энергии и тепла, предприятиям энергетического и общего машиностроения, а также высокого уровня технического образования населения. [2]

Для продвижения темы жидкого моторного биотоплива сегодня необходима, с одной стороны, государственная политика в этом направлении. С другой стороны, инвестиции в данное направление.

Спрос на Западе есть, следовательно, необходимо убедить западных инвесторов, что вкладывать деньги в подобные технологии в Беларуси – безопасно и перспективно.

Литература

1. Биотопливо – проблемы и перспективы// Авто Релиз [Электронный ресурс] – Режим доступа: http://autorelease.ru/articles/automobile/345-biotoplivo-problemy-i-perspektivy.html- Дата доступа 20.05.2013
2. Потенциал использования биомассы в Беларуси// Электронные артикулы [Электронный ресурс] – Режим доступа: http://www.technopark.by/files/esco-article-bio.doc - Дата доступа 20.05.2013
3. Биотопливо: мировой опыт госрегулирования// Электронный ресурс] – Режим доступа: http://www.newchemistry.ru/printletter.php?n_id=692 - Дата доступа 20.05.2013

ПОСЛЕДОВАТЕЛЬНЫЙ ПРОЦЕССОР АЛГОРИТМА ШИФРОВАНИЯ AES НА БАЗЕ FPGA

***А.С. ШАШКОВ*, А.В. СТАНКЕВИЧ**

This article describes the design of the AES-128 encryption and decryption algorithm processor. The design is written in VHDL and is implemented in such FPGA chips as Xilinx Virtex 5,6,7 and Spartan 6. The goal of the work was to build an iterative AES IP-core that is optimized for maximum encryption and decryption bandwidth. Several different designs were implemented and compared. The best designs were able to perform on a par with the best commercial and open-source solutions that are openly available. Thorough analysis of different AES-processor structures described in the work can be of use for the designs with various optimization criteria

Ключевые слова: AES, FPGA, VHDL, processor, encryption

В ходе работы был разработан процессор зашифрования и расшифрования алгоритма AES-128 для различных ПЛИС фирмы Xilinx.

Изначально были спроектированы несколько модификаций процессора, осуществляющего только режим зашифрования. Так, были получены модификации 11-тактового процессора зашифрования, 10-тактового процессора зашифрования, процессора зашифрования на базе T-таблиц, 11-тактового процессора зашифрования с синхронной памятью раундовых ключей, а также модификации данных процессоров с использованием блочной памяти. По результатам процедуры размещения и трассировки на кристалле Virtex 5 была найдены две самые быстрые и эффективные по соотношению «производительность на затраченные ресурсы» версии процессора зашифрования: 11-тактовая модификация процессора и 11-тактовая модификация процессора зашифрования с синхронной памятью ключей.

На базе двух этих модификаций были разработаны две модификации процессора, осуществляющего как процедуру зашифрования, так и процедуру расшифрования. По результатам размещения и трассировки на кристалле Virtex 5 было установлено, что наибольшей производительностью и эффективностью по соотношению «производительность на затраченные ресурсы» обладает версия процессора зашифрования и расшифрования на базе 11-тактового процессора зашифрования с синхронной памятью ключей. Эта модификация и была выбрана в качестве результата проектирования процессора зашифрования и расшифрования с максимальной производительностью при минимальных ресурсах.

Для лучших по показателю быстродействия процессоров зашифрования и зашифрования/расшифрования была проведена процедура размещения и трассировки для кристаллов Xilinx Virtex 5, 6 и 7, а также для Spartan 6. Лучший полученный процессор зашифрования имеет пропускную способность свыше 4 гигабит в секунду, а лучший разработанный процессор зашифрования и расшифрования имеет пропускную способность свыше 3 гигабит в секунду для кристаллов Virtex 5, 6, 7. Полученная пропускная способность позволяет данным разработкам получить применение в быстродействующих системах передачи и хранения данных. Полученные характеристики сравнимы с характеристиками аналогичных разработок.

Можно заключить, что все представленные в работе модификации процессоров могут представлять определённый интерес в зависимости от специфики конкретного приложения.

Литература

1. Advanced Encryption Standard (AES) (FIPS PUB 197) [Электронный ресурс] : Federal Information Processing Standard / National Institute of Standards and Technology. – Электронные данные. – Режим доступа : http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
2. Implementation of the AES-128 on Virtex-5 FPGAs [Электронный ресурс] : Article / Philippe Bulens, Francois-Xavier Standaert, Jean-Jacques Quisquater, Pascal Pellegrin, Gael Rouvroy – Электронные данные. – Режим доступа : perso.uclouvain.be/fstandae/publis/53.pdf.