Московский физико-технический институт
(государственный университет)
Факультет радиотехники и кибернетики
Кафедра радиотехники

Современные возможности аппаратной реализации алгоритма шифрования DES

Автор:
студент 912 группы
В. О. Костенко

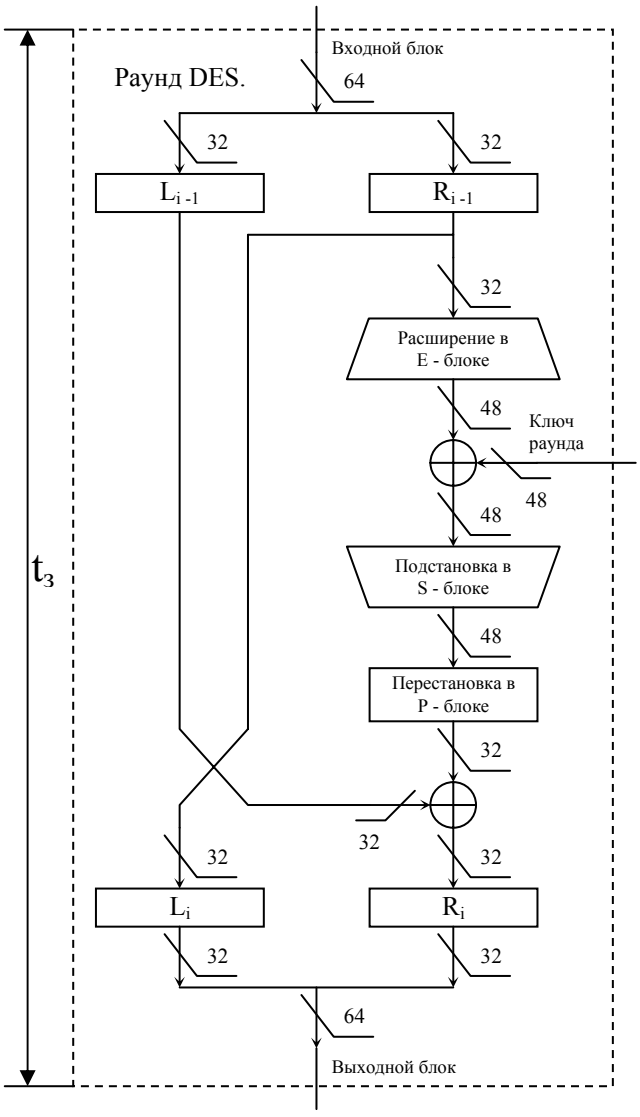
3 мая 2002 г.
Москва

Введение. Алгоритм DES и основы его аппаратной реализации.

Стандарт шифрования данных DES был создан в результате потребности многих коммерческих организаций в едином, стандартном криптографическом алгоритме. Алгоритм должен был гарантировать совместимость криптографического оборудования и безопасность передачи данных по открытым линиям связи. Он должен был быть проверен на криптографическую стойкость, а его реализация должна была стать недорогой и легко доступной.

Возможность эффективной и экономичной аппаратной реализации изначально была одним из требований, предъявляемых к алгоритму. Более того, в принятом впоследствии стандарте требовалась именно аппаратная реализация. Вплоть до 1994 года стандарт официально запрещал программные реализации DES.

Стандарт DES полностью удовлетворяет требованиям к легкой аппаратной реализации. Все производимые алгоритмом операции ограничиваются следующими:



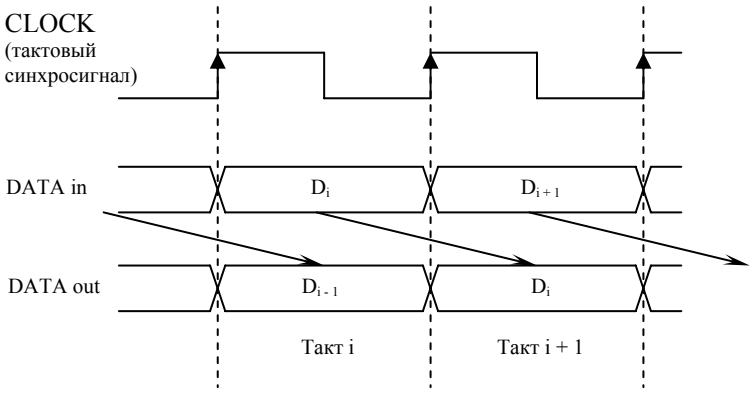
- ✓ Битовые выборки, перестановки и сдвиги битов. Не требуют отдельных ресурсов при аппаратной реализации. Выполняются путем соответствующего соединения логических элементов на печатной плате или внутри криптопроцессора DES.
- ✓ Исключающее ИЛИ. Реализуется простейшим логическим элементом.
- ✓ Подстановка со сжатием. Реализуется на основе постоянного запоминающего устройства (ПЗУ), имеющего 6 – битовый входной адрес и 4 – битовую выходную шину данных. Объем такого ПЗУ 2^6 слов по 4 бита каждое = 256 бит. Это был максимальный объем памяти, которая в начале 70-х годов размещалась внутри одного корпуса микросхемы. Такое ПЗУ также может быть реализовано внутри криптопроцессора DES, т. к. его содержимое определено стандартом. Возможна также реализация в виде оперативной памяти (ОЗУ). В этом случае ее содержимое должно загружаться в блоки подстановки до начала работы алгоритма DES.

Одной из наиболее существенных для аппаратной реализации особенностей является наличие в алгоритме 16 раундов, различающихся только ключами. Это указывает на то, что разработчики стандарта предусматривали в качестве основного варианта реализации последовательное исполнение раундов во времени. Для этого достаточно иметь одно устройство

для реализации раунда DES и простейший регистр для хранения промежуточных блоков между раундами.

Устройство, реализующее раунд DES, является комбинационным. Это означает, что оно не содержит внутри себя никаких элементов с памятью. Основным параметром такого устройства является время задержки $t_з$. Смысл этого параметра следующий: если в момент времени t_0 на вход устройства подать входной 64 – битовый блок и продолжать его удерживать на входе, то в течение времени $t_з$ внутри устройства будут происходить переходные процессы, и его выход будет находиться в неопределенном состоянии. Начиная с момента времени $t_0 + t_з$, на выходе устройства установится правильное значение выходного блока. Если ввести его в некоторое запоминающее устройство, то сразу после этого можно снять со входа текущий входной блок и подать туда следующий.

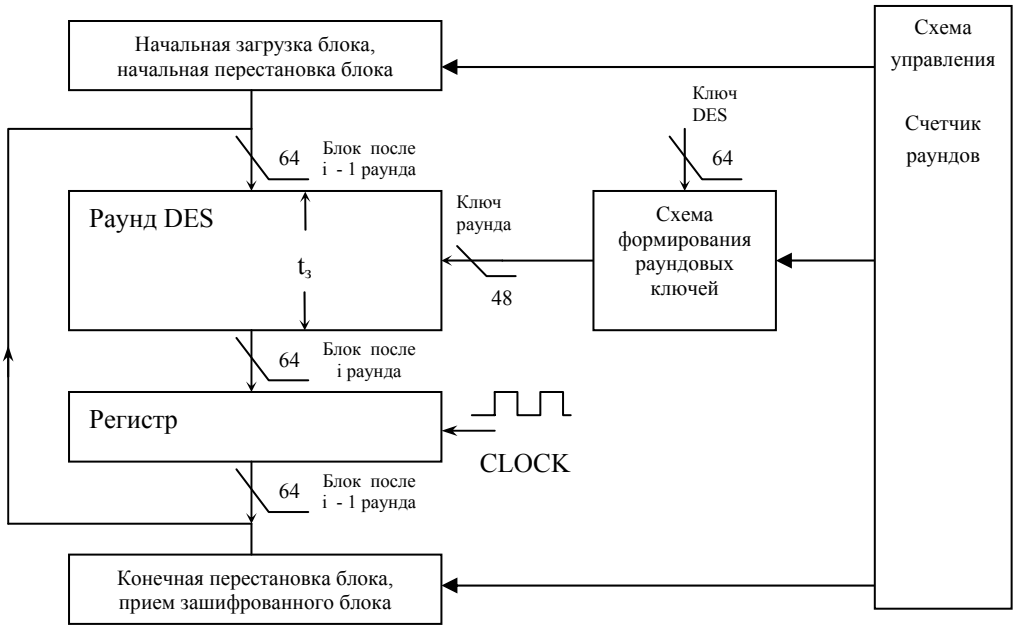
Регистр для хранения промежуточных блоков между раундами можно реализовать на D-триггерах. Такой регистр является синхронным и имеет вход для тактовых синхроимпульсов, период которых является временем хранения данных в регистре. Регистр работает следующим образом: в течение любого определенного такта на выходах регистра хранится значение данных, имевшееся на его входе в конце предыдущего такта. Началом такта, как правило, является момент перехода тактового синхросигнала из состояния логического “0” в состояние логической “1”.



Временная диаграмма работы регистра на основе D-триггеров.

1. Простейшая реализация с одним устройством раунда DES.

С использованием указанных аппаратных средств устройство, реализующее DES, выглядит следующим образом.



Скорость шифрования определяется тактовой частотой. Для полного 16 – раундового шифрования DES требуется соответственно 16 тактов. В свою очередь, максимальная тактовая частота определяется временем задержки устройства раунда DES $t_з$ и равна $f_{max} = 1 / t_з$. В самом деле, именно $t_з$ является минимальным временем, в течение которого регистр должен хранить в себе результат предыдущего раунда, чтобы работа устройства раунда DES была выполнена корректно.

Работа схемы формирования раундовых ключей в целом аналогична работе раунда DES. А именно, схема должна содержать блок сдвига ключа, блок перестановки ключа со сжатием, и регистр, хранящий значение сдвинутого ключа в текущем такте.

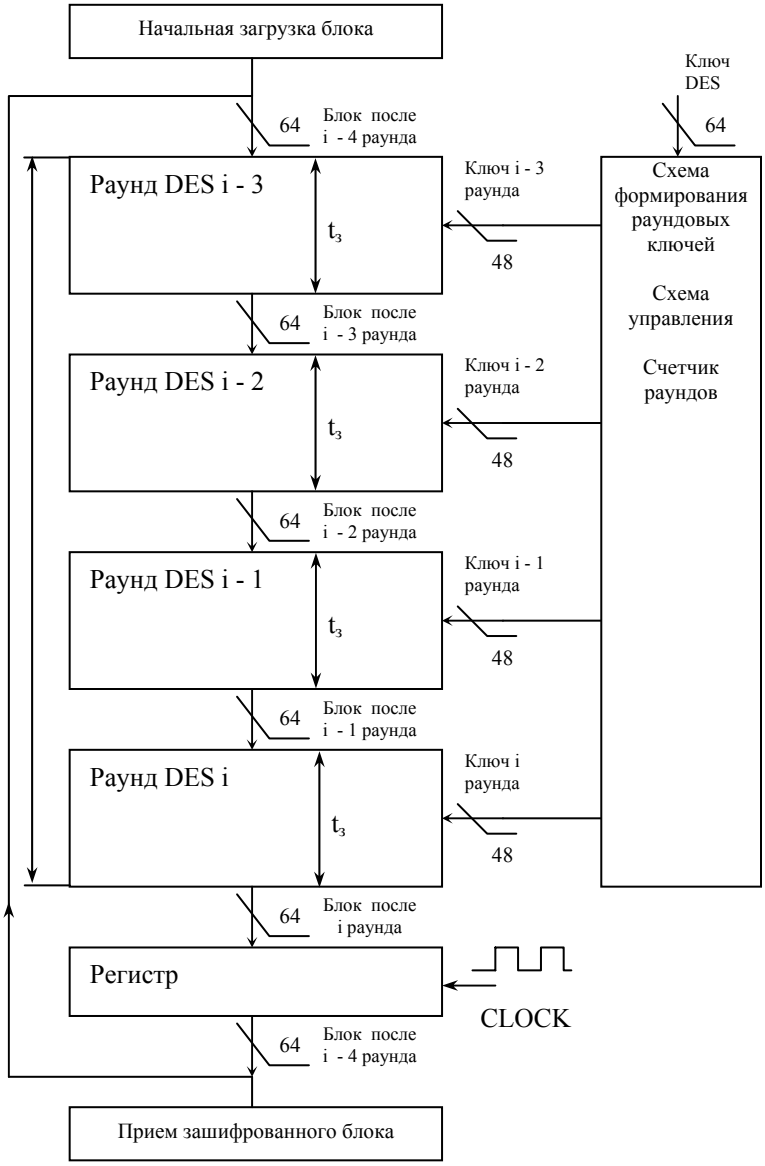
Работа схемы управления заключается в следующем: она должна обеспечить начальную загрузку блока извне, исполнение раунда DES 16 раз (для чего должен присутствовать соответствующий счетчик), и последующую передачу зашифрованного блока наружу.

Именно по этому принципу работали первые аппаратные реализации DES на простейших логических микросхемах. Большинство имеющихся криптопроцессоров DES работают по этой схеме. Ее достоинства для практического использования очевидны: минимум затрат на реализацию при достаточной скорости работы. Повышение скорости шифрования здесь связана исключительно с уменьшением времени $t_з$, что достигается совершенствованием технологии и уменьшением размера транзисторов.

Максимальная скорость работы данной реализации P, в Мбайт/с, выражается через максимальную тактовую частоту $f = f_{max}$, в МГц, следующим образом: $P = 0.477 \cdot f$. Она может быть и чуть меньше из-за того, что помимо 16 тактов шифрования, устройство может тратить 1 – 2 такта на загрузку и выдачу данных.

2. Реализация с последовательным включением нескольких устройств раунда DES.

Дальнейшее увеличение скорости работы криптопроцессора связано с увеличением имеющегося в нем количества устройств, реализующих раунд DES, с их последовательным включением.

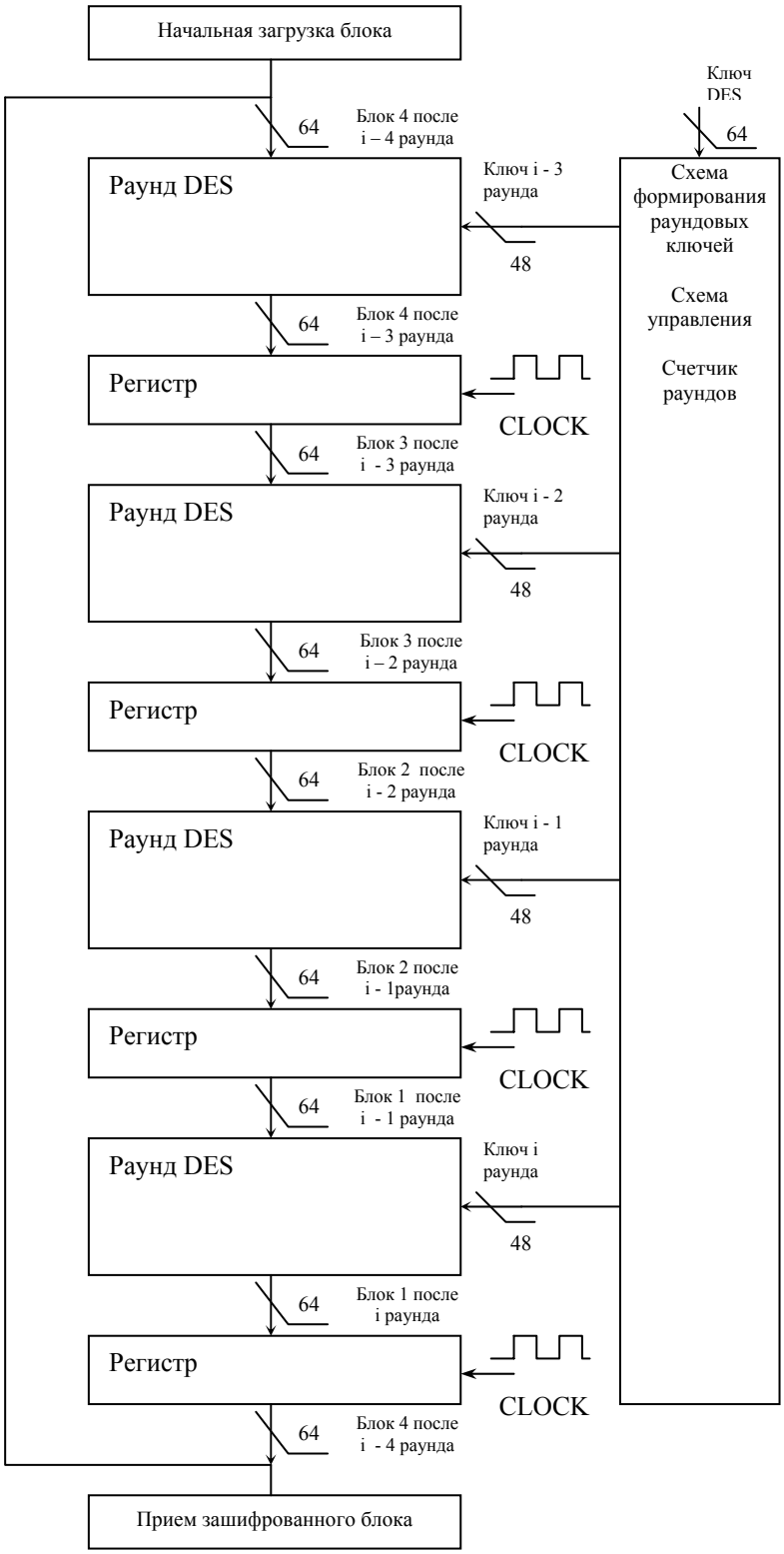


В данном примере используются 4 блока раунда DES. При этом для 16 – раундового шифрования блока потребуется 4 такта. Однако максимальная тактовая частота уменьшится по сравнению с простейшим вариантом также в 4 раза. Производительность, таким образом, по сравнению с простейшим вариантом не увеличится. Этот вариант следует рассматривать как вынужденный в том случае, если технология изготовления микросхемы не позволяет ввести в нее тактовые синхроимпульсы достаточно высокой частоты. Однако он был реализован в некоторых устройствах.

Максимальная скорость работы данной реализации P, в Мбайт/с, выражается через максимальную тактовую частоту $f = f_{max} / N$, в МГц, следующим образом: $P = 0.477 \cdot N \cdot f = 0.477 \cdot f_{max}$, где N – число имеющихся в криптопроцессоре блоков раундов DES, равное 2, 4, 8 или 16, f_{max} – максимальная тактовая частота простейшего варианта реализации 1.

3. Реализация с конвейерным включением нескольких устройств раунда DES.

И, наконец, наивысшая возможная для заданной технологии скорость достигается для варианта, использующего конвейерный принцип обработки информации.



Чтобы получить его из предыдущего варианта, достаточно включить между устройствами раунда DES промежуточные регистры.

В данном примере криптопроцессор DES имеет 4 устройства раунда DES и способен обрабатывать 4 блока одновременно. Это достигается за счет введения т. н. конвейерных

регистров между раундами. Каждый такт обрабатываемый блок продвигается в конвейере на одну позицию. Схема формирования раундовых ключей также должна иметь конвейерные регистры для движения раундовых ключей параллельно соответствующим им блокам. Так что данная схема позволяет, в отличие от предыдущих вариантов, одновременную обработку блоков с различными ключами. Каждая пара блок – ключ движется по конвейеру независимо от остальных. Причем максимальная тактовая частота такая же высокая, как и в простейшем варианте. Но и необходимое количество логических элементов здесь также самое большое.

Максимальная скорость работы данной реализации P, в Мбайт/с, выражается через максимальную тактовую частоту $f = f_{max}$, в МГц, следующим образом: $P = 0.477 \cdot N \cdot f_{max}$, где N – число имеющихся в криптопроцессоре блоков раундов DES, равное 2, 4, 8 или 16, f_{max} – максимальная тактовая частота простейшего варианта.

4. Анализ имеющихся данных об аппаратных реализациях DES.

С учетом вышеизложенного, можно проанализировать имеющуюся статистику по криптопроцессорам и определить, по какой из имеющихся схем они построены. Данные с 1981 по 1995 г. приведены у Б. Шнайера в его “Прикладной криптографии”:

Коммерческие микросхемы DES

Производитель	Микросхема	Год	Тактовая частота	Скорость данных	Доступность	
AMD	Am9518	1981	3 МГц	1.3 Мбайт/с	Н	1
AMD	Am9568	?	4 МГц	1.5 Мбайт/с	Н	1
AMD	AmZ8068	1982	4 МГц	1.7 Мбайт/с	Н	1
AT&T	T7000A	1985	?	1.9 Мбайт/с	Н	?
CE-Infosys	SuperCrypt CE99C003	1992	20 МГц	12.5 Мбайт/с	Д	2
CE-Infosys	SuperCrypt CE99C003A	1994	30 МГц	20.0 Мбайт/с	Д	2
Cryptech	Cry12C102	1989	20 МГц	2.8 Мбайт/с	Д	0
Newbridge	CA20C03A	1991	25 МГц	3.85 Мбайт/с	Д	0
Newbridge	CA20C03W	1992	8 МГц	0.64 Мбайт/с	Д	0
Newbridge	CA95C68/18/09	1993	33 МГц	14.67 Мбайт/с	Д	1
Pijnenburg	PCC100	?	?	2.5 Мбайт/с	Д	?
Semaphore Communications	Roadrunner284	?	40 МГц	35.5 Мбайт/с	Д	2
VLSI Technology	VM007	1993	32 МГц	200.0 Мбайт/с	Д	3
VLSI Technology	VM009	1993	33 МГц	14.0	Д	1
VLSI Technology	6868	1995	32 МГц	64.0 Мбайт/с	Д	2
Western Digital	WD2001/2002	1984	3 МГц	0.23 Мбайт/с	Н	0

Интересно, что некоторые микросхемы работают гораздо медленней, чем простейшая схема 1. Очевидно, они выполняют операции раунда (такие как расширение, исключающее ИЛИ, подстановка и сжатие), последовательно во времени, и являются, скорее всего, микроконтроллерами, запрограммированными на исполнение DES.

В течение нескольких последних лет криптопроцессоры утратили свое значение как отдельные устройства, и превратились в элементы более крупных специализированных чипов, таких как сетевые контроллеры или контроллеры смарт – карт. Информация об их скорости работы не является широко распространенной. При необходимости использования криптопроцессора в малосерийном устройстве, применяют, как правило, программируемые логические микросхемы (ПЛИС). Несколько фирм предлагают описания криптопроцессоров в виде исходных текстов на языках описания аппаратуры (HDL, Hardware Description Language), таких как VHDL или Verilog. Такое описание компилируется специальной программой - компилятором ПЛИС, которая затем способна загрузить прошивку из PC – совместимого компьютера непосредственно в ПЛИС по специальному проводу.

Пример такой реализации – X_DES Cryptoprocessor фирмы AlianceCORE™. Доступен в виде VHDL и Verilog, работает по простейшей схеме 1, тратит 16 операций на шифрование, тактовая частота на ПЛИС фирмы Xilinx семейства Virtex-E 120МГц. Производительность 57 Мбайт/с.

Другой пример реализации – DES Cryptoprocessor Core фирм CAST, Inc и Ocean Logic Pty Ltd. Доступен в виде VHDL и Verilog, также работает по простейшей схеме 1 и тратит 16 операций на шифрование.

5. Реализация криптопроцессора с наибольшей возможной производительностью на ПЛИС Stratix фирмы Altera.

Автором данного эссе была выполнена разработка криптопроцессора, реализующего максимально возможную скорость на новейшей элементной базе. На HDL Verilog было создано описание криптопроцессора по схеме 3, имеющего 16 устройств раунда DES и способного обрабатывать 16 блоков DES одновременно, выдавая по 1 зашифрованному блоку в каждом такте. В качестве чипа ПЛИС был выбран младший представитель последнего семейства ПЛИС фирмы Altera – чип EP1S20F484C5 семейства Stratix. Данное семейство еще не выпускается серийно, но уже сейчас доступны инженерные сэмплы стоимостью около 1200 – 1500 $. Предполагаемая стоимость серийных чипов – около 120$.

Для проверки корректности работы логики был использован тестовый вектор из “Handbook of Applied Cryptology”, A. Menezes, и симулятор ModelSim фирмы Mentor Graphics. Для компиляции использовался последний компилятор фирмы Altera – Quartus II v. 2.2. Были получены следующие результаты:

DES Resource Usage Summary

Resource	Usage
Logic cells	7,281 / 18,460 (39 %)
Registers	2,224 / 19,543 (11 %)
User inserted logic cells	0
I/O pins	194 / 361 (53 %)
Clock pins	2
Dedicated input pins	0
Global signals	2
M512s	0 / 194 (0 %)
M4Ks	0 / 82 (0 %)
M-RAMs	0 / 2 (0 %)
Total memory bits	0 / 1,669,248 (0 %)
Total RAM block bits	0 / 1,669,248 (0 %)
DSP block 9-bit elements	0 / 80 (0 %)
PLLs	0 / 6 (0 %)
Global clocks	2 / 16 (12 %)
Regional clocks	0 / 16 (0 %)
Fast regional clocks	0 / 8 (0 %)
DIFFIOCLKs	0 / 16 (0 %)
SERDES transmitters	0 / 66 (0 %)
SERDES receivers	0 / 66 (0 %)
Maximum fan-out node	clock
Maximum fan-out	2224
Total fan-out	28330
Average fan-out	3.79

DES fmax (not incl. delays to_from pins)

clock, DES_round:round_9|block_out[63]~reg0, DES_round:round_8|block_out[34]~reg0, None, 162.36 MHz (period = 6.159 ns)
clock, DES_round:round_9|block_out[63]~reg0, key_E:key_E|key_shift_1:key_shift_09|key_out[24]~reg0, None, 162.55 MHz (period = 6.152 ns)
clock, DES_round:round_9|block_out[63]~reg0, DES_round:round_8|block_out[64]~reg0, None, 164.88 MHz (period = 6.065 ns)
clock, DES_round:round_9|block_out[63]~reg0, DES_round:round_8|block_out[35]~reg0, None, 165.26 MHz (period = 6.051 ns)
clock, DES_round:round_9|block_out[63]~reg0, key_E:key_E|key_shift_1:key_shift_09|key_out[1]~reg0, None, 168.66 MHz (period = 5.929 ns)
clock, DES_round:round_9|block_out[63]~reg0, DES_round:round_8|block_out[36]~reg0, None, 168.95 MHz (period = 5.919 ns)

Таким образом, созданный крипточип должен использовать около 40 % ресурсов ПЛИС и устойчиво работать на частоте 150МГц. Его производительность составит $150 \cdot 10^6$ блоков DES в секунду = 1.12 Гбайт/с = 8.9Гбит/с, стоимость – около 120$. При этом приобретение большой партии таких чипов будет доступно любой крупной коммерческой фирме.

6. Современные возможности аппаратной реализации прямой атаки DES.

Наибольший интерес представляет собой возможность реализации на базе такого чипа машины для взлома DES путем прямого перебора ключей при одной известной паре текст – шифротекст. Данный крипточип имеет достаточно свободных ресурсов ПЛИС для реализации схемы перебора части ключей и схемы сравнения зашифрованного с текущим ключом текста с известным криптотекстом. Для полного перебора $2^{56} = 7.2 \cdot 10^{16}$ ключей потребуется зашифровать такое же количество блоков. В 1993 г. Майкл Винер спроектировал машину стоимостью в 1 миллион $, для вскрытия DES в среднем за 3.5 часа. Полный перебор происходит при этом за 7 часов = 25200 с, что соответствует скорости $2.9 \cdot 10^{12}$ блоков/с.

Для такого перебора с помощью разработанного чипа со скоростью $1.5 \cdot 10^8$ блоков/с потребуется 19300 чипов суммарной стоимостью 2.28 миллионов $. Если считать, что на печатную плату машины поместится 10 чипов DES, в 19’ корпус поместится 6 таких плат, а в 19’ стойку – 8 корпусов, то такая машина заняла бы около 50 шкафов, набитых криптопроцессорами. Если увеличить время полного перебора до 2 суток, машина будет стоить 350000$ и занимать 7 шкафов. Таким образом, организации, не имеющие возможности организовать собственное производство чипов, и вынужденные пользоваться общедоступной элементной базой, еще долго не смогут построить машину достаточной мощности для быстрого вскрытия DES.

С другой стороны, если предположить, что какой – либо очень крупной фирме удастся создать криптопроцессор с параметрами как у процессора Pentium III: с частотой 1GHz и стоимостью 60$, то для перебора всех ключей за 7 часов потребуется 2900 чипов стоимостью всего 174000$ и те же 7 шкафов. Но неизвестно еще, во что обойдется разработка и выпуск такого чипа сравнительно небольшой серией.

Таким образом, несмотря на свой почти 30 – летний возраст, DES остается хорошей защитой для коммерческого использования. Хотя возможности реализации машины для прямой атаки DES для правительственных учреждений такой страны как США сегодня могут быть вполне реальными, вряд ли это будет для них целесообразным.

7. Приложения.

1. Временные диаграммы работы созданного устройства DES на тестовом векторе и сам тестовый вектор.
2. Исходные тексты описания устройства на языке Verilog.

8. Список литературы.

1. Брюс Шнайер, “Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С”, 2 – е издание.
2. A. Menezes, P. van Oorschot, S. Vanstone, “the Handbook of Applied Cryptography”, CRC Press, 1996.
3. “Block Ciphers & Differential Cryptoanalysis. Laboratory Lesson: Learning about DES”, LearningAboutDes.pdf, http://192.188.189.254, Cryptoanalysis of 3-round DES, DES.zip
4. Сергей Емец. “Verilog – инструмент разработки цифровых электронных схем”, http://www.asicdesign.ru/forum/docs/articles/article04.htm
5. “IEEE Standart Hardware Description Language Based on the Verilog Hardware Description Language”, IEEE, 1995.
6. “ModelSim SE Datasheet”, http://www.model.com/products/NewDatasheets/se.pdf
7. “ModelSim 5.7 Quick Guide”, http://www.model.com/products/documentation/qk_guide.pdf
8. “Altera Stratix family FPGA Datasheet“, http://www.altera.com/literature/ds/ds_stx.pdf
9. “Quartus II Software Overview”, http://www.altera.com/products/software/pld/products/q2/qts-index.html