

чине фиксированным током. Что таким образом позволяет компенсировать погрешность, связанную с сопротивлением утечки.

Устройство создано на основе микроконтроллера ATtiny2313 семейства AVR. Данное семейство микроконтроллеров было выбрано, т.к. AVR микроконтроллеры поддерживают SPI – последовательное программирование – то есть простой интерфейс для записи программного кода, который позволяет использовать простейший вариант самодельного программатора [3]. Данный микроконтроллер имеет два внешних входа для выполнения прерываний INT0, INT1, сигнал на которые поступает с компараторов устройства. Согласно заложенной в контроллер программе – заряд и разряд конденсатора осуществляется путём подачи логического нуля и единицы на вывод микроконтроллера. Ток заряда и разряда лимитируется за счёт ограничительного резистора. Компаратор срабатывает, если напряжение на измеряемом конденсаторе, достигнет уровня, заданного делителями стабилизированного напряжения питания. Ввод посредством динамической индикации на 7-ми сегментный дисплей.

В ходе исследовательской работы на этом же устройстве был так же реализован противопоставляемый метод зарядки ёмкости постоянным током без компенсации сопротивления утечки. В ходе анализа полученных данных, было заключено что предлагаемый способ последовательного заряда и разряда ёмкости постоянным током с целью компенсации влияния сопротивления утечки весьма актуален.

Таким образом, на основании проведённой работы было получено оригинальное устройство и получен патент на изобретение №16741 «Устройство для измерения электрической ёмкости».

Литература

1. Шалавин С.А. Вершинин А.С. «Способ преобразования ёмкости во временной интервал.»– Труды молодых специалистов ПГУ. 2011. – С. 103–105.
2. Шалавин С.А.Вершинин А.С. «Влияние сопротивления утечки на метрологические характеристики преобразования электрической ёмкости во временной интервал.» – Труды молодых специалистов ПГУ. 2011 г. – С. 105-107.
3. Программатор Громова Программатор Громова. [Электронный ресурс] Режим доступа: <http://easyelectronics.ru/avr-shag-regvuj-programmator.html> – Дата доступа: 19.10.2012.

©ПГУ

БИОТОПЛИВО. ПЕРСПЕКТИВЫ ПРОИЗВОДСТВА

Д.А. ШАРИЙ, А.Л. ЛИСОВСКИЙ

The issue of production motor car's biofuel had been discussed in this article

Ключевые слова: биотопливо, биоэтанол, энергия, промышленные отходы

Статья посвящена актуальному на сегодняшний день вопросу производства автомобильного биотоплива. Обосновывается идея о том, что расход топлива не имеет тенденции к снижению и зависит от добычи полезных ископаемых, которые не безграничны. Решение проблемы возможно с использованием биотоплива, перспективам развития которого и уделяется основное внимание в данной статье.

В качестве топлива для двигателя внутреннего сгорания используются не только продукты переработки нефти. Основная проблема состоит в том, что нефть и газ на планете не безграничны, а ведь они являются основным сырьём для топлива. Альтернативой этому служит биомасса. Биомассой принято называть все органические вещества как растительного, так и животного происхождения, источником которых служит существующая биосфера нашей планеты. Биомасса уже давно используется в качестве сырья для производства различного вида топлива, например этанола (этилового спирта). Таким сырьём служат мусор, пищевые и бытовые отходы, опилки и другие отходы лесной и лесоперерабатывающей индустрии, экскременты сельскохозяйственных животных, солома, излишки зерна и т.п. [1]

Цех по производству топлива из вторсырья может работать как на предприятии по переработке отходов, так и прямо на целлюлозно-бумажном комбинате, при этом часть отходов пойдет на выработку энергии, а часть - на изготовление этанола. Для примера, коммерциализация технологии позволит наладить в Европе рентабельное производство биотоплива нового поколения для нужд транспорта, не ставя под угрозу снабжение древесным сырьём лесопромышленные предприятия. Важно, что технология соответствует требованию Евросоюза о повышении эффективности вторичного использования материалов. Так, в комплексе постановлений ЕС по энергии и климату биотопливо на основе отходов и древесины называется более приоритетным по сравнению с прочими видами биотоплива. [3]

Республика Беларусь относится к категории стран, которые не обладают значительными собственными топливно-энергетическими ресурсами, собственные ресурсы ископаемых энергоносителей составляюи не более 15 % от потребности.

Также Республика Беларусь подходит для развития биоэнергетики благодаря наличию больших массивов промышленного леса, равнинного ландшафта, развитой инфраструктуры распределения

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

©БГУИР

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 Т-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 Bultens, Francois-Xavier Standaert, Jean-Jacques Quisquater, Pascal Pellegrin, Gael Rouvroy – Электронные данные. – Режим доступа : perso.uclouvain.be/fstandae/publis/53.pdf.