DES IP의 HDL 구현

문상국* 김정태*

*연세대학교 전기 • 컴퓨터공학과

HDL Implementation of DES IP

Sangook Moon* Jung-Tae Kim*

*Yonsei University

E-mail : lizking@dubiki.yonsei.ac.kr

요 약

컴퓨터나 각종 전산망의 정보를 보호하기 위해서 가장 안전한 수단은 정보의 직접적인 보호라고 할 수 있는데, 정보사회로 갈수록 지적 재산(IP ; Intellectual Property)이나 기타 다른 중요한 정보의 네트워크를 통한 교류가 활성화될 것이다. 본 연구에서는 이러한 보호의 대상이 되는 정보를 암호화시킬 수 있는 알고리즘에 대한 HDL(Hardware Description Language) 구현을 목표로 한다. 현재까지 수많은 알고리즘이 개발되어 왔지만 DES(Data Encryption Standard)가 가장 기본적이고 모든 블록 암호 알고리즘의 기본이 되기 때문에 본 논문에서는 DES에 대한 기본적인 구조를 제시하고 그에 대한 Verilog-HDL 구현을 목표로 하였다. HDL로 설계된 회로는 LG-0.35um 표준 셀 라이브러리를 사용한 synopsys 툴을 이용하여 합성되었다. 전체 회로의 동작 주파수는 약 236MHz로 예상되고 초당 15104비트의 데이터를 암호화 시킬 수 있다.

Ⅰ. 서 론(휴먼고딕10, 중간정열)

최근 인터넷과 광대역 통신망의 보급으로 전 세계적으로 전자상거래나 정보 보호에 관심이 높아지고 있다. 이러한 주변 여건에서 국내 정보 통신 기술의 외국 종속을 극복하고 세계 시장에 진출하기 위해서는 정보 보호 기술에 대한 투자가 시급하다. 전자 상거래를 포함한 인터넷을 통한 정보 서비스들을 사용자들이 신뢰하고 공급자들이 정보 누출에 대한 위험성에서 벗어날 수 있기 위해서는 정보 시스템의 보안이 최우선적으로 보장되어야 하기 때문에 새로운 정보보호 시스템의 개발은 미래 시장의 선점과 정보 교환 기술의 핵심 기반 기술이 되고 있다.

현재 암호화를 소프트웨어 방식으로 할 경우 속도 문제가 발생할 수가 있고 속도를 빠르게 하기 위해서 암호화의 정도를 약하게 하면 해킹의 위험성이 발생할 수 있다. 따라서 반드시 하드웨어의 도움을 받아서 정보를 암호화 해야 하는데 이에 가장 기본이 되는 알고리즘이 DES이다. 본 논문에서는 DES를 Verilog-HDL로 구현하여 이 알고리즘을 효율적으로 빠르게 처리할 수 있도록 구현한다.

Ⅱ. DES의 구조

DES는 IBM에서 Lucifer 시스템을 개선하여 개발한 암호 시스템으로, 1977년 미국 상무성의 국립 표준국(NBS ; National Bureau of Standard, NBS)에서 미국 표준 암호 알고리즘으로 채택한 64비트 블록의 입력 및 출력을 가지는 64비트 블록 암호이다. 사용되는 64비트의 키 중 56비트는 실제 키가 되고 나머지 8비트는 검사용 비트로 사용된다.

Ⅱ.1. 기본 구조

DES는 기본적으로 16라운드로 구성되며, 암호화는 동일한 동작 과정의 반복으로 이루어진다. 복호화는 암호화 과정과 동일하나 사용되는 키만 역순으로 작용하면 된다. DES를 실현시키는 중요한 기법은 치환(P-box), 대치(S-box), 키 스케줄 등이 있고 기본 구조는 그림1, 그림2와 같다.

정보 암호화부의 내부는 16라운드의 인벌루션(involution) 형태로 되어 있고, 입력부의 초기치환 IP와 출력부의 역초기치환(IP^{-1})으로 구성되어 있다. 구체적인 초기치환은 정해진 표에 의해서

이루어진다.

키 생성부에서는 먼저 64비트의 키로부터 8비트의 패리티 비트가 제거된 다음 나머지 56비트의 키에서 48비트의 동작 키K_i(i = 1, 2, ..., 16)가 생성되어 데이터 암호화부에 작용한다.

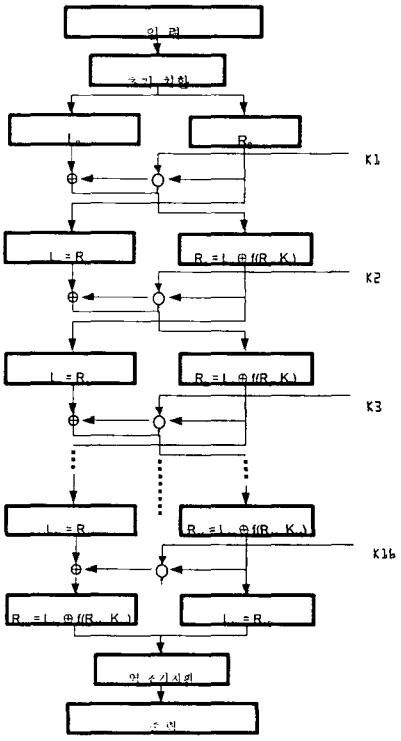


그림 1 DES 블록의 전체 구조도

II.2. f 함수의 구조

f 함수는 크게 선형 구조를 이루는 비트 선택표 E와 치환 P, 그리고 비선형 구조를 나타내는 table look-up 방식인 S-box로 구성되어 있다. 즉 치환(permutation)과 대치(substitution)로 구성되어 있다.

f 함수의 구성도는 그림 2에 나타나 있다. 그림에서 E는 32비트를 48비트로 확장하는 비트 선택표를 사용하고 P는 32비트 선형 치환이다. 8개의 S-box는 비선형적인 성질을 가지는 복잡한 table에 의해 치환된다. 각 S-box는 (4x16)의 행렬 형태로 구성되어 있고, 6비트의 입력 중 최상위 비트와 최하위 비트가 행렬의 행의 어드레스로, 나머지 4비트가 열의 어드레스로 입력되어 이 어드레스에 저장된 4비트의 데이터가 출력되는 비선형 구조로 구성되어 있다. 전체 8개의 S-box의 입력은 48비트이고 출력은 32비트이다. 각 S-box는 그 입력의 1비트 값이 변화했을 때 적어도 출력의 두 비트의 값이 변화하는 성질이 있다.

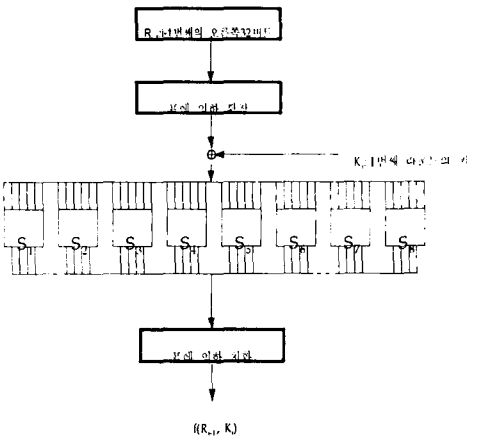


그림 2. f 함수의 구조

II.3. 키 생성부

64비트의 키 데이터는 표에 의한 선택치환에 의해 8비트 검사용 패리티 비트를 제거한 후 나머지 56비트가 28비트씩 나뉘어져 28비트 쉬프트 레지스터 C와 D에 입력된다. 일정 규칙에 의해 레지스터 C_{i-1}과 D_{i-1}의 내용을 1 혹은 2비트씩 좌측으로 쉬프트한 후 또다른 table에 의한 선택치환에 의해 48비트의 라운드 키를 생성한다. 쉬프트 스케줄은 $C_0 = C_{16}$, $D_0 = D_{16}$이 되도록 설계되어 있다. 키 생성부의 블록도는 그림3과 같다.

복호화 과정의 라운드 키 생성 과정은 암호화 과정과 동일하고 쉬프트의 방향만 바뀐다.

II.4. DES의 암호화 복호화 동작

64비트 평문 입력 블록은 초기 치환을 거친 후 좌측 32비트 L(0)와 우측 32비트 R(0)로 나누어진다. 이후 그림 3과 같은 방식으로 라운드 키 K_1, K_2, ..., K_{16}과 결합하여 L(16), R(16)을 발생하고, 역 초기 치환을 거쳐 암호문 블록 64비트를 발생시킨다. 즉,

$$L_r = R_{r-1}$$
$$R_r = L_{r-1} \oplus f(R_{r-1}, K_r) \quad r = 1, 2, ..., 16$$

여기서 f함수는 앞에서 설명한 바와 같다.

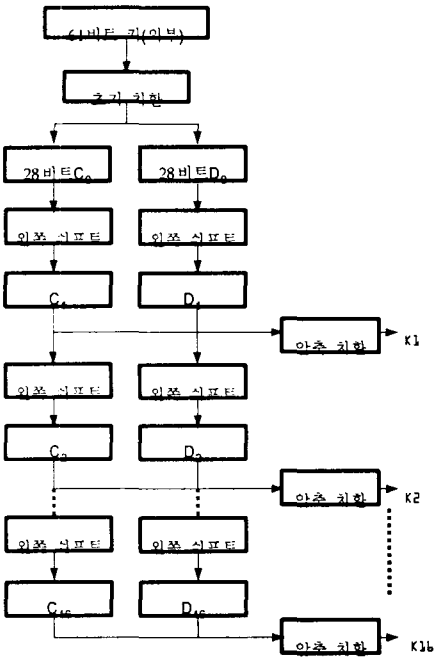
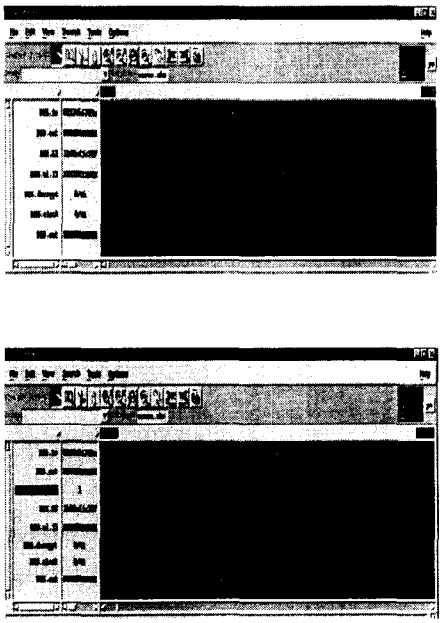


그림 3. DES 키 생성부의 블록도

복호화는 암호화와 동일하며, 다만 키의 입력을 역순으로 수행하면 된다.

III. 알고리즘 구현 및 시뮬레이션

DES 알고리즘을 구현하는 방법은 여러 가지가 있을 수 있는데, 첫 번째는 하나의 라운드만을 가지는 하드웨어 자원을 공유하는 방법이다. 이 방법은 DES의 16 라운드를 하나의 블록을 반복 사용하여 구현할 수 있어 적은 수의 게이트로 구현이 가능하지만 제어가 복잡하고 라운드 수만큼 다음 데이터 블록의 처리가 지연되어 그만큼 시간적인 면에서 손해를 볼 수 있다는 단점이 있다. 두 번째 방법은 16 라운드를 모두 풀어서 구현하는 방법이다. 이 방법은 16개의 라운드에 별도의 하드웨어 자원을 할당하여 구현하는 방법인데 라운드 수만큼 게이트의 수가 소요되게 되지만 블록 버퍼링을 제외한 나머지 16라운드를 파이프라인 처리할 수 있어 고속 동작에 유리하고 그만큼 데이터 처리 속도에 향상을 기할 수 있는 방법이다. 또다른 방법으로는 위 두가지 방법을 혼합하여 n개의 라운드에 하나의 하드웨어 자원을 할당하여 사용하는 방식이다. 이 방법은 1라운드 반복 방식에 비해서는 속도 향상을 기할 수 있지만 제어부가 상당히 복잡해지기 때문에 본 논문에서는 16라운드 블록 방식을 사용하였다. 그림 4에서는 DES IP로 평문 0x0123456789a를 암호화, 복호화 했을때의 암호화 초기단계, 16번째 라운드 암호화 단계, 복호화단계에 대한 파형을 나타낸다. 암호화 단계에서는 16진수 0123456789a 가 16진수 85e813540f0ab405로 변화하는 것을 볼 수 있고 역으로 복호화 하는 경우에는 반대의 경우를 볼 수 있다.



위 시뮬레이션 결과를 바탕으로 synopsys 합성 툴로 합성을 수행하였다. 회로 합성에 사용된 라이브러리는 LG 0.35um 표준공정이고, key 모듈과 block 모듈에 대해서 독립적으로 합성을 수행하였다. key 모듈의 면적 합성결과는 14844개의 NAND 게이트에 해당하는 면적이 예상되었고, typical한 경우에서의 16라운드의 모든 키가 셋업되는데 필요한 시간은 1.87ns였다. block 모듈의 면적 합성 결과는 12517개의 NAND 게이트에 해당하는 면적이 예상 결과로 나왔고 최악 지연 경

로의 지연 시간은 레지스터에서 레지스터까지 4.23ns가 예상되었다. 실제로 이러한 시스템이 적용될 때에는 키가 셋업 된 다음에 데이터의 전달이 이루어지기 때문에 실제 최악 지연 시간은 block 모듈에서 걸리는 것이고 이 모듈을 16라운드 파이프라인 구조로 구현하였기 때문에 이 시스템을 칩으로 구현한다면 결과적으로 약 236MHz에서 매 사이클마다 암호화/복호화된 데이터가 나올 수 있도록 동작한다고 예상할 수 있다. 이 결과는 이렇게 구현된 DES 암호 시스템에서 초당 15104비트의 속도로 암호화/복호화를 수행할 수 있다는 것을 뜻한다. 이 결과를 다음과 같이 표 1에 나타내었다.

표 1. 합성 결과

	Key module	Block module
# of NAND's	14844	12517
Critical Delay	1.87ns	4.23ns

IV. 결론

본 논문에서는 정보보호의 하드웨어적인 기본이 되는 DES IP를 HDL로 설계하고 synopsys 합성 툴로 LG-0.35 표준 셀 라이브러리의 typical한 경우에 대해서 합성을 수행하였다. 회로는 면적에 구애받지 않고 속도를 빠르게 하기 위해서 throutput을 한 사이클에 나오도록 16라운드 전개 방식을 사용하였다. 전체 회로의 면적은 NAND 게이트의 약 2만7천개 정도의 면적이 소요되었고 실제 암호화하는데 필요한 최악 지연 시간은 4.23ns이다. 이를 주파수로 따지면 약 236MHz가 된다. 위 회로 설계에 있어서 s-box table을 구현하는데에 boolean function을 사용하여서 1.63ns의 지연시간이 여기에 해당되는데, 라이브러리에서 보다 속도가 빠른 ROM을 사용할 수 있다면 지연시간을 훨씬 단축시킬 수 있으리라 예상된다.

참고문헌

[1] NBS, "Data Encryption Standard", FIPS Pub. 46, U.S, National Bureau of Standards, Washington DC. Jan. 1997.
[2] 김 철, "암호학의 이해", 영풍문고, 1996.
[3] Bruce Schneier, "Applied Cryptography", 3rd, ed.
[4] Donald E. Thomas, "The Verilog Hardware Description Language", Kluwer Academic Publishers, 1991.
[5]http://aci.net/kalliste/des.htm