УДК *004.272, 004.31*

РЕАЛИЗАЦИЯ НА FPGA АЛГОРИТМА ШИФРОВАНИЯ СТБ 34.101.31

М.В. Качинский, А.В.Станкевич, А.И.Шемаров
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье рассматривается реализация алгоритма шифрования блока СТБ 34.101.31 на базе программируемой логической интегральной схемы (ПЛИС) с архитектурой field-programmable gate array (FPGA), обладающая более высокой производительностью по сравнению с известными. Описываются архитектурные особенности реализации. Приводится сравнение аппаратных затрат и производительности предлагаемой реализации с известными решениями.
Ключевые слова: СТБ 34.101.31; алгоритм шифрования блока; реализация на FPGA; итерация; блок данных; ключ; раунд алгоритма; итеративная, конвейерная архитектура процессора; аппаратные ресурсы кристалла FPGA; производительность.

FPGA IMPLEMENTATION OF THE STB 34.101.31 ENCRYPTION ALGORITHM

M.V. Kachinsky, A.V. Stankevich, A.I. Shemarov
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. This article discusses an implementation of the STB 34.101.31 encryption algorithm based on a field-programmable gate array (FPGA) architecture, which offers higher performance than existing solutions. The architectural features of the implementation are described. A comparison of the hardware costs and performance of the proposed implementation with existing solutions is provided.
Keywords: STB 34.101.31; block encryption algorithm; FPGA implementation; iteration; data block; key; algorithm round; iterative, pipelined processor architecture; FPGA hardware resources; performance.

Введение

Алгоритм шифрования блока является базовым алгоритмом СТБ 34.101.31 для различных режимов шифрования, выработки имитовставки и других алгоритмов стандарта. Производительность его реализации будет существенно определять общую производительность реализаций

упомянутых алгоритмов. При необходимости высокопроизводительной реализации алгоритмов стандарта требуется их аппаратная реализация.

Основная часть

СТБ 34.101.31 описывает блочный алгоритм шифрования с размером блока 128 бит и длиной ключа 256 бит. Алгоритм шифрования блока выполняется за 8 раундов, каждый раунд имеет 9 вычислительных шагов.

В результате анализа известных источников были найдены две статьи [1, 2], описывающие реализации на FPGA алгоритма режима простой замены СТБ 34.101.31. В этом режиме исходное сообщение разбивается на блоки по 128 бит, которые поблочно шифруются алгоритмом шифрования блока.

Режим простой замены на практике используется редко из-за повторения зашифрованных значений для одинаковых блоков данных. Для режимов сцепления блоков и гаммирования с обратной связью использование конвейерной архитектуры не эффективно с точки зрения аппаратных затрат в связи с тем, что для шифрования следующего блока необходимо дождаться завершения шифрования предыдущего блока. Поэтому для последующего сравнительного анализа конвейерные реализации [2] рассматривать не будем и выберем наиболее производительную реализацию Belt_par из статьи [1] и последовательную реализацию из статьи [2].

Одним из преобразований алгоритма СТБ 34.101.31 является подстановка, задаваемая таблицей из 256 8-разрядных значений. Для реализации таблицы подстановки проект Belt_par использует блочную память FPGA (RAMB16s), последовательная реализация [2] для этой цели использует распределенную память кристалла FPGA.

Предлагаемая реализация имеет следующие особенности:

Блок памяти (RAMB16 или RAMB18E в зависимости от ПЛИС) сконфигурирован как двухпортовый, что позволяет одновременно и независимо обращаться к каждой ячейке памяти по двум портам. В одном блоке памяти хранится одна таблица подстановки H. За счет независимой адресации к этой таблице по портам A и B с помощью одного блока реализуется две подстановки $H(u_i)$;

Предлагаемая реализация предусматривает максимально возможное распараллеливание шагов алгоритма. Один раунд алгоритма выполняется за 5 тактов. При этом одновременно не будет использоваться более двух преобразований Gr, каждое из которых требует применения 4 таблиц подстановки. Общее число блоков памяти для двух преобразований Gr – 4.

Для доступа к таблицам подстановки на разных шагах алгоритма используются мультиплексоры;

Для уменьшения числа использованных LUT в предлагаемой реализации широко используются трехвходовые сумматоры.

Реализации [1, 2] выполнены на устаревших кристаллах FPGA, которые современная среда проектирования Vivado уже не поддерживает. С целью получения результатов для сравнения были выполнены следующие три варианта предлагаемой реализации (характеристики реализаций после процедур размещения и трассировки кристалла ПЛИС приведены в таблице):

Реализация 1 на базе ПЛИС xc3s400-5-fg456 с использованием среды проектирования ISE 14.7 для сравнения с реализацией Belt_par [1];

Реализация 2 на базе ПЛИС xc6vlx130t-1-ff1156 с использованием среды проектирования ISE 14.7 для сравнения с последовательной реализацией [2];

Реализация 3 на базе современной ПЛИС xcku3p-ffvb676-2-e с использованием среды проектирования Vivado.

Приведенные результаты свидетельствуют о более высокой производительности предложенной реализации по сравнению с известными при относительно небольших аппаратных затратах и реализации как зашифрования, так и расшифрования блока.

Характеристики реализаций алгоритма шифрования блока СТБ 34.101.31
Characteristics of implementations of the STB 34.101.31 block encryption algorithm

Характеристика	Предлагаемая реализация			Belt_par [1]	Последовательная [2]
	1	2	3		
Slice Flip Flops	747	776	748	302	847
LUTs	2065	1357	1304	2050	1173
RAMB	4	4	4	28	-
Количество тактов на один блок данных	43	43	43	211	66
Тактовая частота, МГц	66	133	290	–	112
Производительность, Мбит/с	196	395	863	–	217

Заключение

Предложена реализация алгоритма шифрования блока СТБ 34.101.31 на базе FPGA, обладающая более высокой производительностью по сравнению с известными реализациями при относительно небольших аппаратных затратах. Реализация может быть использована для любых режимов шифрования стандарта.

Список использованных источников

1. Поляков А.С., Самсонов В.Е. (2011) Характеристики аппаратной реализации некоторых симметричных алгоритмов шифрования. *Информатика.* (1), 89-94.

2. Ланкевич Ю. Ю. (2013) Процессор алгоритма шифрования «Belt» на базе ПЛИС. *Материалы международной научной конференции «Информационные технологии и системы* 2013» (ИТС 2013). 190–191.

References

1. Poljakov .A.S., Samsonov V.E. (2011) Hardware implementation performances of some symmetric encryption algorithms. *Informatics*. (1), 89-94.

2. Lankevich Y.Y. (2013) FPGA-based Belt encryption algorithm processor. *Information Technologies and Systems 2013 (ITS 2013). Proceeding of The International Conference*. 190–191.

Сведения об авторах

Качинский М.В., канд. техн. наук, доц., доцент кафедры встраиваемых вычислительных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», kachinsky@bsuir.by.

Станкевич А.В., канд. техн. наук, доц., доцент кафедры встраиваемых вычислительных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», stankevich@bsuir.by.

Шемаров А.И., канд. техн. наук, доц., доцент кафедры встраиваемых вычислительных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», shemarov@bsuir.by.

Information about the authors

Kachinsky M., Ph.D. in Computer Sciences, Associate Professor, department of electrical engineering, Educational Institution "Belarusian State University of Informatics and Radioelectronics", kachinsky@bsuir.by

Stankevich A., Ph.D. in Computer Sciences, Associate Professor, department of electrical engineering, Educational Institution "Belarusian State University of Informatics and Radioelectronics", stankevich@bsuir.by.

Shemarov A., Ph.D. in Computer Sciences, Associate Professor, department of electrical engineering, Educational Institution "Belarusian State University of Informatics and Radioelectronics", shemarov@bsuir.by