정보보호 시스템을 위한 재구성형 프로세서 설계†

차정우*, 김일휴*, 김창훈**, 김동휘**
*대구대학교 컴퓨터정보공학과
**대구대학교 컴퓨터·IT공학부
e-mail:cjw3827@gmail.com

Design of Reconfigurable Processor for Information Security System

Jeong-Woo Cha*, Il-Hyu Kim*, Chang-Hoon Kim**, Dong-Hwi Kim*
*Dept of Computer and Information Engineering, Daegu University
**School of Computer and IT Engineering, Daegu University

요 약

최근 IT 기술의 급격한 발전으로 개인정보, 환경 등 다양한 정보를 수시로 수집 및 관리하면서 사용자가 원할시 즉각적인 정보서비스를 제공하고 있다. 그러나 유·무선상의 데이터 전송은 정보의 도청, 메시지의 위·변조 및 재사용, DoS(Denial of Service)등 외부의 공격으로부터 쉽게 노출된다. 이러한 외부 공격은 개인 프라이버시를 포함한 정보서비스 시스템 전반에 치명적인 손실을 야기 시킬 수 있기 때문에 정보보호 시스템의 필요성은 갈수록 그 중요성이 부각되고 있다. 현재까지 정보보호 시스템은 소프트웨어(S/W), 하드웨어(ASIC), FPGA(Field Progr- ammable Array) 디바이스를 이용하여 구현되었으며, 각각의 구현방법은 여러 가지 문제점이 있으며 그에 따른 해결방법이 제시되고 있다.

본 논문에서는 다양한 환경에서의 정보보호 서비스를 제공하기위한 재구성형 SoC 구조를 제안한다. 제안된 SoC는 비밀키 암호알고리즘(AES), 암호학적 해쉬(SHA-256), 공개키 암호알고리즘(ECC)을 수행할 수 있으며, 마스터 콘트롤러에 의해 제어된다. 또한 정보보호 시스템이 요구하는 다양한 제약조건(속도, 면적, 안전성, 유연성)을 만족하기 위해 S/W, ASIC, FPGA 디바이스의 모든 장점을 최대한 활용하였으며, MCU와의 효율적인 통신을 위한 I/O 인터페이스를 제안한다. 따라서 제안된 정보보호 시스템은 기존의 시스템보다 다양한 정보보호 알고리즘을 지원할 뿐만 아니라 속도 및 면적에 있어 상충관계를 개선하였기 때문에 저비용 응용뿐만 아니라 고속 통신 장비 시스템에도 적용이 가능하다.

1. 서론

최근 휴대폰, 무선 랜, 블루투스와 같은 모바일 컴퓨팅 디바이스의 급속한 발전과 무선 랜, 블루투스 등 통신장비의 성능 향상 및 가격 하락으로 모바일 컴퓨팅 디바이스 간의 통신이 보편화 되었다. 뿐만 아니라 RFID 시스템, 무선 센서 네트워크 등 초소형 전자 디바이스까지 망으로 연결되어 인산의 삶을 개선시켜주는 유비쿼터스(Ubiquitous) 환경이 급속히 진행되고 있다.

이러한 IT 기술은 개인정보, 환경 등 다양한 정보를 수시로 수집 및 관리하면서 사용자가 원할시 즉각적인 정보서비스를 제공해야 한다. 그러나 유·무선을 통한 데이터 전송은 정보의 도청, 메시지의 위·변조 및 재사용, DoS(Denial of Service)등 외부의 공격으로부터 쉽게 노출된다. 이러한 외부 공격은 개인 프라이버시를 포함한 정보서비스 시스템 전반에 치명적인 손실을 야기 시킬 수 있다[1].

그러므로 정보보호 시스템은 매우 중요한 문제로 인식되어 현재 국·내외에서 다양한 연구를 진행 중에 있으며, 연구 분야는 크게 보안 정책, 보안 프로토콜, 인증 기법, 키 관리 기법, 암호 및 해쉬 알고리즘 설계, 암호 알고리즘의 효율적인 소프트웨어 및 하드웨어 구현으로 구분 할 수 있다[2].

현재까지 정보보호 시스템은 소프트웨어(S/W), 하드웨어(ASIC), FPGA(Field Progr- ammable Array) 디바이스를 이용하여 구현되었다. S/W의 구현은 다양한 정보보호 알고리즘에 대해 높은 유연성을 제공하나 속도, 전력, 안전성 측면에서 매우 취약하며, ASIC 구현은 속도, 전력 측면에서는 매우 우수하지만 구현의 특성상 다양한 보안 플랫폼을 지원할 수 없다. 이러한 문제점들의 상충관계를 개선하기 위해 최근 FPGA 디바이스 상에서의 구현이 많이 이루어 졌다. 그러나 FPGA 디바이스 역시 면적, 속도, 전력 측면에서는 ASIC 구현에 비해 현저히 낮은 성능을 보인다.

본 논문에서는 이러한 문제점들을 해결하기 위해 Configurable 하드웨어를 포함한 Reconfigurable SoC 기술을 적용한 정보보호 시스템을 개발하려 한다[3]. Reconfigurable SoC 기술은 S/W, ASIC, FPGA 디바이스가 혼합된 형태로서 S/W, ASIC, FPGA 구현의 모든 장점을 얻을 수 있다. 따라서 정보보호 시스템에 Reconfigurable SoC 기술을 적용한다면 다양한 정보보호

† 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2010-0006324)

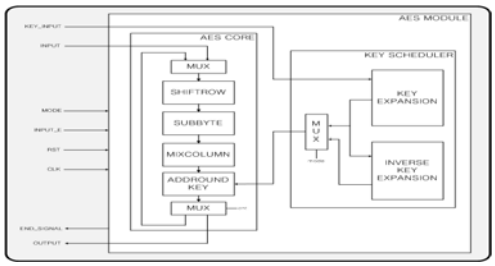
프로토콜이 요구하는 성능요소(속도, 면적, 전력, 유연성, 안전성)를 만족 시킬 수 있다.

2. 정보보호 모듈 설계

2.1 32bit 기반 AES 설계[4]

본 AES 모듈은 32bit 입력과 32bit 출력으로 이루어져있다. 128bit의 Data와 Key Data를 32bit씩 입력받아 출력하도록 되어있다.

기존의 AES 모듈들을 보면 128bit의 Data를 한 번에 처리 하도록 되어있어서 메모리 낭비 및 하드웨어 면적이 넓은 문제점을 가지고 있지만 본 논문에서는 32bit씩 4번 수행하도록 되어있어서 메모리 및 하드웨어의 낭비를 감소시킨다. 그러나 수행 횟수가 늘어나기 때문에 처리속도는 기존의 방식에 비해 증가한다.



(그림 1) AES 모듈 전체 구조

AES의 SubByte에 대한 S-box table 정보는 내부 ROM에 저장하도록 설계되어있다. 내부 ROM에 S-box table 정보를 저장함으로써 S-box의 값을 구하기 위한 연산을 수행하지 않아도 되는 이점이 있으며 연산을 하지 않아도 되기 때문에 향상된 높은 속도를 보여준다. ShiftRow 연산에서는 128 bit의 데이터를 시프트 연산이 이루어지도록 되어있다. 그러나 본 논문의 AES 모듈은 32bit씩 연산이 이루어지기 때문에 ShiftRow연산을 하기 위해서는 128 bit 데이터를 저장을 해놓아야 한다. 그 방법으로는 Shift-Register를 이용하여 한 클럭마다 32bit씩 데이터를 출력하도록 모듈을 구성하였다.

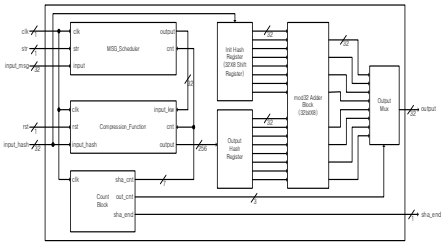
본 논문에서의 Mixcolumn은 내부적으로 암호화에 사용되는 Forward Mixcolumn과 복호화에 사용되는 Inverse Mixcolumn 두 개의 부분으로 구성되어있다. 32비트 단위의 데이터 처리를 하기위해 각 모듈은 32비트 데이터를 입력으로 취하고 32비트 Mixcolumn 값을 출력한다. 입력된 32비트 데이터는 8bit 씩 4개의 원소로 분리된 원소들은 4개의 32비트 레지스터에 8비트 단위로 쉬프트 되어 저장되고 이후 비트단위 쉬프트 연산과 XOR 연산을 통해 새로운 32비트 워드로 출력된다.

GF(2^8)에서의 덧셈은 비트단위 XOR 연산으로 간단하게 구해지며 곱셈은 좌측 쉬프트 연산으로 구할 수 있다. 비트단위 쉬프트 연산에서 최상위 비트가 1이면 x^4, x^3, x, 1에 해당하는 비트에 최상위 비트를 더함으로써 곱셈 연산을 간단하게 구현하였으며 병렬적으로 32비트 데이터를 처리함으로써 처리 속도를 향상시켰다.

2.2 32bit 기반 SHA-256 설계

그림 2는 본 논문에서 설계한 SHA-256의 전체적인 구조를 나타낸다. 설계된 SHA-256은 크게 2개의 블록 Message Scheduler와 Compression Function 블록과 이들은 포함하는 IO Interface 블록으로 구성된다.

IO Interface는 SHA-256 연산에 필요한 512 비트의 메



(그림 2) SHA-256 하드웨어 구성도

시지 블록, 한 블록의 메시지 처리를 위해 입력되는 초기 해쉬 값, 시작을 알리는 str 신호와 리셋을 알리는 rst 신호를 입력으로 받아 Message Scheduler 블록과 Compression Function 블록에 전달하는 역할을 한다. 또한, 연산이 완료된 256 비트의 해쉬 값을 매 clock 마다 32비트 씩 8번 출력하는 역할도 한다.

SHA-256의 처리 과정에서의 데이터는 32비트를 기본단위로 연산이 이루어지며 하나의 Count Block을 사용하여 전체적인 데이터 및 연산의 동기를 맞추도록 설계되었다. 모든 연산을 마친 결과는 최초 입력으로 사용되었던 초기 해쉬 값에 더해져 최종 결과로 출력된다. SHA-256에서 사용되는 덧셈은 mod 32에서 이루어지는 덧셈이므로 초기 값과 연산결과로 얻은 해쉬 값을 mod32 Adder 블록에 의해 각 32 비트씩 덧셈을 하여 Output Mux에 연결된다.

Message Scheduler는 512 비트 메시지 블록을 입력으로 64개의 32비트 워드를 출력한다. 0에서 15 clock 동안에 주어지는 입력은 블록의 쉬프트 레지스터에 연결되어 순차적으로 값이 채워지게 되며 이후 채워진 값들은 σ0, σ1, 논리 함수를 통과하여 mod 32 Adder에 의해 더해져서 확장된 워드를 생성하게 되고, 이렇게 생성된 워드들은 다시 쉬프트 레지스터의 입력으로 주어지게 된다.

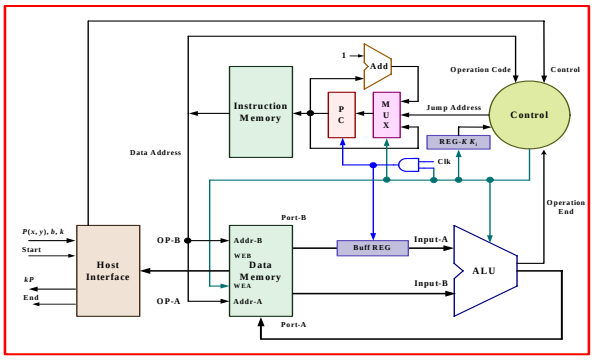
Message Scheduler의 출력은 Compression Function의 입력으로 연결된다. 쉬프트 레지스터의 R0 레지스터에서 출력을 내보내지 않고 R9 레지스터에서 출력을 내보내는 것은 초기화 해쉬 값의 입력이 끝나는 타이밍과 맞추어 Compression Function의 연산을 수행하기 위함이며 이러한 설계는 R8 레지스터부터 R0 레지스터까지 데이터가 이동해서 출력되는 9 클록을 줄여주기 위함이다.

SHA-256의 핵심은 압축 함수이다. IO Interface에서 입력되는 값 중 Input_hash 값은 Compression Function에서 해쉬 연산의 초기 값으로 입력된다. 32비트 워드의 해쉬 값을 8번, 총 256비트를 입력으로 취한다. 입력이 끝나는

시점에서 Message Scheduler 블록에서 확장된 워드인 w와 SHA-256 상수인 k값이 더해져서 Compression Function의 입력으로 들어오게 된다. IO Interface에서 입력되는 카운트 값을 통해 초기 해쉬 값 256비트가 입력되는 동안에는 연산을 매인 루프에 값을 넣지 않게 되며 초기 해쉬 값의 입력이 끝나면 매인 루프에 값을 전달하는 구조로 설계되었다. 이 후 연산된 해쉬 값은 다시 매인루프로 전달되어지며 총 64번의 반복을 통해 최종 해쉬 값을 얻어낸다. 출력된 결과는 IO Interface에서 초기화 해쉬와 더해져 최종 결과를 출력한다.

2.3 Elliptic Curve Cryptosystem(ECC) 설계[5][6]

그림 4은 본 논문에서 설계한 타원곡선 암호프로세서의 전체적인 구조를 나타낸다. 본 연구에서 개발된 타원곡선 암호 프로세서는 크게 5개의 블록 Host Interface, Data Memory, Instruction Memory, Control, ALU로 구성된다. Host Interface는 타원곡선의 베이스 포인터, 곡선 파라메타 b, 비밀키 k 그리고 연산의 시작을 알리는 start 신호를 Host 프로세서로부터 입력 받아 타원곡선 암호프로세서로 전달한다. 타원곡선 프로세서의 데이터 전송 및 연산은 모두 163-비트로 이루어지며, Instruction Memory로부터 명령어 및 데이터 메모리의 주소를 전송받아 컨트롤 신호와 함께 연산을 수행한다.

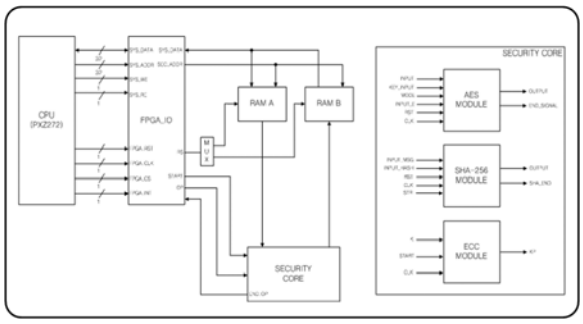


(그림 4) GF(2^{163})상의 타원곡선 암호 프로세서 구조

Data Memory는 Dual Port 메모리로 구성하였으며, Port-A는 상승 에지에 Port-B는 하강 에지에 각각 동작한다. 그 외 모든 연산기 및 레지스터는 상승 에지에 동작한다. 따라서 데이터의 동기를 맞추기 위해 ALU의 Input-A와 Data Memory의 Port-B 사이에 Buffer 레지스터를 두었다. 따라서 모든 연산은 4사이클(명령어 패치 + 데이터 패치 + 데이터 로더 + 연산 수행 및 저장) 만에 수행된다. 곱셈 연산의 경우 $\lceil m/d+1 \rceil$ 사이클이 소요되며, 나눗셈 연산의 경우 Kim 등이 제안한 확장 바이너리 GCD 알고리즘을 이용하여 2m 사이클이 소요된다.

3. Integrated Interface의 전체 구조

본 논문에서 구현된 보안 모듈은 하나의 공통된 인터페이스를 공유함으로써 통합된 형태로 구현된다. Security Core는 구현된 보안 모듈인 AES와 SHA-256, ECC 모듈이 포함되며 각각의 모듈은 FPGA_IO 모듈을 통해 제어신호와 입력 값을 전달받게 된다. FPGA_IO 모듈은 보드상의 CPU인 PXZ272로부터 데이터와 제어신호를 전달받게 되며 전달된 데이터는 사용되어질 보안 모듈에 따라 RAM_A와 RAM_B에 입력시킨다. 또한 전달된 제어신호는 Security Core에 입력되어 주어진 데이터가 어떠한 모듈을 사용할지 결정하게 된다. 보안 모듈의 수행을 거친 데이터는 RAM_B에 적재되고 이와 동시에 출력되는 end 신호에 의해 다시 CPU로 출력한다. 아래의 그림 5는 설계된 Total Interface의 전체 구조를 나타낸다.

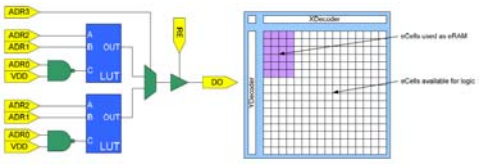


(그림 5) Integrated Interface 전체 구조

메인 CPU와 연결된 인터페이스이다. Security Module과 내부 RAM 및 내부 ROM의 제어를 맡고 있고 내부 레지스터 맵의 정보에 따라 데이터를 각각의 모듈에 전송한다.

3.1 내부 RAM

보안 모듈에서의 암호화 데이터 및 암호 키 값을 저장하기 위해서 설계되었다. 아래 그림 6는 eASIC社의 eRAM 구조를 나타내고 있다. eRAM은 Nextreme 구조의 ASIC 장치에서 사용하는 전용 메모리이다. 각각의 암호 모듈이 RAM의 주소를 참조하여 데이터를 송 · 수신 받는다.



(그림 6) eASIC社의 eRAM 구조

3.1 내부 ROM

각각의 보안 모듈에서의 미리 정의된 데이터에 대해서는 ROM에 저장하도록 설계가 되어있다. 예를 들어 AES의 S-Box, ECC 연산에 필요한 명령어 Set, SHA-256 연산에 필요한 상수 값은 암호 모듈 연산에 필수 데이터이고 연산을 하더라도 변하지 않는 값이므로 ROM에 저장하여 읽기만 수행하도록 설계하였다. 아래 그림 7은 eASIC社의 eROM 구조를 나타내고 있다. eROM에서 'write' 기능이 있지만 본 논문에서는 그 기능은 사용하지 않는다.

4. 성능 평가

본 장에서는 설계한 SoC의 성능을 평가하기위해 정보보호 시스템을 위한 구현 환경 을 설명하고, 그 결과를 바탕으로 본 논문에서 제안한 시스템의 성능을 분석한다.

4.1. 성능 평가 환경

본 논문에 제안된 정보보호 시스템의 FPGA 구현 및 기능 검증을 위해 VHDL로 회로를 기술하였고, Xilinx사의 회로합성 툴(XST : Xilinx synthesis technology)을 사용하여 회로를 합성, Net-list 파일을 추출한 후, Mento Graphics 사의 ModelSim SE 6.0을 이용하여 시뮬레이션 하였다. 또한 Xilinx사의 ISE 10.0i를 이용하여 Place & Route 과정을 거친 후, 타이밍 및 칩 사용율에 대해 분석하였다. FPGA 칩은 Xilinx사의 Virtex4 시리즈인 XC4VLX60을 대상 디바이스로 선택하였다.

4.2. 제안된 정보보호 시스템의 결과 분석

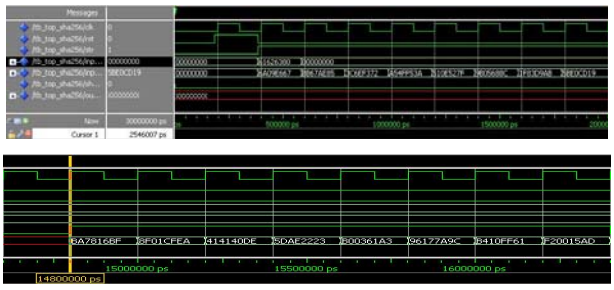
본 절에서는 본 논문에서 제안한 정보보호 시스템의 구현 결과를 분석한다. 제안된 정보보호 시스템은 기존의 한 가지의 보안 표준만을 지원하는 정보보호 시스템에 비해 여러 가지 보안 표준을 선택적으로 사용할 수 있으며 사용자의 설정에 따라 여러 가지의 보안 표준을 결합하여 사용할 수 있도록 설계되어있다.

(그림 9) AES 테스트 결과

<표 2> AES 구현 결과

SLICE 개수	LUT	FF	최대 주파수
1898	3657	399	87MHz

SHA-256 모듈을 테스트하기 위해 표준 문서의 테스트 값인 "abc" 문자열을 사용하여 테스트 하였다. 본 논문에서 설계된 SHA-256 모듈은 메시지와 초기 해쉬값을 입력으로 주어야하기 때문에 입력으로 해쉬값이 같이 주어진다.



(그림 10) SHA-256 테스트 결과

<표 3> SHA-256 구현 결과

SLICE 개수	LUT	FF	최대 주파수
1994	3359	1320	43MHz

ECC 모듈의 입력 값으로는 키 값인 k와 두 좌표인 x, y 값을 넣어주었으며 그 결과는 그림 11와 같이 출력되었다.

(그림 11) ECC 테스트 결과

<표 4> ECC 구현 결과

SLICE 개수	LUT	FF	최대 주파수
5195	9640	2120	106MHz

5. 결론

본 논문에서의 정보보호 시스템을 위한 재구성형 SoC는 최신 정보보호 시스템의 다양한 요구사항인 속도, 면적, 전력, 유연성, 안전성을 만족시키기 위해서 S/W, ASIC, FPGA 디바이스의 모든 장점을 가진 정보보로 시스템을 제안하고 그 요구사항에 최적화된 정보보호 모듈과 FPGA 통합 인터페이스를 개발하였다.

제안된 정보보호 시스템은 다양한 정보보호 알고리즘과 그 알고리즘을 제어 및 CPU 통신을 위한 FPGA 통합 인터페이스, ROM, RAM으로 구성되어있다. 정보보호 시스템에서 고속의 처리가 필요한 부분인 RAM과 ROM은 ASIC으로 구성하고 추가 확장이 가능한 정보보호 프로토콜 및 인터페이스 부분은 FPGA로 구현하여 시스템의 성능을 높였으며 추가, 확장이 용이하도록 레지스터 맵으로 구성하였다.

기존의 시스템에서 하나의 정보보호 알고리즘만 지원하는 방식이 아닌 다양한 정보보호 알고리즘을 지원하여 그 활용도를 높였으며, 파라미터에 따라 속도 및 면적에 있어 상충관계를 개선할 수 있기 때문에 RFID/USN과 같은 저비용의 응용 뿐만 아니라 VPN과 같은 고속 통신 장비 시스템에도 적용이 가능하기 때문에 그 활용분야는 매우 높을 것으로 예상한다.

참고문헌

[1] 김신효, 강유성, 정병호, 정교일, "u-센서 네트워크 보안 기술 동향," 전자통신동향 분석, Vol. 20, No. 1 pp. 93-99, 2005. 2월.

[2] 주학수, 주홍돈, 김승주, "고속 암호연산 프로세서 개발 현황", 정보보호학회지, 제 12권, 제 3호, pp. 48 - 56, 2002. 6.

[3] J.R. Goodman, Energy Scalable Reconfigurable Cryptographic Hardware for Portable Applications, PhD thesis, MIT, 2000.

[4] NIST, Advanced Encryption Standard(AES), FIPS 197, 2001.

[5] N. Koblits, "Elliptic Curve Cryptosystems," Mathematics of Computation, Vol. 48, No.177, pp. 203-209, 1987.

[6] 5.S. Miller, "Use of Elliptic Curves in Cryptography," in Advances in Cryptology-Proc. of CRYPTO'85, pp. 417-426, 1986.