирование проектов, реализующих рассматриваемые криптографические алгоритмы:

1) для каждого из перечисленных выше алгоритмов с помощью системы проектирования XILINX Ise 9.2i разрабатывался проект в базисе микросхем типа FPGA. При этом использовались как библиотечные элементы системы, так и элементы, сгенерированные с помощью имеющегося в системе блока Core Generator. Предпочтение отдавалось комбинационным схемам как наиболее быстродействующим, а для управления процессом выполнения алгоритма применялись синхронные автоматы, написанные на языке VHDL;

2) производились отладка проектов и проверка правильности реализации алгоритмов, для чего использовались тестовые примеры, приведенные в приложении к стандарту;

3) с помощью системы XILINX выполнялись этапы синтеза (Synthesize) и имплементации (Translate, Map, Place&Route) проектов, в результате чего были получены объемные характеристики – данные о количестве оборудования, необходимого для аппаратной реализации алгоритмов;

4) с помощью системы моделирования ModelSim 6.2f производилось логическое моделирование проектов, в результате которого определялись скоростные (временные) характеристики алгоритмов, поскольку логическое моделирование позволяет получить сведения о количестве синхротактов, необходимых для выполнения как отдельных этапов алгоритма, так и алгоритма в целом.

3. Объемные характеристики алгоритмов

Достаточно полную информацию о количестве оборудования, требуемого для аппаратной реализации алгоритма, можно получить с помощью опции Synthesize. После выполнения этого этапа система проектирования выдает информацию о количестве базовых элементов (Slice, LUT, RAM), мультиплексоров, регистров, элементов памяти, используемых входных контактов микросхемы и т. п. На следующих этапах в результате оптимизации размещения элементов и соединений между ними количество используемых элементов микросхемы, как правило, уменьшается. Поэтому в качестве оценки количества (объема) требуемого оборудования использовались результаты этапа Synthesize.

Для получения сравнительных оценок в случае реализации алгоритмов на различных микросхемах моделирование проектов было выполнено для двух типов микросхем – Spartan 3 и

Virtex 4. Полученные результаты представлены в табл. 1 и 2 соответственно, где указаны абсолютные значения показателей, а в скобках приведено процентное соотношение требуемых затрат оборудования к объему оборудования, имеющемуся в микросхемах.

Таблица 1

Объемные характеристики алгоритмов (микросхема xc3s1500-5fg676)

Номер алгоритма	Наименование алгоритма	Количество аппаратуры			
		Slice	Триггеры	4 Input LUTs	BRAM
1	Belt	973 (7,3 %)	463 (1,8 %)	1814 (6,9 %)	28 (87,5 %)
2	Belt_pz	1172 (8,8 %)	606 (2,3 %)	2115 (8,0 %)	28 (87,5 %)
3	Belt_s_bl	1478 (11,1 %)	797 (3,0 %)	2586 (9,7 %)	28 (87,5 %)
4	Belt_gam	1244 (9,4 %)	793 (3,0 %)	2151 (8,1 %)	28 (87,5 %)
5	Belt_s	1303 (9,8 %)	918 (3,5 %)	2329 (8,8 %)	28 (87,5 %)
6	Belt_imit	1483 (11,2 %)	1178 (4,5 %)	2624 (10 %)	28 (87,5 %)
7	Belt_e_im	9886 (75 %)	1498 (5,7 %)	17454 (65,6 %)	28 (87,5 %)
8	Belt_ed_imkey	1835 (13,8 %)	1311 (5,0 %)	3349 (12,6 %)	28 (87,5 %)

Таблица 2

Объемные характеристики алгоритмов (микросхема xc4vlx15-12ff668)

Номер алгоритма	Наименование алгоритма	Количество аппаратуры			
		Slice	Триггеры	4 Input LUTs	BRAM
1	Belt	936 (15,3 %)	174 (1,4 %)	1755 (14,3 %)	28 (59 %)
2	Belt_pz	1194 (19,5 %)	629 (5,2 %)	2088 (17,0 %)	28 (59 %)
3	Belt_s_bl	1499 (24,4 %)	796 (6,5 %)	2622 (21,4 %)	28 (59 %)
4	Belt_gam	1275 (20,8 %)	792 (6,5 %)	2189 (17,9 %)	28 (59 %)
5	Belt_s	1343 (21,9 %)	917 (7,5 %)	2351 (19,2 %)	28 (59 %)
6	Belt_imit	1377 (22,5 %)	1176 (9,6 %)	2339 (19,1 %)	28 (59 %)
7	Belt_e_im	9843 (160 %)	1498 (12,2 %)	17315 (141 %)	28 (59 %)
8	Belt_ed_imkey	1883 (30,7 %)	1310 (10,7 %)	3384 (27,6 %)	28 (59 %)

Примечание к табл. 1 и 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 2 Кбит.

Для правильного понимания представленных результатов необходимо учитывать следующее:

1. Во всех исследуемых алгоритмах в качестве базового (т. е. осуществляющего операции шифрования блоков данных) использовался алгоритм Belt. Поэтому и затраты оборудования на реализацию представленных алгоритмов незначительно отличаются от затрат на реализацию базового алгоритма Belt (за исключением алгоритмов Belt_e_im и Belt_ed_imkey).

2. В данном исследовании проекты аппаратной реализации алгоритмов шифрования разрабатывались с ориентацией только на выполнение тестов, представленных в приложении к стандарту. Естественно, при этом не предусматривались те операции, которые обязательно будут присутствовать при практическом применении алгоритмов шифрования. Имеются в виду операции по вводу данных в микросхему и выводу результатов в компьютер; операции проверки количества блоков данных в передаваемом сообщении, проверки появления последнего блока данных и полноты последнего блока данных. Соответственно при практической реализации алгоритмов шифрования могут увеличиться затраты оборудования на хранение исходных данных и результатов шифрования, организацию указанных выше проверок, пересылок информации и т. п.

4. Временные характеристики алгоритмов

Основным показателем быстродействия блочного симметричного криптографического алгоритма является время обработки (зашифрования или расшифрования) одного блока данных (в рассматриваемом стандарте равного 128 битам). Выше было отмечено, что с помощью логического проектирования получены данные о числе тактов, затрачиваемых на выполнение исследуемого алгоритма или его отдельных этапов. Располагая такими сведениями, можно легко определить быстродействие или производительность алгоритма, разделив значение частоты работы микросхемы на число синхротактов, необходимых для выполнения конкретного алгоритма.

Заметим, что исследуемые алгоритмы отличаются по структуре и содержанию выполняемых операций. В частности, алгоритмы 2–4 в качестве базового имеют алгоритм Belt, поэтому их быстродействие равно быстродействию базового алгоритма Belt. Алгоритмы Belt_s и Belt_imit не содержат в себе базового алгоритма, поэтому их временные характеристики значительно отличаются от характеристик алгоритмов 1–4.

Для алгоритмов 1–4 выполнение операции шифрования занимает 216 синхротактов. Алгоритм Belt_s требует для получения первого зашифрованного блока данных 438 тактов, а для шифрования последующих блоков данных – такое же количество тактов, как и алгоритмы 1–4. Алгоритм 6 выработки имитовставки выполняется за 872 синхротакта.

Результаты моделирования алгоритмов шифрования представлены в табл. 3.

Таблица 3

Временные характеристики алгоритмов шифрования

Номер алгоритма	Название алгоритма	Количество тактов, необходимое для шифрования одного блока данных
1	Belt	216
2	Belt_pz	
3	Belt_s_bl	
4	Belt_gam	218
5	Belt_s	438
6	Belt_imit	218 + 218 x n (n – число блоков данных)
7	Belt_e_im	218 (для шифрования одного блока данных) 1959 (для выработки имитовставки)
8	Belt_ed_imkey	1328

Используя данные табл. 1 и 2, можно вычислить быстродействие рассматриваемых алгоритмов шифрования. Например, для алгоритма Belt быстродействие определяется делением скоростных характеристик используемой микросхемы на число тактов, необходимых для выполнения алгоритма. Если для реализации выбрать микросхему с частотой 100 МГц, то быстродействие алгоритма Belt вычисляется следующим образом: 100 МГц : 216 тактов = = 462 962 блока/с или 7,4 Мбайт/с.

Заключение

Поскольку все алгоритмы шифрования СТБ 34.101.31–2011 используют в качестве базового алгоритма Belt (шифрование блока данных), то и характеристики быстродействия для них практически одинаковы, что подтверждается данными табл. 3.

Анализ табл. 1 и 2 показывает, что объем оборудования для реализации отличительных операций в каждом из алгоритмов невелик (за исключением алгоритма Belt_e_im, в котором выработка имитовставки производится за 1989 тактов), основные затраты оборудования приходятся на реализацию базового алгоритма Belt. Поскольку используется небольшая часть возможностей микросхем (7 – 11 % для микросхемы xc3s1500-5fg676 и 15 – 24 % для микросхемы xc4vlx15-12ff668), то в одной микросхеме можно разместить несколько алгоритмов шифрования и выбрать тот, который более всего подходит для использования в конкретной ситуации.

Список литературы

1. Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности : СТБ 34.101.31–2011. – Введ. 31.01.2011. – Минск : Госстандарт, 2011. – 31 с.

2. Кузелин, М.О. Современные семейства ПЛИС фирмы Xisinx : справочное пособие / М.О. Кузелин, Д.А. Кнышев, В.Ю. Зотов. – М. : Горячая линия – Телеком, 2004. – 440 с.

3. Spartan-3. FPGA Family Data Sheet: DC and Switching Characteristics [Electronic resource]. – Mode of access : www.xilinx.com/support/documentation/data_sheets/099.pdf. – Date of access : 12.08.2013.

4. Virtex-4. FPGA Family Data Sheet: DC and Switching Characteristics [Electronic resource]. – Mode of access : www.xisinx.com/support/documentation/data_sheets/ds302.pdf. – Date of access : 12.08.2013.

Поступила 5.09.2013

Объединенный институт проблем информатики НАН Беларуси,
Минск, Сурганова, 6
e-mail: sveby@mail.ru
alexpolja@tut.by

A.S. Poljakov, V.E. Samsonov

EVALUATING TIME AND VOLUME CHARACTERISTICS OF HARDWARE IMPLEMENTATION OF CRYPTOGRAPHIC ALGORITHMS IN STANDARD STB 34.101.31–2011

Processing time and hardware requirements of hardware implementation of 8 algorithms of national standard of the Republic Belarus based on FPGA microchips are provided. The results of algorithms implementation on the platform of Spartan 3 and Virtex 4 microcircuits are considered.