ПОСЛЕДОВАТЕЛЬНЫЙ ПРОЦЕССОР АЛГОРИТМА ШИФРОВАНИЯ AES НА БАЗЕ FPGA

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Шашков А. С.

Станкевич А.В. − к. т. н., доцент

Сегодня шифрование применяется почти в любых устройствах передачи и хранения данных. Одним из самых популярных алгоритмов шифрования, в том числе реализуемых аппаратно, является алгоритм AES. В данном проекте была осуществлена попытка оптимальной реализации этого алгоритма на итерационной структуре для ПЛИС по критерию максимальной производительности при минимальных затратах ресурсов.

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 конечного результата проектирования. Структурная схема такого процессора показана на рисунке 1.

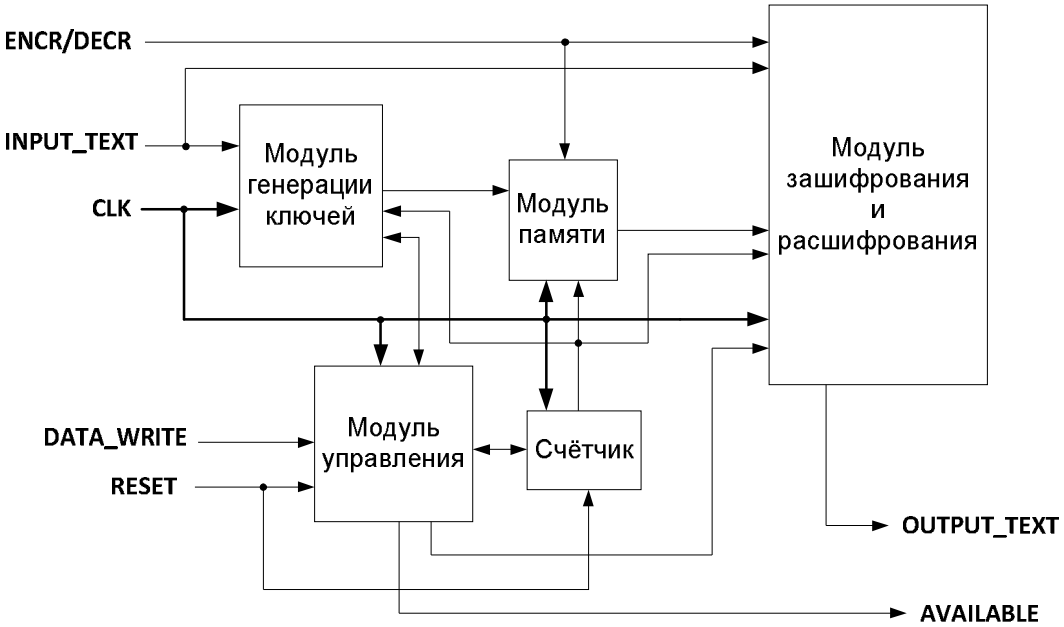

Рисунок 1 – Структурная схема процессора зашифрования и расшифрования

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 (смотрите таблицу 1). Полученная пропускная способность позволяет данным разработкам получить применение в быстродействующих системах передачи и хранения данных. Полученные характеристики разработанных модификаций процессоров лучше или сравнимы с характеристиками аналогичных разработок от фирмы Helion Technology [2], которые являются одними из лучших разработок на рынке (смотрите таблицу 2).

Также можно заключить, что все представленные в проекте модификации процессоров могут представлять определённый интерес в зависимости от специфики конкретного приложения.

Таблица 1 – Отчёт о быстродействии и занимаемых ресурсах для процессоров зашифрования/расшифрования

Кристалл ПЛИС	Макси-мальная частота, МГц	Слайсы, штук	Энергопо-требление, мВт	Пропускная способность, Мбит/сек
Для процессора зашифрования:				
Virtex 5 (-3) xc5vlx30-ff676-3	360	346	790	4190
Virtex 6 (-3) xc6vlx75t-ff784-3	425	392	1780	4941
Virtex 7 (-3) xc7vx330t-ffg1157-3	445	588	371	5176
Spartan 6 (-2) xc6slx45-fgg676-2	223	407	171	2594
Для процессора зашифрования и расшифрования:				
Virtex 5 (-3) xc5vlx30-ff676-3	258	738	890	3001
Virtex 6 (-3) xc6vlx75t-ff784-3	292	654	1865	3395
Virtex 7 (-3) xc7vx330t-ffg1157-3	318	814	455	3706
Spartan 6 (-2) xc6slx45-fgg676-2	150	612	225	1745

Таблица 2 – Сравнение характеристик процессора зашифрования с синхронной памятью ключей и сходной разработкой фирмы Helion Technology для различный кристаллов ПЛИС

Версия процессора	Spartan 6 (-2)	Virtex 5 (-3)	Virtex 6 (-3)
Процессор зашифрования с синхронной памятью ключей	407 слайсов, 223 МГц, 2594 Мбит/сек	346 слайсов, 360,1 МГц, 4190 Мбит/сек	392 слайса, 424,6 МГц, 4941 Мбит/сек
Процессор зашифрования фирмы Helion Technology [3]	332 слайса, 162 МГц, 1885 Мбит/сек	342 слайса, 363 МГц, 4224Мбит/сек	331 слайс, 450 МГц, 5236 Мбит/сек

Список использованных источников:

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. High Performance AES (Rijndael) cores for Xilinx FPGA [Электронный ресурс] : Datasheet / Helion Technology. – Электронные данные. – Режим доступа : www.heliontech.com/downloads/aes_xilinx_helioncore.pdf.

3. 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 : www.perso.uclouvain.be/fstandae/publis/53.pdf.

4. FPGA Implementations of S-box vs. T-box iterative architectures of AES [Электронный ресурс] : Article / Bhupathi Kakarlapudi, Nitin Alabur – Электронные данные. – Режим доступа : www.teal.gmu.edu/courses/ECE746/project/reports_2008/AES_T-box_report.pdf.