파이프라인 구조의 3DES 암호알고리즘의 설계 및 구현

이완복* · 김정태**

Design and Implementation of 3DES crypto-algorithm with Pipeline Architecture

Wan-Bok Lee* · Jung-Tae Kim**

요 약

대칭키 암호 알고리즘들은 전치와 치환의 연속적인 반복 과정이며, 동작방식에 따라 CBC, ECB, CFB, OFB의 네가지 모드가 있다. 또한 이들 알고리즘들에서는 내부적으로 여러 라운드의 연산을 반복적으로 수행해야 최종 암호문이 완성되기 때문에, 많은 연산 시간이 소요된다. 본 논문에서는 블록 암호 알고리즘의 ECB 모드에서 암호 연산을 가속화할 수 있는 파이프라인드 설계 방법을 제시한다. 제안된 방법에서는 여러 라운드의 암호 연산 블록을 파이프라인드 구조로 구성하고 연속적으로 실행하기 때문에 전체 연산 속도를 매우 높일 수 있다. 또한 파이프라인드 구조로 암호칩을 설계한 후 검증한 결과, 수십 배의 성능 향상이 가능하다는 것을 알 수 있다.

ABSTRACT

Symmetric block ciper algorithm consists of a chains of operations such as permutation and substitution. There exists four kinds of operation mode, CBC, ECB, CFB, and OFB depending on the operation paradigm. Since the final ciper text is obtained through the many rounds of operations, it consumes much time. This paper proposes a pipelined design methodology which can improve the speed of crypto operations in ECB mode. Because the operations of the many rounds are concatenated in serial and executed concurrently, the overall computation time can be reduced significantly. The experimental result shows that the method can speed up the performance more than ten times.

키워드

3DES, 암호 알고리즘, 파이프라인 구조

Ⅰ. 서 론

컴퓨터와 네트워크 기술이 끊임없이 발달하고, 정보화 과정이 눈부시게 진척되고 있는 현대 사회에서는 정보 보호 문제가 시간이 지날수록 더욱 중요해지고 있다. 특히 고속의 암호화 연산이 가능하도록 하드웨어에 기반 한 보안 장비들이 앞으로는 더욱 주목받을 전망이다. 본 논문에서는 DES 블록 암호 알고리즘의 고속화를 위한 설계 기법에 대해 다룬다. 제안된 파이프라인드 설계 기법에서는 DES 알고리즘의 내부 라운드를 순차적으로 처리할 수 있기 때문에 버스트(burst) 모드의 IP 패키 처리에 용이할 것으로 전망된다. 특히, 파이프라인드 설계로 제작할 경

* 중부대학교 컴퓨터 · 게임학부
** 목원대학교 정보전자영상공학부

접수일자 : 2006. 1. 5

우의 칩 성능을 평가하기 위하여 VHDL을 사용하여 구조적 모델링을 행하였으며, Xilinx사의 ISE 5.2i 툴을 이용하여 논리 합성을 수행하였다. FPGA 구현을 위해서 Xilinx사의 ISE 5.2i 툴과 Modelsim을 이용하여 타이밍 시뮬레이션을 수행한 결과 수십 배의 성능 향상이 가능함을 알 수 있다.

Ⅱ. 암호 시스템

암호시스템은 암호화 키(key)와 복호화 키가 동일한가의 여부에 따라 대칭형(symmetric) 암호시스템과 비대칭형(asymmetric) 암호시스템으로 분류할 수 있다. 대칭형 암호 알고리즘은 암호화키와 복호화 키가 동일한 암호 알고리즘을 말하며, DES, 3DES(Triple Data Encryption Standard), SEED, AES(Adnanced Encryption Standard)등이 있다.[1-3] 비대칭형 암호 알고리즘은 암호화키와 복호화 키가 동일하지 않은 암호 알고리즘을 말하고, RSA (Rivest-Shamir- Adleman), ECC등이 이에 속한다. 본 논문에서는 대표적인 블록 암호 알고리즘인 DES, 3DES에 대해서만 그 구조를 간략히 살펴보도록 한다. SEED, AES 등의 기타 알고리즘들도 DES와 유사한 구조를 가지며, 제시한 설계 기법을 통하여 마찬가지로 가속화 될 수 있다.[2][3]

2.1 DES/3DES 알고리즘

가장 대표적인 블록 암호화 알고리즘으로 알려진 DES는 64 비트의 데이터와 56 비트 길이의 키를 사용하여 64 비트의 암호화 결과를 생성한다. DES는 암호화, 복호화 알고리즘이 대칭적이며 치환(Permutation)과 대치(Substitution) 그리고 S_box로 구성된 블록 암호화 시스템이다.

DES암호화에 대한 전체적인 구성이 그림 1에 나타나 있다. 그림에서 알 수 있듯이 암호화 과정에는 암호화하고자 하는 평문(Plaintext)과 키(k1 ... k16)의 두 가지 입력이 들어간다. 64 비트의 평문 블록은 초기 치환(initial permutation : IP)후에 32 비트씩 좌(L0), 우(R0)부분으로 나뉘게되며 그 다음 16라운드의 계산을 거치게 된다. 16라운드 후에는 오른쪽(R16)과 왼쪽(L16) 부분이 합쳐져서 역 초기 치환 (inverse initial permutation : IP-1 : INVERT_IP)을 거침으로써 암호문(Ciphertext)

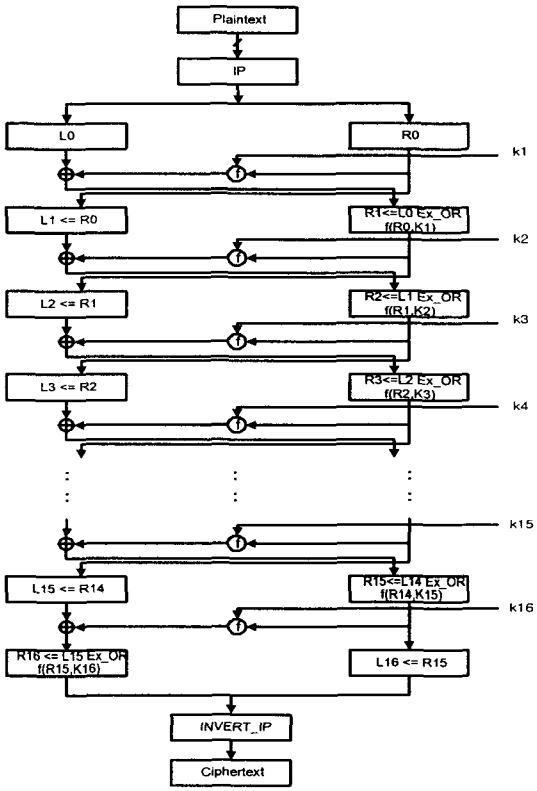

그림 1. DES의 암호화 과정
Fig 1. Encryption Process for DES

이 생성된다. 본질적으로 대치된 64 비트 입력은 16라운드를 거치며 매 라운드의 결과로 64 비트의 중간 값을 생성한다.[1]

DES에서 복호화 과정은 암호화 알고리즘과 비슷하기 때문에 구현이 간단하다. 차이가 있다면 단지 반대의 순서로 계산을 행한다는 것뿐이다. 이것은 암호화를 위한 각 라운드의 키가 K1, K2, K3, ... K16이라면 복호화를 위한 키는 K16, K15, K14, ... K1이 되는 것이다. 두 개의 암호 키를 사용하여 첫 번째 키로 암호화하고 다시 두 번째 키로 복호화한 다음 또 다시 첫 번째 키로 암호화하면 강한 암호를 얻을 수 있는데, 이것이 3DES 알고리즘이다.

Ⅲ. 고속 암호 칩의 설계

본 논문에서는 DES알고리즘의 성능을 개선하는 방안으로 Loop unrolling 파이프라인 방식을 사용하였다. 이 방

식은 DES 내부의 16 라운드 단계에 대해 각각 모듈로서 구현하고, 순차적인 데이터 흐름을 만들어내도록 하여서 속도를 개선시키는 방식이다.

3.1 DES 알고리즘의 파이프라인드 설계

기존의 Iterative방식의 DES알고리즘은 64비트의 암호문이 매번 16clocks후에 생성되는 반면, 파이프라인 방식을 적용하면 16clocks이후에는 매 clock마다 64비트의 암호문이 생성된다.

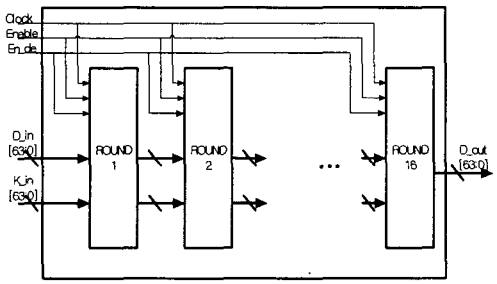

그림 2. DES의 파이프라인 구조
Fig 2. Pipelined Structure of DES

그림 2는 Loop unrolling 파이프라인방식을 적용한 DES알고리즘의 구조를 나타낸다. 각각의 ROUND에는 키 생성을 위한 블록과 암호과정을 위한 블록이 포함되며, ROUND1과 ROUND16에 각각 초기 치환(initial permutation : IP)과 역 초기 치환(inverse initial permutation : IP-1 : INVERT_IP)을 포함하고 있다.

3.2 3DES 알고리즘의 파이프라인드 설계

그림 3은 파이프라인 방식을 적용한 3DES알고리즘의 구조를 나타낸다.

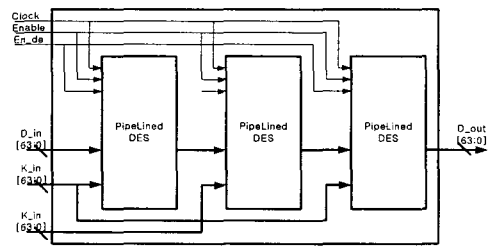

그림 3. 3DES 시스템의 구조
Fig 3. Architecture of 3DES System

그림 3에서 알 수 있듯이 3DES는 DES파이프라인 구조를 3개를 사용하여 구성되어지며, 64비트의 Key값 2개를 받아 처음과 마지막 DES블록에서 첫 번째 64비트 키를 사용하고 두 번째 DES블록에서는 두 번째 64비트 키를 사용한다. 이 구조에서는 48clocks이후에 매 clock마다 64비트의 암호문을 생성할 수 있다.

Ⅳ. 시스템 구현 및 성능 평가

위 파이프라인드 설계의 성능 평가를 위하여 Xilinx ISE 5.2i 툴을 이용하여 VHDL 설계 및 합성을 수행하였다. 또한, 설계 검증을 위한 타이밍 시뮬레이션을 Modelsim을 이용하였고, Xilinx FPGA XC2V8000을 타겟으로 FPGA를 구현하였다.[4]

4.1 전체 시스템의 구조

그림 4는 PCI버스 인터페이스, FIFO, packet processor, 그리고 Crypto Core로 구성된 전체 시스템의 블록도를 나타낸다. PCI BUS Interface블록은 PCI BUS로부터 입력되는 데이터를 Wr_en시그널(FIFO Write Enable)과 함께 W_FIFO블록에 저장하는 역할을 한다. W_FIFO

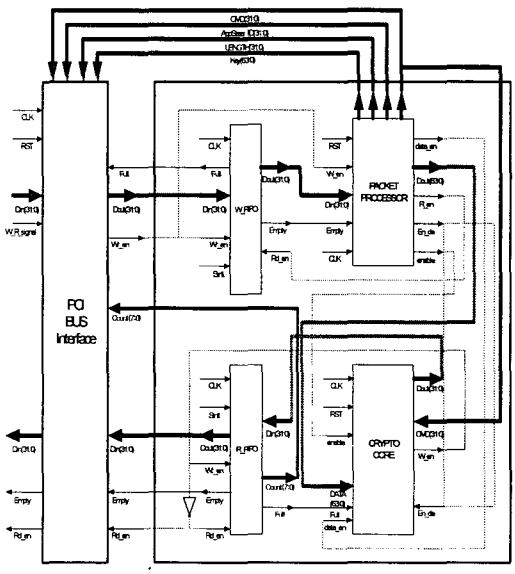

그림 4. 시스템의 전체 구조
Fig 4. Total Structure of System

블록은 입력데이터를 저장하는 역할을 한다. Packet Processor블록은 입력된 데이터를 Key, CMD, Data, Length, AppSess를 각각 분리하여 PCI BUS Interface블록과 Crypto Core 블록으로 전달하는 역할을 한다. Crypto Core 블록은 데이터를 입력받아 DES 알고리즘으로 패킷을 암복호화하여 R_FIFO블록에 전달하며, R_FIFO블록은 출력데이터를 저장하는 역할을 한다. 그림 5는 Pipelined DES의 합성결과를 나타내며, 그림 6은 Pipelined 3DES의 합성결과를 나타낸다.

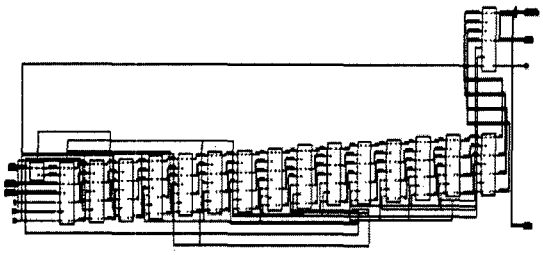

그림 5. Pipelined DES 합성결과
Fig 5. Synthesis Result of Pipelined DES

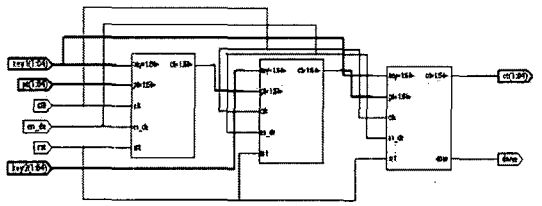

그림 6. Pipelined 3DES 최상위 구조
Fig 6. Top Structure of Pipelined 3DES

4.2 시뮬레이션을 통한 설계 검증

암호화 및 복호화 과정의 검증을 위하여 Modelsim을 이용한 타이밍 시뮬레이션을 행하였다. 검증에 사용된 TestBench는 FIPS-46에서 발표된 벡터를 이용하였고, 시뮬레이션결과 암복화된 값들이 서로 일치함을 확인하였다. 그림 7은 Pipelined 3DES의 암호화 시뮬레이션 결과를 나타내며, 그림 8는 복호화 시뮬레이션 결과를 나타낸다.

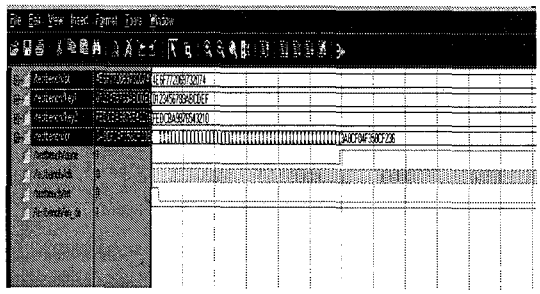

그림 7. Pipelined 3DES 암호화 시뮬레이션 결과
Fig 7. Simulation Result of Encryption for Pipelined 3DES

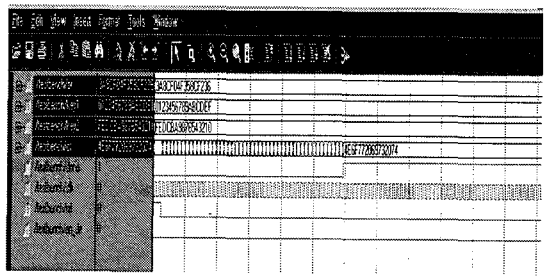

그림 8. Pipelined 3DES 복호화 시뮬레이션 결과
Fig 8. Simulation Result of Decryption for Pipelined 3DES

4.3 성능 평가

파이프라인드 설계 방식이 적용되었을 경우의 성능 향상 정도를 평가하기 위하여, Xilinx사의 CAD 툴을 이용하여 합성 및 시뮬레이션을 수행하였다. Target library는 VertexII를 이용하였으며, 합성시에는 area 우선 옵션을 주었다.

표 1. 성능 평가
Table 1. Performance Estimation

	No. of gates (Silces)	Throughput (Frequency)
DES	28107 (1041)	320Mbps (80Mhz)
3DES	63720 (2360)	106Mbps (80Mhz)
DES*	32778 (1214)	3.8Gbps (70Mhz)
3DES*	110592 (4096)	3.3Gbps (52Mhz)

(*는 파이프라인드 설계가 적용되었음을 의미함)

표 1에서 알 수 있듯이 파이프라인드 설계 기법을 적용할 시, 소요 게이트 수는 다소 증가되지만, 성능은 열 배 이상으로 매우 개선될 수 있음을 확인할 수 있다.

V. 결 론

본 논문에서는 블록 암호 알고리즘을 가속화할 수 있는 파이프라인드 설계 방법을 제시하였다. 제안한 방법에서는 여러 라운드의 암호 연산 블록을 각각의 모듈로 구현하고, 연속적으로 실행하기 때문에 burst 모드에서 전체 연산 속도가 매우 증가 될 수 있다. 하지만, 이 구조는 ECB 모드에서만 효율적으로 적용될 수 있으며, 칩의 면적이 다소 커지게 되는 단점이 있다.

참고문헌

[1] NBS, Data Encryption Standard, FIPS Pub. 46, U.S, National Bureau of Standards, Washington DC. Jan. 1977.

[2] 한국정보보호센터, "128비트 블록 암호알고리즘(SEED) 개발 및 분석보고서", KISA, 2003.

[3] KISA, SEED Algorithm Test Vector, KISA. 2003.

[4] http://www.xilinx.com/

[5] 한국정보보호센터, "128비트 블록 암호알고리즘(SEED) 개발 및 분석보고서", KISA, 2003.

저자소개

이 완 복(Wan-Bok Lee)

2004년 2월 : KAIST 전자전산학과 박사
2003년 3월~현재 : 중부대학교 이공대학 컴퓨터·게임학부 교수

※ 관심 분야: Information Security, Discrete Event System Simulation, Computer Game

김 정 태(Jung-Tae Kim)

2001년 8월 : 연세대학교 대학원 전자공학과 박사
1991년 8월~1996년 2월 : 한국전자통신연구원(ETRI) 선임연구원
2002년 10월~현재 : 목원대학교 공과대학 정보전자영상공학부 교수

※ 관심 분야: Optically fed wireless communi cation system design, Information security system design, Network Security, ASIC Design.