УДК 681.324

А.А. Баркалов, А.А. Красичков, В.О. Кузьменко
ун-т Зеленогурский (Польша),
Донецкий национальный технический университет, г. Донецк,
кафедра электронных вычислительных машин
E-mail: A.Barkalov@iie.uz.zgora.pl

РЕАЛИЗАЦИЯ АЛГОРИТМА ШИФРОВАНИЯ DES НА БАЗЕ FPGA

Abstract
Barkalov A.A., Krasichkov A.A., Kuzmenko V. O. Hardware Realization of algorithm DES base on FPGA. *Realization of algorithm DES is offered. The method is based on simultaneous and conveyer methods of the information processing. The features of realization of the algorithm DES on FPGA are considered.*
Keywords: *data encryption standart, key, conveyer, cryptoprocessor, implementation.*

Анотація
Баркалов О.О., Красічков О.О., Кузьменко В.О. Реалізація алгоритма шифрування DES на базі FPGA. *Запропоновано реалізацію алгоритму DES. Метод заснований на паралельній конвеєрній обробці інформації. Розглядаються особливості реалізації алгоритму DES на FPGA.*
Ключові слова: *стандарт шифрування даних, ключ, конвеєр, криптопроцесор, імплементація.*

Аннотация
Баркалов А.А., Красичков А.А., Кузьменко В.О. Реализация алгоритма шифрования DES на базе FPGA. *Предложена реализация алгоритма DES. Метод основан на параллельной конвейерной обработке информации. Рассматриваются особенности реализации алгоритма DES на FPGA.*
Ключевые слова: *стандарт шифрования данных, ключ, конвейер, криптопроцессор, имплементация.*

Общая постановка проблемы

Время активного использования симметричного алгоритма шифрования Data Encryption Standart (DES) на государственном уровне уже прошло, сузилась область применения. Из-за использования 56-битного ключа DES стал уязвим для современного поколения ЭВМ. С 1997 г. компания RSA Data Security Inc спонсировала три успешных публичных взлома DES. Самый короткий из них длился 22 ч 15 мин, участвовало в нем около 100 тыс. компьютеров [1].

Несмотря на указанные недостатки, DES находит широкое применение в банковском и биржевом деле, а так же в других областях гражданского применения.

Возможность эффективной и экономичной аппаратной реализации изначально была одним из требований, предъявляемых к алгоритму. Более того, в принятом впоследствии стандарте требовалась именно аппаратная реализация.

В этой статье представлена аппаратная реализация алгоритма DES, учитывающая особенности ПЛИС с архитектурой FPGA.

Постановка задач и целей исследований

В данной статье показано влияние трёх аспектов синтеза схемы шифрования DES на производительность и безопасность алгоритма:

1. сокращение критического пути за счёт параллельного выполнения отдельных частей алгоритма;
2. реализация алгоритма DES с использованием конвейерного принципа обработки данных;
3. безопасность передачи ключа в алгоритм и смены ключа при необходимости.

Решение задач и результаты исследований

Алгоритм DES полностью удовлетворяет требованиям к простой аппаратной реализации [2]. Рассмотрим алгоритм DES и особенности его реализации на FPGA.

Начальная и конечная перестановки не влияют на безопасность алгоритма и служат для облегчения загрузки данных в микросхему. Хотя алгоритм без данных перестановок не менее безопасен, но он не может называться DES, так как не соответствует стандарту. Данные операции выполняются на основе программируемых межсоединений и не требуют аппаратных затрат [3].

Следующий этап — шифрование с помощью 16 идентичных этапов (раундов) шифрования. Структура одного этапа приведена на рис. 1.

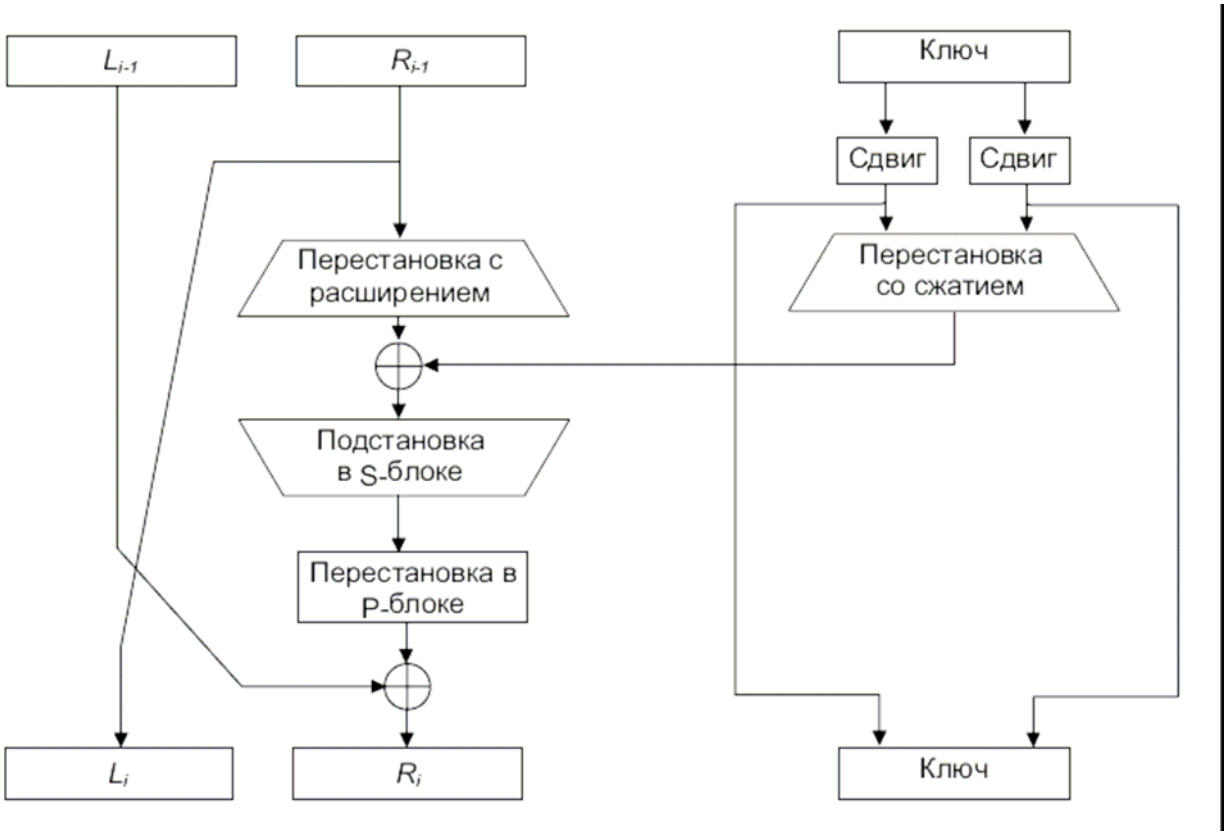

Рисунок 1 — Один этап шифрования алгоритма DES

Здесь: L_{i-1} и R_{i-1} — соответственно левая и правая части 64-битного слова для шифрования, каждая по 32 бита, L_i и R_i — соответственно левая и правая части 64-битного зашифрованного слова, каждая по 32 бита, S-блок — комбинационная схема, выполняющая смешивание битов данных с битами ключа, P-блок — комбинационная схема, выполняющая перестановку битов данных, смешанных с ключом.

На данном этапе реализации можно выделить два вида функций со схожей аппаратной реализацией:

- Перестановка с расширением, перестановка в P-блоке. Так же как начальная и конечная перестановки, каждый из 16-ти этапов не требует значительных аппаратных затрат и физически представляет собой соединение логических элементов ПЛИС.
- Подстановка в S-блоке, XOR. Реализуется с помощью табличного генератора логических функций LUT (Look Up Table), при этом отпадает необходимость использование ПЗУ для подстановки в S-блоке. Такая реализация подстановки в S-блоке даёт возможность параллельной выборки из всех восьми блоков, что существенно снижает величину критического пути и увеличивает быстродействие всей схемы.

Дальнейшее увеличение быстродействия схемы может быть достигнуто путём конвейеризации этапов шифрования (рис. 2).

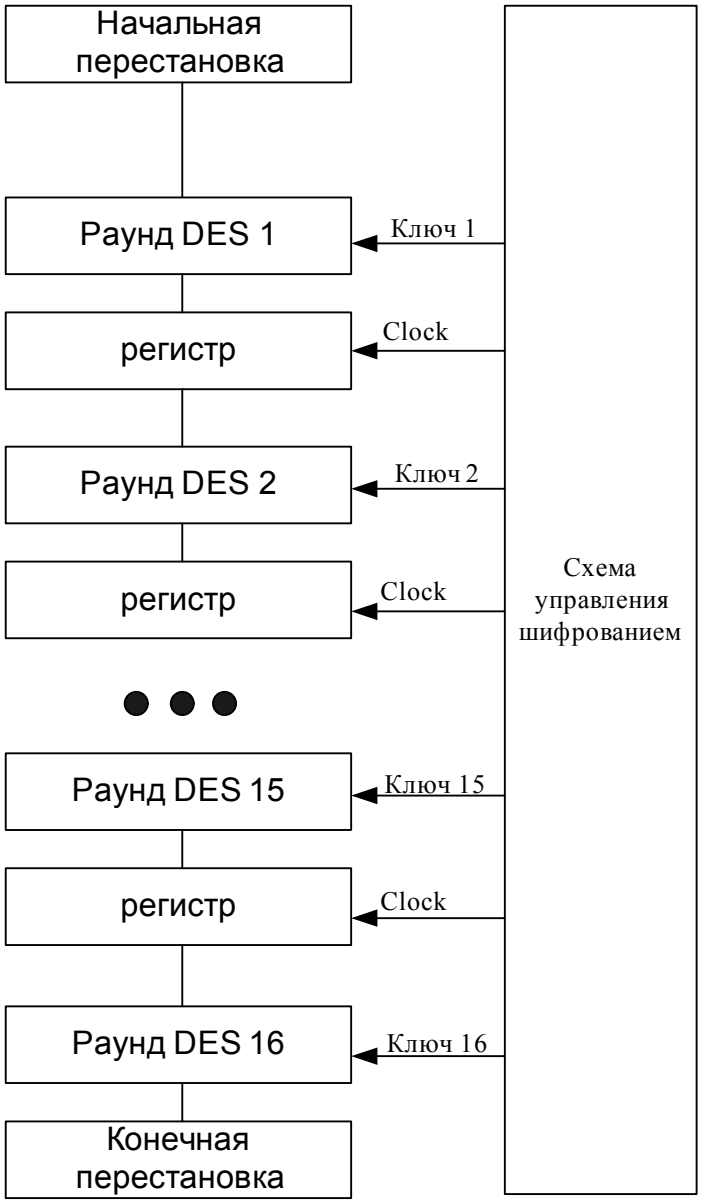

Рисунок 2 — Схема конвейеризации шифрования

В данном примере криптопроцессор DES имеет 16 устройств для каждого раунда и способен обрабатывать 16 этапов алгоритма одновременно. Это достигается за счет введения так называемых конвейерных регистров между раундами. В каждом такте по синхросигналу Clock обрабатываемый блок продвигается в конвейере на одну позицию (рис.3). Схема управления шифрованием также должна иметь конвейерные регистры для движения раундовых ключей (Ключ 1 – Ключ 16) параллельно соответствующим им блокам раундов DES. Таким образом, данная схема может выполнять одновременную обработку блоков данных с различными ключами.

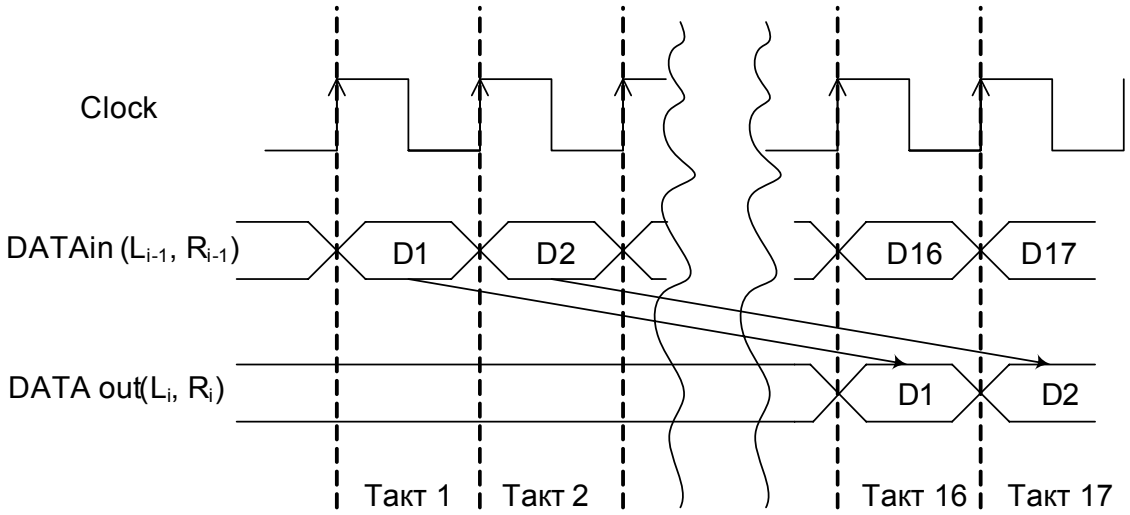

Рисунок 3 — Временная диаграмма работы схемы шифрования

В программных и аппаратных реализациях практически всех криптографических алгоритмов всегда остро стоял вопрос безопасности передачи ключа в алгоритм и смены ключа при необходимости. При реализации на FPGA данная проблема может быть решена путём занесения ключа в саму схему шифрования на этапе проектирования, при этом ключ становится недоступным для чтения.

Далее полученная схема описывается на языке VHDL для последующего автоматического синтеза и окончательной имплементации на FPGA посредством САПР Active HDL и Xilinx ISE [4].

Данная реализация алгоритма DES имеет следующие достоинства:

- сокращение критического пути за счёт параллельного выполнения отдельных блоков алгоритма;
- ускорение шифрования за счёт применения конвейерного принципа обработки данных в 16 раз;
- отсутствие управляющего автомата;
- простота интерфейса;
- безопасность ключа (хранится в ПЛИС).

Из недостатков можно выделить:

- статичность ключа, который можно изменить только при перепрошивке схемы;
- использование 64-битного интерфейса алгоритма;
- достаточно большая площадь на кристалле.

Выводы

При имплементации данной схемы шифрования на FPGA серии Spartan-IIe при помощи пакета Xilinx ISE 4.1 были получены следующие результаты (см. табл. 1).

Таблица 1

Аппаратурные ресурсы ПЛИС	Число использованных ресурсов	Процент использования ресурсов ПЛИС
Число триггеров	960 из 6144	15%
Число LUT-блоков	3328 из 6144	54%
Число блоков ввода-вывода	176 из 325	54%
Минимальный период	14,7 нс	—
Максимальная частота	68 МГц	—

Таким образом, схема обеспечивает шифрование данных со скоростью:

68 МГц * 64 бит = 4,25 Гбит/с.

При реализации данной логической схемы шифрования без использования конвейера скорость шифрования уменьшится в 16 раз, что соответствует стандартной реализации алгоритма DES [5–8]:

68 МГц * 64 бит / 16 = 272 Мбит/с.

Проведенные исследования показывают, что данная реализация алгоритма DES может быть успешно использована при проектировании различных телекоммуникационных систем, устройств хранения и передачи данных [9,10]. Полученные результаты могут также использоваться в учебном процессе при изучении дисциплин по проектированию цифровых систем на ПЛИС и защите информации.

Литература

1. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы исходные тексты на языке С. — 2–е издание.
2. Ростовцев А., Маховенко Е. Введение в криптографию с открытым ключом. — СПб.: Мир и семья. — Интерлайн, 2001. — 354 с.
3. Баркалов А.А. Синтез устройств управления на программируемых логических устройствах. — Донецк: ДонНТУ, 2002. — 262 с.
4. Суворова Е.А., Шейнин Ю.Е. Проектирование цифровых систем на VHDL. — СПб.: БХВ-Петербург, 2003. — 576 с.: ил.
5. Чмора А.Л. Современная прикладная криптография. — М.: Гелиос АРВ, 2001.
6. Саломаа А. Криптография с открытым ключом. — Москва: "Мир", 1995. — 318 с
7. Устинов Г.Н. Основы информационной безопасности. — М: Синтег, 2000.
8. Menezes A., van Oorschot P., Vanstone S. "Handbook of Applied Cryptography" , CRC press, 1996.
9. Schneier B. "Applied Cryptography" , John Wiley & Sons Inc, 1996.
10. Agranovsky A.V., Hady R.A. "Crypto miracles with random oracle", The Proceedings of IEEE SIBCOM'2001, The Tomsk Chapter of the Institute of Electrical and Electronics Engineers, 2001.

Здано в редакцію:
23.03.2009р.

Рекомендовано до друку:
д.т.н, проф. Башков Є.О.