PCI Bus 기반의 IPSEC용 Hash 함수의 FPGA 설계

강 용 규, 석 정 희, 최 준 림
경북대학교 전자공학과

요약

Message authentication for information security is an essential technique to verify that received messages come from the alleged source and have not been altered. A key element of authentication schemes is the use of a message authentication code (MAC). One technique to produce MAC is based on hash function and is referred to HMAC. SHA-1, HAS-160 and MD5 are hash algorithms, which have been specified for use in Internet protocol security (IPSEC), as the basis for HMAC. We integrated cryptographic HMAC accelerators based on a hash algorithm such as SHA-1, HAS-160 and MD5. These hash algorithm have been implemented using Altera's EP20K1000EBC652-3 with PCI bus interface.

1. 서론

해쉬 함수는 일반적인 데이터를 일방향 함수를 써서 특정한 비트의 길이로 압축 요약하는 기능을 가진 함수인데 여러 알고리즘들이 알려져 있다. 본 논문에서는 SHA-1, HAS-160, MD5 세 가지 해쉬 함수 알고리즘을 하드웨어로 구현하였다. 실제 전자상거래를 위한 서버를 구축할 때 전자 서명 시스템의 한 요소로 해쉬 함수 연산기가 필요하며 소프트웨어로 구현된 시스템에 비해 속도와 보안 면에서 유리한 특성을 가진다. 세 가지 해쉬 함수 알고리즘을 하드웨어로 구현하기 위해 Verilog HDL을 써서 기술했으며 Altera사의 Quartus tool을 이용해서 컴파일 및 시뮬레이션을 하였고 실제 물리적인 동작검증을 의해 FPGA 디바이스인 Altera EP20K1000EBC652-3에 PCI 인터페이스를 사용해 검증하였다.

2. 전체 하드웨어 구조

원 칩에 SHA-1, HAS-160, MD5 세 개의 해쉬 함수 알고리즘을 연산할 수 있도록 설계하였다. 전체 구조는 그림 1과 같은 블록다이어 그램으로 나타낼 수 있다.

3. SHA-1의 구조

SHA-1의 연산부 전체 구조는 중간값 생성기와 내부 연산 블록들로 구성되어 있고 내부 연산 블록은 쉬프트 연산기, 덧셈기, 부울 연산기 등으로 구성되어 있다 [2]. SHA-1 연산기의 구조도는 그림2와 같다. 160비트 입력 버퍼에는 160비트 초기값이 입력되고 512비트 입력 버퍼에는 512비트 입력데이터가 입력된다. 그리고 중간값 생성회로에서 각 라운드에 필요한 중간값이 컨트롤 회로로 제어되어 출력되어 32×5 덧셈기에 입력된다. 그리고 내부 연산 블록에서는 SHA-1 알고리즘에 의해 연산을 수행한다. 한 클럭에 한 라운드의 연산이 수행되는 구조로 되어 있으며 80클럭에 512비트 블록 입력을 처리할 수 있다.

4. HAS-160의 구조

HAS-160의 연산부의 구조는 SHA-1의 구조와 유사하다. 본 HAS-160 연산기의 구조는 그림3과 같다. 한 클럭에 한 라운드 연산이 수행이 되고 96클럭에 512비트 블록이 처리되는 구조로 되어 있다 [3]. HAS-160이 80단계의 연산 과정을 요구하지만 96클럭이 필요하게 된 것은 연산에 필요한 중간값을 라운드 연산 전에 미리 저장하는 구조이기 때문이다. 15클럭을 중간값 생성을 위해 라운드 연산 전에 소비한다.

5. MD5의 구조

MD5의 하드웨어 구조도 위의 두 알고리즘의 하드웨어 구조와 큰 차이가 없다. 하지만 MD5의 경우 128비트 초기값을 가지므로 내부 연산 과정이 위의 두 알고리즘에 비해 단순해지고 연산의 중간값을 생성하는 회로가 512비트 입력값의 선택적인 와이어링에 불과 하기 때문에 멀티플렉서 하나로 쉽게 구현이 된다 [1]. 그림4는 MD5의 블록다이어그램이다.

6. 성능 분석

본 논문에서 제시한 해쉬 함수 연산기는 Altera사의 Quartus II를 이용해 설계 및 타이밍 시뮬레이션을 하였다. 실제 제작하는데 사용한 디바이스는 EP20K1000EBC652-3을 사용하였고 PCI 인터페이스를 통해 시스템을 구현하였다. 전체 시스템은 그림5와 같으며 성능 분석 결과는 표 1과 같다.

7. 결론

본 논문에서는 전자 서명 시스템의 구현을 위한 해쉬 함수 연산기의 설계 및 구현을 그 목적으로 하였다. 수행 시간의 측면에서 보면 SHA-1의 해쉬 함수 연산을 81클럭에 수행할 수 있으며 HAS-160은 96클럭, MD5는 65클럭에 수행할 수 있고 설계한 회로의 최고 동작 주파수는 SHA-1가 18MHz이고 HAS-160는 30MHz 그리고 MD5는 18MHz에서 동작 확인하고 PCI bus를 이용하여 PC 기반에서 검증하였다.

참고 문헌

[1] R. Rivest, "The MD5 Message-Digest Algorithm," RFC 1321, MIT LCS & RSA Data Security, Inc., April 1992.

[2] National Institute of Standards and Technology, "Secure Hash Standard (*SHA-1*)," Federal Information Processing Standards Publication #180-1, 1993.

[3] 한국정보통신기술협회, "해쉬 함수 알고리즘 표준 (*HAS-160*)," TTAS. KO-12.0011, 2000.

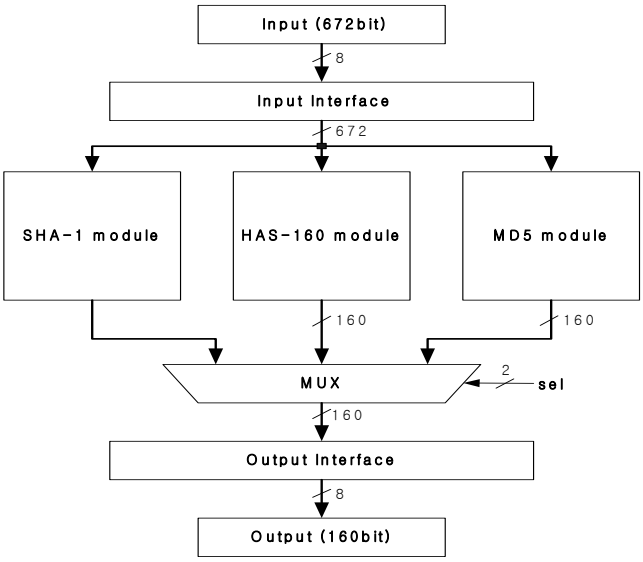

그림 1. 해쉬 연산기의 전체 블록도

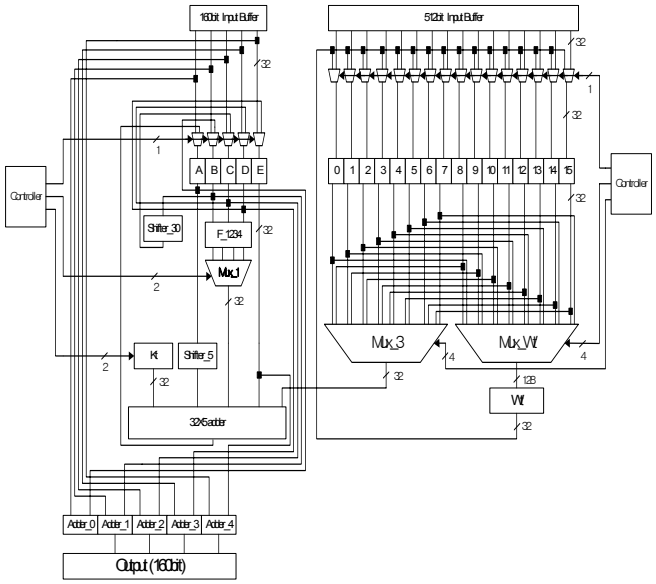

그림 2. SHA-1 전체 연산기 구조

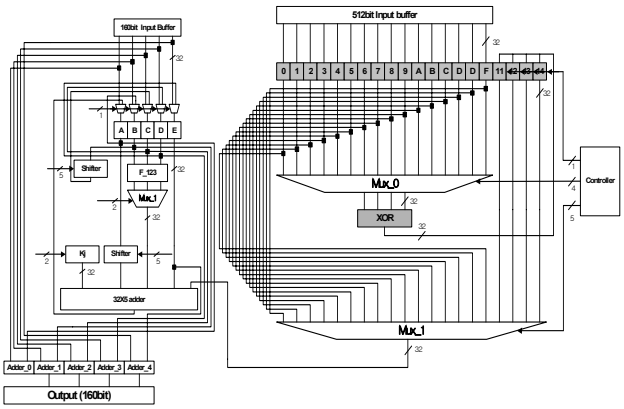

그림 3. HAS-160 전체 연산기 구조

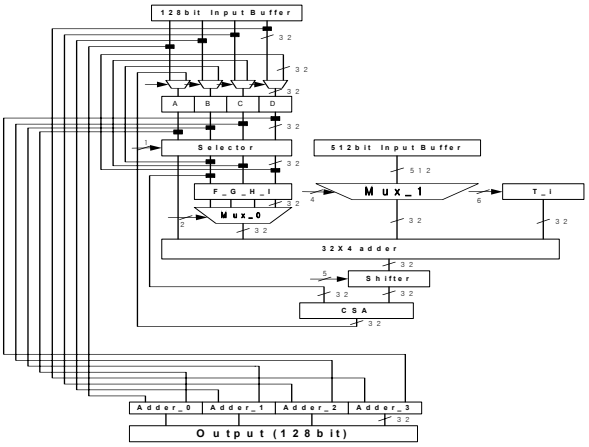

그림 4. MD5 전체 연산기 구조

그림 5. PCI 인터페이스를 사용한 해쉬 함수 연산기의 전체 시스템

표 2. 동작 성능 분석표

	SHA-1	HAS-160	MD5
Clock Cycles	81	96	65
Frequency	18MHz	30MHz	18MHz
Throughput	114Mbit/s	160Mbit/s	142Mbit/s