3중 DES 와 DES 암호 알고리즘용 암호 프로세서의 VLSI 설계

°정 진 욱, 최 병 윤
동의대학교 컴퓨터 공학과

VLSI Design OF Cryptographic Processor for Triple DES and DES Encryption Algorithm

°Jin-Wook Jeong and Byeong-Yoon Choi
Department of Computer Eng., Dongeui University

Abstract

This paper describes VLSI design of cryptographic processor which can execute triple DES and DES encryption algorithm. To satisfy flexible architecture and area-efficient structure, the processor has 1 unrolled loop structure without pipeline and can support four standard mode, such as ECB, CBC, CFB, and OFB modes. To reduce overhead of key computation, the key precomputation technique is used. Also to eliminate increase of processing time due to data input and output time, background I/O techniques is used which data input and output operation execute in parallel with encryption operation of cryptographic processor. The cryptographic processor is implemented using Altera EPF10K40RC208-4 devices and has peak performance of about 75 Mbps under 20 Mhz ECB DES mode and 25 Mbps under 20 Mhz triple DES mode.

1. 서 론

정보 보호 기술은 위성 통신, CATV 등을 비롯하여, 각종 통신 이용 산업 및 인터넷 전자 문서 교환(EDI, Electronic Data Exchange)을 포함하는 전자 상거래(EC, Electronic Commerce), 스마트 카드 등의 거의 모든 정보 통신 관련 산업 분야에서 요구되고 있다. 특히 전자 상거래 및 인터넷을 통한 정보 서비스를 사용자들이 신뢰하며 사용하기 위해서는 정보 시스템의 보안과 처리 속도가 우선적으로 보장되어야 한다. 대부분의 정보 보호를 위한 시스템이 소프트웨어 방식으로 구현되고 있어서, 암호화 속도 문제와 해킹에 의한 불법적인 정보 유출의 위험성이 높다. 그러므로 고속 통신 시스템에 암호화를 적용하거나, 키의 보다 안전한 관리를 위해서는 암호 알고리즘의 하드웨어 구현이 필요하다. 현재 보편적으로 널리 사용되고 있는 DES 암호 알고리즘은 고속 프로세서의 개발로 알고리즘 자체의 안전성에 위협이 되고 있는 상황이다. 이에 대한 대안으로 제안된 방법 중 한가지인 3중 DES 암호 알고리즘은 거의 안전한 것으로 평가되고 있다[1].

따라서 본 연구에서는 다양한 응용 분야와 안전성, 기존 시스템과의 호환 등을 고려하여, DES 암호 알고리즘과 3중 DES 암호 알고리즘을 모두 구현하는 암호 프로세서를 설계하였으며, 설계한 프로세서는 FPGA로 구현하여 성능을 분석하였다.

2. DES 와 3중 DES 암호 알고리즘

DES 암호 알고리즘은 IBM의 Lucifier 암호 알고리즘을 기반으로 개발되었으며, Feistel 구조를 갖는 64-비트 데이터와 64비트 키(패리티 비트 8비트 포함)를 갖는 암호 알고리즘이다. 그림 1은 DES 암호 알고리즘의 구조를 나타낸다[2-3].

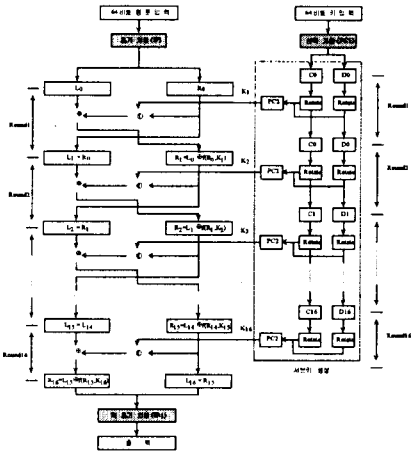

그림 1 DES 암호 알고리즘의 구조

DES 암호 알고리즘은 다양한 Permutation과 Substitution을 통해, Shannon이 제안한 이상적인 암호 시스템의 Diffusion과 Confusion의 근사적인 특성을 구현한다.

현재 1977년에 발표된 DES 암호 알고리즘의 취약성의 개선하기 위한 방안으로 크게 새로운 암호 알고리즘을 사용하는 방안과 다중 DES 암호 알고리즘 방식으로 나뉜다. 첫 번째 방안은 미국의 표준 기술연구소(NIST)가 DES를 대체할 수 있는 새로운 암호 알고리즘 AES(advanced encryption standard)를 공모하여, 조만간 새로운 암호 알고리즘이 선정될 예정이다. 반면 다중 DES 암호 방식은 기존 DES 알고리즘을 반복적으로 적용하여 보안을 강화한 구조이다. 그 중 2개 키를 사용하는 3중 DES 방식이 안전성 측면과 기존 DES와 호환이 쉽게 유지되는 장점이 있어서, 키 관리 표준인 ANS X9.17과 ISO 8732에 표준으로 채택되고 있다. 그림 2는 2개의 키를 갖는 3중 DES 암호 알고리즘에 대한 구조를 나타낸다.

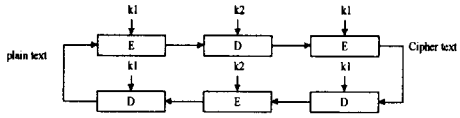

그림 2. 2개 키를 갖는 3중 DES 암호 시스템

3중 DES 방식의 경우, K1 = K2인 경우 기존 DES와 동일한 암호 및 복호화 동작을 할 수 있으며, 현재까지 안전한 시스템으로 평가되고 있다.

그리고 DES의 경우 안전도와 Stream Cipher 응용을 고려하여, 4가지 동작 모드의 구현을 필요로 한다. 3중 DES 시스템의 경우, ECB 모드만 표준으로 정의되어 있는데, CBC, CFB와 OFB 모드에 대한 구현 방안으로 one-loop 구조와 three-loop 구조가 제안되고 있는데, 본 연구에서는 하드웨어 복잡도와 기존 DES 하드웨어 공유 등을 고려하여, one-loop 구조를 사용하여 3중 DES 암호 알고리즘의 CBC, CFB와 OFB 모드를 구현하였다.

3. 암호 프로세서의 VLSI 설계

본 연구의 암호 프로세서는 외부 호스트 프로세서에 대한 암호 보조 프로세서 형태로 설계되어, 다양한 컴퓨터 시스템 환경에 접속이 가능하도록 개발되었다. 그림 3은 암호 보조 프로세서의 전체 구조를 나타낸다. 외부의 데이터 버스를 통해 키와 초기값, 입력 데이터를 입력한다. 단, 암호 동작과 외부 입출력 동작을 동시에 할 수 있도록 하여, 입출력 시간에 따른 성능 저하를 방지하기 위해, 데이터 입·출력 레지스터(I/O R) 과 내부 암호 모듈의 입출력 레지스터(DIN/OUT R)을 분리시켜, start신호

발생 시, 이전 데이터의 암호화 결과와 새로운 입력 데이터가 서로 swap되는 동작을 수행한다. 그리고 암호 연산 수행 동안 Busy Flag가 High상태로 되어, 암호 동작이 진행 중임을 나타낸다. Busy가 High인 동안 Host Processor는 암·복호화 할 새로운 데이터를 IOR에 두고, Busy가 0이 될 때까지 대기한다. 그리고 외부 Host 프로세서가 8 비트, 16비트, 32 비트 등의 다양한 시스템이 가능 할 수 있도록 data_in_out 모듈은 외부 Host 시스템의 특성에 맞게 databus[n-1:0]으로 데이터가 전달될 수 있도록 하는 기능을 담당한다. 여기서 n은 지원하는 Host 프로세서의 데이터 크기를 나타낸다.

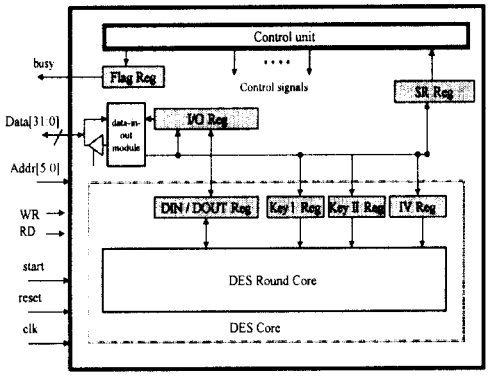

그림 3 암호 프로세서 구조

DES Core는 데이터 Round Core와 Key Round Core로 구성된다. 데이터 Round Core는 64 비트 입력 데이터와 Key Round Core에서 생성한 키를 사용하여, 64비트 암호문 또는 복호문을 생성한다. 단, ECB 모드만을 지원할 경우, 파이프라인 구조를 통해 고속 구현이 가능하지만, 16 라운드가 개별적으로 존재해야 하므로 하드웨어 양이 지나치게 많이 필요하다는 문제가 있다. 그리고 ECB 모드는 동일 입력 값에 대해 동일한 암호문이 생성되므로, 외부 암호 공격에 취약하다는 문제가 있으므로, CBC, CFB, OFB 모드의 구현이 필요하다, 이러한 3가지 모드는 결과 값이 피이드백(feedback)되므로, 파이프라인 구조가 불가능하다. 따라서 이러한 4가지 모드를 구현하기 위해, 1 round 구조의 하드웨어를 배치하고, 16 라운드 동안 반복적으로 사용하는 구조가 바람직하다. 그림 4는 DES의 4가지 암호화 모드와 함께 3중 DES의 암호화 모드를 구현하기 위한 DES core에 대한 구조를 나타낸다.

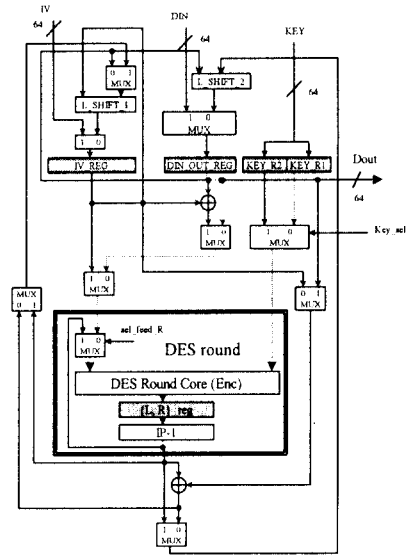

그림 4. DES Core 구조

DES Round Core는 내부에 데이터를 암호화를 위한 Data Round Core와 키를 생성하는 Key Round Core로 구성된다. 그림 5는 DES Round Core에 대한 구조를 나타낸다. 그림 5는 그림 1의 DES 암호 알고리즘의 하나의 라운드를 구현하는 하드웨어를 갖고 있다. 단, 3중 DES 암호알고리즘을 구현하기 위해 결과 값이 출력되지 않고 재사용되는 경우가 있으므로, 그림 5와 같이 Sel_feed_R신호에 따라 이전 결과가 새로운 16 라운드에 대한 입력으로 재사용 될 수 있다. 그리고 그림 1의 DES 암호 알고리즘을 보면 각 Round 동작 전에 key의 계산이 선행되어야 하는데, 이러한 키의 계산은 동작 주파수를 떨어지게 하는 문제를 야기 시킨다. 이러한 문제를 해결하기 위해, 본 연구에서는 각 round보다 하나

앞선 round에서 키를 미리 계산하는 키의 precomputation 기법을 통해 키의 연산 시간이 동작 주파수에 영향을 주는 것을 배제하도록 하여 동작 주파수를 향상시켰다.

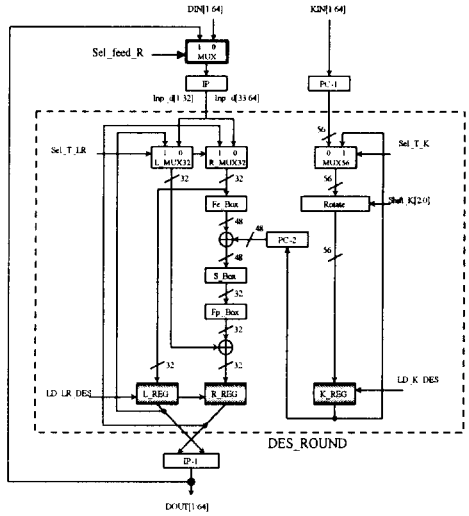

그림 5. Data Round Core 구조

제어 회로는 DES 와 3중 DES 암호 알고리즘에 따라, 동작 흐름을 ASM Chart로 표현한 후, 이를 F/F당 하나의 상태를 할당하는 방식(one-hot assignment) 방식으로 FSM(finite state machine)를 구현하여 제어 회로를 구현하였다.

4. 검증, 성능 분석 및 결론

본 연구에서 설계한 암호 프로세서는 먼저 암호 알고리즘을 C 언어로 모델링 한 후, 이를 Verilog HDL 언어로 변환하여, 2가지 동작이 일치하는 지 확인하는 과정을 사용하였다. 이러한 검증 동작 후에 설계된 회로는 한백 전자 HBE-DTK-40K 실험용 보드의 EPF 10K40RC208-3 칩에 프로그램 한 후, PC에 장착한 ISA 보드를 통해 회로 올바른 동작이 이루어짐을 확인하였다. 그림 6은 암호칩 검증에 사용된 시스템 환경 을 나타낸다. 그리고 표 1은 제작한 암호 칩의 구조적 특성을 나타낸다. 현재 암호칩을 FPGA에 구현하였기 때문에 충분한 동작 속도가 얻어지지 않지만, CMOS 반도체 공정으로 전용 칩 형태로 제작할 경우, 설계한 암호 보조프로세서의 구조적인 특성으로 FPGA 구현에 비해 훨씬 높은 동작 주파수를 얻을 수 있을 것으로 평가된다. 따라서 본 연구에서 설계한 암호 보조 프로세서는 대칭키 암호 알고리즘이 필요한 분야에 적용 가능하다고 판단된다.

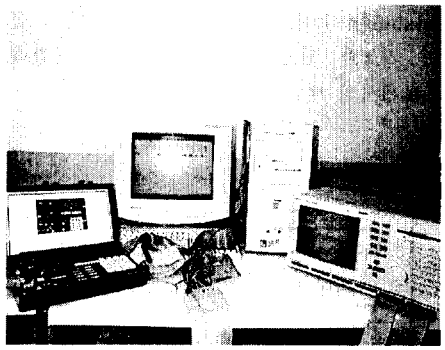

그림 6. 암호 보조 프로세서 검증 환경

표 1. 암호 보조 프로세서의 구조적 특성

지원 암호 알고리즘	DES, 3중 DES
게이트 수	약 28,000
동작 주파수	20 Mhz
최대 성능	75Mbps @ECB, DES 25Mbps @ECB 3중 DES
구현에 사용한 칩	EPF10K40RC208-3

참고 문헌

[1] 최 병 윤, "암호프로세서용 제어기 설계", ETRI 과제 최종 보고서, 1999.11

[2] Hans Eberle, "A High-speed DES Implementation for Network Applications", CRYPTO'92 August 16-20, 1992

[3] Jens-Peter Kaps, High-Speed FPGA Architetcure for the Data Encryption Standard, Mater Thesis, WPI, 1998. 5