7.8Gbps 파이프라인 LEA 크립토 프로세서

성미지* · 신경욱*

*금오공과대학교

A 7.8Gbps pipelined LEA crypto-processor

Mi-ji Sung* · Kyung-wook Shin*

*Kumoh National Institute of Technology

E-mail : smj920307@kumoh.ac.kr

요 약

3가지 마스터키 길이 128/192/256 비트를 지원하는 파이프라인 LEA(Lightweight Encryption Algorithm) 크립토 프로세서를 설계하였다. 높은 처리율을 얻기 위해 16개의 라운드 스테이지가 파이프라인 방식으로 동작하며, 각 라운드 스테이지는 128비트 데이터패스를 갖도록 설계하였다. 설계된 LEA 프로세서는 FPGA 구현을 통해 하드웨어 동작을 검증하였다. Xilinx ISE로 합성한 결과, 최대 동작주파수 122MHz로 동작하여 7.8Gbps의 성능을 갖는 것으로 평가되었다.

키워드

LEA, Block cipher, Information Security, Secret Key Encryption

Ⅰ. 서 론

정보통신 기술의 발달에 따라 인터넷에 연결된 다양한 기기들이 사람의 개입이나 지시를 받지 않고, 실시간으로 데이터를 주고받아 처리하는 사물인터넷(Internet of Things; IoT) 기술이 보편화되고 있으며, 모든 IoT 기기가 보안공격의 대상이 될 수 있으므로 정보보안 기술의 적용이 필수적이다. 최근에는 IoT 보안에 적합하도록 개발된 저전력/저면적의 경량 블록암호 알고리듬에 대한 연구가 활발히 이루어지고 있다. 사물인터넷이 보편화되면서 센서 네트워크에 의해 수집된 대량의 데이터를 안전하게 전송, 저장하기 위해서는 보안 알고리듬의 고속 하드웨어 구현이 필요하다.

본 논문에서는 국가보안기술연구소에서 개발한 128비트 경량 블록암호 LEA를 고성능 보안시스템에 적합하도록 파이프라인 구조를 적용하여 구현하였으며, FPGA 구현을 통해 하드웨어 동작을 검증하였다.

Ⅱ. 블록암호 LEA

LEA는 128/192/256 비트의 마스터키를 이용하여 평문/암호문을 128 비트 단위의 블록으로 암호화/복호화 하여 128 비트의 암호문/평문을 생성하는 대칭키 방식의 블록 암호 알고리듬이다. ARX(Addition-Rotation-XOR) 연산을 기반으로 하는 Type-3 Feistel 구조이며, 벨기에 COSIC 연구소로부터 안전성을 검증받았다[1]. LEA의 라운드 함수 연산은 32 비트 단위로 구성되어 있어 소프트웨어 플랫폼에서 고속으로 동작이 가능하며, 또한 비선형 치환 S-Box를 사용하지 않아 하드웨어 구현에도 적합한 것으로 평가된다[2].

그림 1은 LEA의 암호/복호 과정을 보인 것이다. Round^{enc}과 Round^{dec}은 각각 암호화 라운드 함수와 복호화 라운드 함수를 나타내며, RK_i^{enc}과 RK_i^{dec}은 각각 i번째 라운드 함수에 사용되는 암호화 라운드 키와 복호화 라운드 키를 의미한다. Nr은 마스터 키 길이에 의해 결정되는 라운드 수, X_i는 $i-1$번째 라운드 함수에서 출력되어 i번째 라운드 함수에 입력되는 128 비트 내부 상태 변수를 나타낸다.

전체구조는 128/192/256 비트의 마스터 키로부터 192 비트의 라운드 키를 생성하는 키 스케줄러와 암호화/복호화 연산을 수행하는 라운드 함수로 구성된다. 라운드 함수는 128/192/256 비트의 키 길이에 따라 24/28/32번 라운드 변환을 수행하며, 키 스케줄링 또한 라운드 변환과 동일한 횟수로 수행된다. 암호화와 복호화는 서로 역연산으로 구현되며, 라운드 키도 역순으로 사용된다.

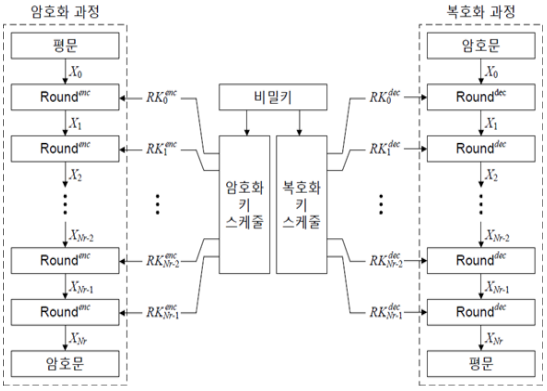

Figure 1. Encryption and decryption of LEA

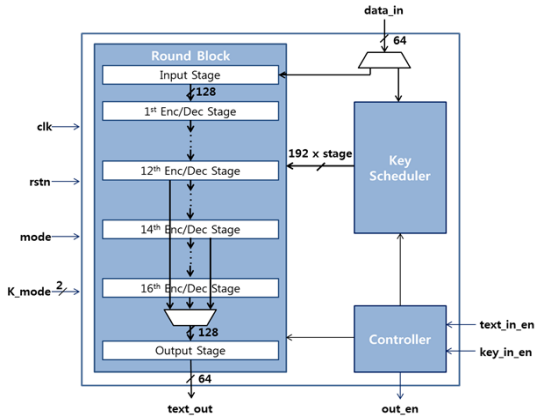

Figure 2. Structure of LEA crypto-processor

III. LEA 암호/복호 회로 설계

128/192/256 비트의 마스터키로 128 비트의 데이터 블록을 암호화/복호화 하여 128 비트의 암호문/평문을 생성하는 LEA 크립토 프로세서를 설계하였다. 처리율을 높이기 위해 파이프라인 구조를 적용하였고, 라운드 함수를 데이터 블록의 크기인 128 비트의 데이터패스로 설계하였다. 설계된 LEA 프로세서의 구조는 그림 2와 같으며, 라운드 블록, 키 스케줄러 블록, 제어 블록으로 구성된다.

3.1 라운드 블록

라운드 블록은 입력 스테이지와 16개의 라운드 스테이지 그리고 출력 스테이지로 구성되며, 마스터 키 길이(128/192/256 비트)에 따라 12/14/16개의 라운드 스테이지가 사용된다. 각 스테이지에서 2회의 라운드 연산이 수행되며, 전체 라운드 스테이지는 파이프라인 방식으로 동작한다. 암호 라운드 연산은 XOR, 모듈로 가산, 비트 순환이동, 바이트 순환이동 등으로 이루어지며, 복호 라운드 연산은 암호 연산의 역연산 과정이다.

입력되는 128 비트의 평문/암호문은 64 비트 단위로 2클록 주기에 걸쳐 입력 스테이지 레지스터에 저장된다. 128 비트의 평문/암호문의 입력과 키 스케줄러에서 키 생성이 완료된 후, mode 신호에 따라 암호화 또는 복호화 라운드 연산이 수행된다. 1 클록 주기에 한 라운드 연산이 처리되며, 라운드 변환이 완료되면 128 비트의 암호문/복호문이 출력 스테이지를 거쳐 64 비트 단위로 2 클록 주기에 거쳐 출력된다.

3.2 키 스케줄러 블록

암호/복호 라운드 연산에 사용되는 192 비트 라운드 키는 키 스케줄링 알고리듬에 의해 생성된다. 본 논문에서 설계된 키 스케줄러는 마스터 키로부터 라운드 키를 확장하는 키 스케줄러와 각 라운드에서 사용되는 라운드 키를 저장하는 키 저장 레지스터를 포함한다. 키 스케줄러는 키 스케줄링 알고리듬에 기반하여 설계되었으며, 마스터 키와 첫 번째 데이터 블록이 입력된 다음에 키 확장을 수행한다. 암호화 라운드 키 확장은 상수 생성기에서 생성된 상수 값을 이용한 모듈로 가산과 비트 순환이동을 통해 이루어지며, 복호화 라운드 키 확장은 역연산 과정으로 이루어진다. 생성된 192 비트의 라운드 키는 키 저장 레지스터에 저장되고, 모든 라운드의 라운드 키 생성이 완료되면 데이터 블록의 라운드 변환이 시작된다. 암호화/복호화 과정 중에는 키 스케줄러의 키 확장이 실행되지 않고, 키 저장 레지스터에 저장된 라운드 키 값이 사용된다.

설계된 키 스케줄러 블록은 마스터 키의 길이(128/192/256 비트)와 암호/복호 모드에 따라 동작이 달라진다. 라운드 블록과 마찬가지로, mode 신호에 따라 암호화 키 스케줄링 또는 복호화 키 스케줄링이 이루어지고, 마스터 키 길이에 따라 LEA-128, LEA-192, LEA-256 모드의 키 스케줄링이 수행된다.

IV. 검증 및 성능평가

Verilog HDL을 이용하여 설계된 LEA 크립토 프로세서의 기능검증 결과는 그림 3과 같다. 그림 3(a)는 표준문서[3]에 제시된 256 비트의 마스터키 “0f1e2d3c 4b5a6978 . . .” 와 512 비트(4블록)의 평문 데이터 “d76d0d18 327ec562 . . .” 을 암호화한 시뮬레이션 결과를 보이고 있다. 암호화 결과로 512 비트의 암호문 “e25c46a4 b39220ff . . .” 가 출력되어 표준문서의 참조 구현 값과 일치하는 것을 확인하였다. 암호문을 다시 복호화 한 결과는 그림 3(b)와 같으며, 평문 “d76d0d18 327ec562 . . .” 이 출력되어 설계된 LEA 프로세서의 논리기능이 올바로 동작함을 확인하였다. 기능검증이 완료된 LEA 크립토 프로세서는 FPGA 구현을 통해 하드웨어 동작을 검증하였다. FPGA 보드, UART 인터페이스, 구동 소프트웨어로 구성된 검증 시스템을 이용하였으며, Xilinx Vertex5 XC5VSX-95T FPGA 디바이스가 사용되었다. 그림 4는 데모 프로그램을 이용한 FPGA 검증 결과이

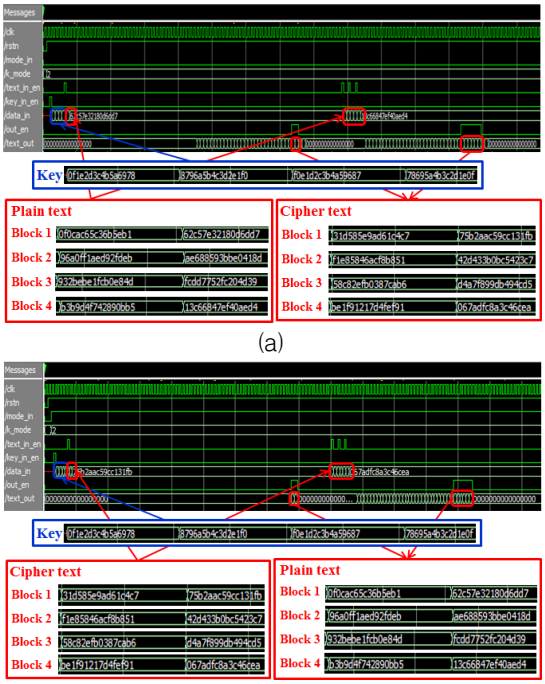

Figure 3. Functional verification results of LEA crypto-processor (a) encryption, (b) decryption

며, 평문을 암호화 하고, 이를 다시 복호화하면 원래의 평문이 출력되어 정상적으로 동작함을 확인하였다.

설계된 LEA 크립토 프로세서는 Xilinx ISE를 이용하여 합성한 결과, 최대 동작주파수 122MHz로 동작하여 7.8Gbps의 성능을 갖는 것으로 평가되었다.

V. 결 론

본 논문에서는 한국정보통신기술협회 표준으로 등록된 128 비트 블록암호 알고리듬 LEA를 파이프라인 구조를 적용하여 하드웨어로 구현하였다. 설계된 LEA 크립토 프로세서는 최대 122MHz 클록으로 동작 가능하며, 7.8Mbps의 성능을 갖는 것으로 평가되어 IoT 서버, 클라우드 서버 등 대량의 데이터를 고속으로 처리해야하는 응용분야의 정보보안에 사용이 가능할 것으로 예상된다.

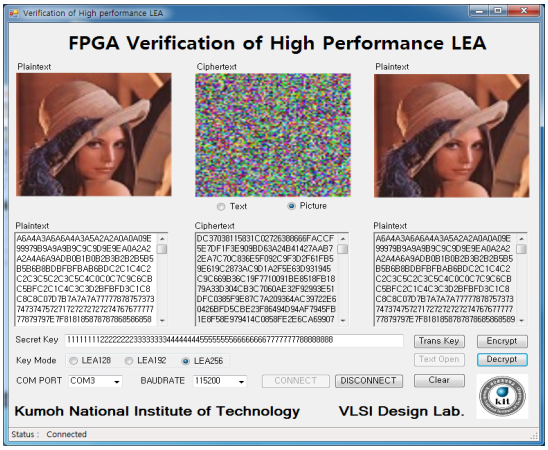

Figure 4. FPGA verification result of LEA crypto-processor

감사의 글

· 금오공과대학교 학술연구비 지원에 의한 연구결과임.
· 반도체설계교육센터(IDEC)의 CAD Tool 지원에 감사드립니다.

참고문헌

[1] Deukjo Hong et al, “LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors”, WISA, 2013.

[2] 한국정보통신기술협회, “128비트 블록암호 LEA”, TTA Standard, TTAK.KO-12.0223, 12월 2013년.

[3] 한국정보통신기술협회, ““128비트 블록암호 LEA 운영모드“, TTA Standard, TTAK.KO-12.0246, 2014년.