ЗАЩИТА ИНФОРМАЦИИ

УДК 681.324 .067

А.С. Поляков, В.Е. Самсонов

АНАЛИЗ ВОЗМОЖНОСТЕЙ АЛГОРИТМОВ МЕЖДУНАРОДНОГО СТАНДАРТА «ОБЛЕГЧЕННАЯ КРИПТОГРАФИЯ» – ISO/IEC 29192-2:2012

Приводятся данные о характеристиках алгоритмов международного стандарта «Облегченная (легковесная) криптография» при их аппаратной реализации в базисе микросхем типа FPGA. Дается сравнение характеристик этих алгоритмов с характеристиками нескольких широко используемых стандартных алгоритмов шифрования и оцениваются возможности алгоритмов легковесной криптографии.

Введение

В 2007 г. коллектив авторов [1] представил алгоритм шифрования под интригующим названием «ультралегкий», имея в виду, что алгоритм обладает высокой производительностью (быстродействием), сравнительно неплохой криптостойкостью в сравнении с используемыми стандартными алгоритмами, а главное – требует небольших затрат (т. е. является ультралегким) при его аппаратной реализации.

Немного позже, в 2009 г., Аксель Пошманн в своей работе [2] привел аргументацию и обоснование необходимости развития направления «облегченная криптография» с учетом повсеместного и бурного развития компьютеризации всех аспектов жизнедеятельности общества: с одной стороны, внедрения компьютерных технологий в широкие сферы социальной жизни, характеризующегося требованием реализации функций шифрования с использованием малых объемов ресурсов (памяти, логических элементов и т. п.); с другой стороны, обеспечения необходимой защиты информации пользователей открытых сетей типа Интернет от несанкционированного доступа.

К облегченной криптографии относятся алгоритмы, разрабатываемые специально для устройств с ограниченными или крайне малыми ресурсами [3, 4]. Общим свойством таких алгоритмов являются низкие требования:

– к требуемой площади кристалла, на котором алгоритм может быть аппаратно реализован;

– вычислительной мощности микропроцессора, на котором выполняются вычисления;

– оперативной памяти вычислительного устройства и т. п.

Видимо, проблема перехода, по крайней мере в отдельных областях применения криптографической защиты данных, к малоресурсным (в смысле высказанных выше требований) алгоритмам шифрования созрела настолько, что организации ISO и IEC очень быстро приняли и утвердили в 2012 г. международный стандарт «Lightweight Cryptography» [5], в русскоязычном переводе – «Облегченная (легковесная) криптография».

К настоящему времени уже разработано много алгоритмов, относящихся к облегченной криптографии. Некоторые их них рассмотрены в работе [4]. В данной статье внимание будет уделено двум алгоритмам, включенным в стандарт [5]:

PRESENT – блочный шифр с размером блока данных 64 бита и размером ключа 80 бит – PRESENT-80 или размером ключа 128 бит – PRESENT-128;

CLEFIA – блочный шифр с размером блока данных 128 бит и размерами ключей шифрования 128, 192 или 256 бит – CLEFIA-128, CLEFIA-192, CLEFIA-256 соответственно.

Данные алгоритмы, основанные на концепции малых затрат ресурсов на их реализацию и получение высокого быстродействия, вызывают повышенный интерес специалистов в части соответствия продекларированных и реальных характеристик этих алгоритмов, а также сравнения их с широко применяемыми на практике стандартными криптографическими алгоритмами. Имеются исследования (см., например, [6]), которые показывают, что при реализации на неко-

торых аппаратных платформах алгоритмы PRESENT и CLEFIA по производительности уступают алгоритму AES.

Поскольку рассматриваемые алгоритмы изначально были ориентированы на аппаратную реализацию, в данной работе исследованы их основные характеристики: быстродействие (временные) и сложность реализации (объемные), а также проведено сравнение с характеристиками некоторых широко применяемых стандартных алгоритмов при их реализации в базисе микросхем типа FPGA.

1. Краткое описание исследуемых алгоритмов

Авторы алгоритма *PRESENT* подчеркивают, что разработали его для узкоспециальных применений, для которых не подходит более универсальный, но и более ресурсоемкий алгоритм AES. По их мнению, алгоритм PRESENT рассчитан на аппаратную реализацию и его предлагается применять прежде всего в микрочипах в тех случаях, когда требуются низкие затраты ресурсов и допускаются пониженные требования к криптографической стойкости шифра.

Алгоритм PRESENT включает два алгоритма: PRESENT-80 и PRESENT-128, которые по составу операций и порядку их применения идентичны. Разница заключается лишь в том, что в алгоритме PRESENT-80 раундовый ключ длиной 64 бита формируется с помощью соответствующих операций из первоначально заданного образующего ключа длиной 80 бит, а в алгоритме PRESENT-128 в качестве образующего используется ключ длиной 128 бит. Правила формирования раундовых ключей в алгоритмах немного отличаются, но при этом используется одинаковый набор операций.

Алгоритм PRESENT основан на принципе SP-сети и предусматривает выполнение 31 раунда шифрования. Перед выполнением операции шифрования данных производится процедура генерации 32 64-битовых раундовых ключей.

Шифрование блока данных длиной 64 бита выполняется за 31 раунд, на каждом из которых производятся следующие операции:

– сложение по mod 2 текущего состояния блока данных с очередным раундовым ключом;

– преобразование усложнения, состоящее в замене полубайтов блока данных соответствующими значениями четырехбитовых S-блоков подстановки;

– перемешивающее преобразование, предусматривающее перестановку значений битов в текущем состоянии блока данных в соответствии с заданными правилами;

– завершающая операция – сложение по mod 2 результата, полученного после выполнения 31-го раунда алгоритма, с последним раундовым ключом.

Алгоритм *CLEFIA* разработан корпорацией Sony [7], является симметричным блочным шифром и соответствует требованиям к шифру AES [8]: размер блока – 128 бит, поддерживаемые длины ключей шифрования – 128, 192 и 256 битов, что соответствует алгоритмам CLEFIA-128, CLEFIA-192, CLEFIA-256. Число раундов зависит от длины ключа и равно 18, 22, 26 соответственно.

Структура алгоритма представляет собой обобщенную сеть Фейстеля и предусматривает выполнение следующих операций:

1) при генерации раундовых ключей используется заданный начальный ключ шифрования и специальная таблица 32-битовых констант. В зависимости от размера заданного начального ключа – 128, 192 или 256 битов – создается массив 32-битовых раундовых ключей в количестве 36, 44 или 52 ключа соответственно;

2) для алгоритма CLEFIA-128 блок данных и исходный ключ шифрования разделяются на четыре 32-разрядных слова, которые обрабатываются в течение 18 раундов с помощью функций F_0 и F_1, предусматривающих выполнение следующих операций: суммирование по mod 2 слова блока данных с очередным раундовым ключом, подстановка байтов полученного результата с использованием соответственно таблиц S_0 и S_1; умножение двух полиномов степени меньше 8, вычисление модуля результата умножения полиномов по неприводимому полиному $z^8 + z^4 + z^3 + + z^2 + 1$. При выполнении очередного раунда i используются раундовые ключи с номерами $(2i – 1)$ и $2i$.

Особенностью алгоритма CLEFIA является использование операции «отбеливание»: перед выполнением первого раунда алгоритма второе и четвертое слова блока данных суммируются по mod 2 со вторым и четвертым словами исходного ключа, а после выполнения последнего раунда полученные результаты шифрования, соответствующие первому и третьему словам блока данных, суммируются по mod 2 с первым и третьим словами исходного ключа соответственно.

Из множества алгоритмов CLEFIA исследование характеристик проводилось только для самого простого варианта – CLEFIA-128, поскольку на основании изучения описания алгоритмов CLEFIA-192 и CLEFIA-256 был сделан вывод о нецелесообразности проведения их исследований в связи с повышенной сложностью этих алгоритмов в сравнении с алгоритмом CLEFIA-128.

2. Объемно-временные характеристики алгоритмов PRESENT и CLEFIA

Анализ показателей аппаратной реализации рассматриваемых алгоритмов производился следующим образом: для каждого из алгоритмов с помощью системы проектирования фирмы XILINX были разработаны реализующие их проекты в базисе микросхем типа FPGA, затем произведено выполнение проектов (этапы Synthesize, Translate, Map), в результате чего получены данные о количестве (объеме) оборудования, необходимого для реализации рассматриваемых алгоритмов.

С помощью моделирующей системы ModelSim производилось логическое моделирование разработанных проектов, результаты которого позволили определить количество тактов, необходимых для шифрования одного блока информации каждым из алгоритмов. Логическое моделирование позволило также проверить правильность реализации алгоритмов, для чего использовались тестовые примеры, приведенные в приложении к стандарту [5].

Объемные характеристики аппаратной реализации алгоритмов PRESENT-80, PRESENT-128 и CLEFIA-128 в базисе микросхем типа FPGA серий Spartan 3 и Virtex 4 представлены в табл. 1, в которой указаны абсолютные значения показателей характеристик, а в скобках приведено процентное соотношение количества требуемых элементов оборудования к количеству оборудования, имеющегося в соответствующих микросхемах.

Таблица 1

Объемные характеристики алгоритмов PRESENT-80, PRESENT-128, CLEFIA-128

Характеристика	Тип и серия микросхемы					
	Spartan 3, xc3s2000-4fg456			Virtex 4, xc4vlx15-10sf363		
	PRESENT-80	PRESENT-128	CLEFIA-128	PRESENT-80	PRESENT-128	CLEFIA-128
Slice	146 (0,8 %)	316 (1,6 %)	2061 (10 %)	147 (2,4 %)	316 (5,0 %)	2081 (34%)
Триггеры	227 (0,6 %)	275 (0,7 %)	1964 (4,8 %)	227 (1,9 %)	275 (2,3 %)	1967 (16%)
Четырехвходовой LUT	292 (0,7 %)	341 (0,9 %)	2712 (6,7 %)	293 (2,4 %)	341 (2,6 %)	2743 (22%)
BRAM	35 (88 %)	36 (90 %)	18 (45 %)	35 (73 %)	36 (75 %)	18 (38%)

Примечание: 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.

3. Сравнение характеристик алгоритмов PRESENT и CLEFIA с характеристиками стандартных алгоритмов

Считается, что PRESENT является одним из самых компактных криптоалгоритмов, существует оценка, что для его аппаратной реализации требуется приблизительно в 2,5 раза меньше логических элементов, чем для AES или CLEFIA [4].

Для сравнения характеристик были выбраны известные и широко применяемые стандартные алгоритмы: AES [8], ГОСТ 28147-89 [9] и алгоритм Belt [10], недавно введенный в действие в качестве стандарта Республики Беларусь [11]. Выбор этих алгоритмов обусловлен следующим:

– ГОСТ 28127-89, имеющий размер ключа 256 бит, считается одним из самых криптостойких алгоритмов шифрования [12] и используется во многих странах СНГ;

– AES (Advanced Encryption Standard) является стандартом шифрования США, выбранным в результате конкурса из множества алгоритмов как наиболее соответствующий современным требованиям к криптографическим алгоритмам и широко используемый во многих странах мира;

– алгоритм Belt с размером ключа 256 бит представляет интерес для сравнения в качестве нового современного алгоритма шифрования, имеющего высокую криптоскойкость.

Данные по объему оборудования и быстродействию алгоритмов PRESENT-80, PRESENT-128, CLEFIA-128 и сравниваемых с ними стандартных алгоритмов представлены в табл. 2 и 3. При этом использованы результаты исследования характеристик аппаратной реализации стандартных алгоритмов шифрования, приведенные в работе [13].

Таблица 2

Затраты оборудования на реализацию алгоритмов

Алгоритм	Количество Slice	Количество триггеров	Количество четырехвход. LUT	Количество BRAM
ГОСТ 28147-89	349	233	479	9
Belt	1070	302	2050	28
AES-128	2107	504	3461	35
PRESENT-80	146	227	292	35
PRESENT-128	316	275	341	36
CLEFIA-128	2081	1967	2743	18

Таблица 3

Затраты времени на шифрование данных, число тактов

Алгоритм	Размер блока данных, бит	Количество тактов на один блок данных	Количество тактов на блок данных размером 64 бита
ГОСТ 28147-89	64	129	129
Belt	128	211	106
AES-128	128	97	49
PRESENT-80	64	97	97
PRESENT-128	64	97	97
CLEFIA-128	128	419	210

При оценке и сравнении показателей характеристик алгоритмов, приведенных в табл. 2 и 3, следует учитывать, что проекты всех алгоритмов были реализованы на одинаковом аппаратном базисе – микросхемах типа FPGA серий Spartan 3 и Virtex 4, все проекты были максимально оптимизированы (насколько это удалось авторам) путем распараллеливания всех операций, допускающих распараллеливание. Поэтому можно считать, что сравнение показателей характеристик алгоритмов производится корректно.

В табл. 3 не приведены данные о затратах времени на подготовку раундовых ключей, которые составляют:

ГОСТ 28147-89 – подготовка раундовых ключей не требуется;
AES-128 – 210 тактов;
PRESENT-80 – 130 тактов;
PRESENT-128 – 130 тактов;
CLEFIA-128 – 460 тактов.

Belt – дополнительное время на подготовку раундовых ключей не требовалось, так как в представленном в табл. 2 и 3 варианте реализации алгоритма Belt подготовка ключей для по-

следующего раунда производилась одновременно (параллельно) с выполнением очередного раунда шифрования.

Затраты времени на шифрование блока данных алгоритмами PRESENT-80 и PRESENT-128 одинаковы, а затраты на оборудование отличаются. Это объясняется тем, что подготовка 64-битовых раундовых ключей в алгоритме PRESENT-80 производится с использованием начального ключа размером 80 бит, а в алгоритме PRESENT-128 начальный ключ имеет размер 128 бит, что потребовало дополнительных затрат аппаратных ресурсов.

Заключение

Из табл. 1 видно, что микросхемы типа FPGA для реализации алгоритмов PRESENT, исходя из экономических критериев, не совсем пригодны, поскольку при незначительных затратах логических элементов на реализацию алгоритмов требуются большие объемы памяти, которые в дешевых микросхемах типа FPGA отсутствуют.

Анализ табл. 2 показывает, что для реализации алгоритмов PRESENT-80 и PRESENT-128 требуется не намного меньше оборудования, чем для сравниваемых стандартных алгоритмов, но зато необходимо значительно больше элементов памяти.

По быстродействию алгоритмы PRESENT лишь немного превосходят алгоритмы Belt и ГОСТ 28147-89, но вдвое уступают алгоритму AES-128.

Возможно, что на других аппаратных платформах алгоритмы PRESENT могут иметь значительные преимущества перед обычными криптографическими алгоритмами, но в базисе FPGA они явно неконкурентоспособны.

Анализ характеристик алгоритма CLEFIA-128 и сравниваемых с ним стандартных алгоритмов показывает, что алгоритм CLEFIA-128 по всем показателям (ресурсоемкости, быстродействию) значительно уступает известным стандартным алгоритмам и поэтому ни по каким показателям не может быть отнесен к «облегченным».

Исследование характеристик алгоритмов CLEFIA-192 и CLEFIA-256 не проводилось, поскольку показатели для этих алгоритмов будут значительно хуже, чем у CLEFIA-128, из-за увеличения количества раундов (22 и 26 соответственно вместо 18).

Возможно, что на других аппаратных платформах (например, специально разработанных интегральных схемах), характеристики алгоритмов CLEFIA будут лучше, чем на платформе микросхем типа FPGA, но существенных изменений ожидать не приходится, поскольку и сложность алгоритмов и набор выполняемых операций остаются неизменными при реализации на любой платформе.

Список литературы

1. PRESENT: An ultra-lightweight Block Cipher / A. Bogdanov [et al.] // Proc. of CHES 2007. – Springer-Verlag, 2007. – P. 450–466.

2. Poschmann, A. Lightweight Cryptography – Cryptographic Engineering for a Pervasive World : dissertation for the degree Doktor-Ingenieur Faculty of Electrical Engineering and Information Technology Ruhr-University Bochum, Germany [Electronic resource]. – Mode of access : eprint.iacr/2009/516.pdf. – Date of access : 16.06.2014.

3. Панасенко, С. Облегченные алгоритмы шифрования / С. Панасенко, С. Смагин // Мир ПК. – 2011. – № 7. – С. 50–52.

4. Агафьин, С.С. LW-криптография: шифры для RFID-систем / С.С. Агафьин // Безопасность информационных технологий. – 2011. – № 4.

5. ISO/IEC 29192-2:2012. Information technology – Security techniques – Lightweight Cryptography – Part 2: Block ciphers.

6. Masanobu, Katagi. Lightweight Cryptography for the Internet of Things // Masanobu Katagi, Shibo Moriai [Electronic resource]. – Mode of access : http://www.iab.org/wp-content/IAB-uploads/2011/030Kaftan.pdf. – Date of access : 10.01.2014.

7. The 128-Bit blockcipher CLEFIA / T. Shirai [et al.] // Proceedings of Fast Software Encryption – FSE'07 / ed. A. Biryukov. – Springer-Verlag, 2007. – Vol. 4593. – P. 181–195.

8. Announcing the Advanced Encryption Standard (AES) // Federal Information Processing Standards Publication [Electronic resource]. – Mode of access : http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, http://www.nist.gov/CryptoToolkit. – Date of access : 12.12.2013.

9. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования : ГОСТ 28147-89. – М. : Изд-во стандартов, 1989. – 28 с.

10. Алгоритм шифрования Belt // С.В. Агиевич [и др.]. – Управление защитой информации. – 2002. – № 4. – С. 407–412.

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

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

13. Поляков, А.С. Характеристики аппаратной реализации некоторых симметричных алгоритмов шифрования / А.С. Поляков, В.Е. Самсонов // Информатика. – 2011. – № 1. – С. 89–94.

Поступила 14.05.2014

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

A.S. Poljakov, V.E. Samsonov

ANALYSIS OF THE CHARACTERISTICS OF INTERNATIONAL STANDARD ALGORITHMS «LIGHTWEIGHT CRYPTOGRAPHY» – ISO/IEC 29192-3:2012

The data on the characteristics of international standard algorithms «lightweight cryptography» while application in hardware implementation based on microchips of FPGA are provided. A comparison of the characteristics of these algorithms with the characteristics of several widely-used standard encryption algorithms is made and possibilities of lightweight cryptography algorithms are evaluated.