블록암호 CLEFIA-128의 효율적인 하드웨어 구현

배기철* · 신경욱*

*금오공과대학교

An Efficient Hardware Implementation of Block Cipher CLEFIA-128

Gi-Chur Bae* · Kyung-Wook Shin*

*Kumoh National Institute of Technology

E-mail : bae921216@kumoh.ac.kr

요 약

128-비트 마스터키를 지원하는 블록암호 CLEFIA-128의 저면적 하드웨어 구현에 대해 기술한다. 라운드 키 생성을 위한 중간값 계산과 라운드 변환이 단일 데이터 프로세싱 블록으로 처리되도록 설계하였으며, 변형된 GFN(Generalized Feistel Network) 구조와 키 스케줄링 방법을 적용하여 데이터 프로세싱 블록과 키 스케줄링 블록의 회로를 단순화시켰다. Verilog HDL로 설계된 CLEFIA-128 프로세서를 FPGA로 구현하여 정상 동작함을 확인하였다. Vertex5 XC5VSX50T FPGA에서 823 slices로 구현되었으며, 최대 145 Mhz 클록으로 동작하여 105 Mbps의 성능을 갖는 것으로 예측되었다.

ABSTRACT

This paper describes a small-area hardware implementation of the block cipher algorithm CLEFIA-128 which supports for 128-bit master key. A compact structure using single data processing block is adopted, which shares hardware resources for round transformation and the generation of intermediate values for round key scheduling. In addition, data processing and key scheduling blocks are simplified by utilizing a modified GFN(generalized Feistel network) and key scheduling scheme. The CLEFIA-128 crypto-processor is verified by FPGA implementation. It consumes 823 slices of Virtex5 XC5VSX50T device and the estimated throughput is about 105 Mbps with 145 MHz clock frequency.

키워드

CLEFIA, Cryptography, Block cipher, Security, Internet of Things

Ⅰ. 서 론

유·무선 통신 시스템의 보편화에 따라 통신망을 통한 정보의 유통이 급격하게 증가하고 있으며, 이에 따라 통신망을 통해 유통되는 정보가 제삼자에게 유출되거나 위·변조 되지 못하도록 하는 정보보안의 중요성이 날로 높아지고 있다. 특히, 무선 환경에서는 기지국 영역 내에 있는 모든 단말기들이 다른 사람의 정보를 수신할 수 있으므로, 허가된 수신자 이외에 제 3자가 정보를 알지 못하게 하는 데이터 기밀성과 사용자인증 등 정보보안 기술이 필수적으로 요구된다.[1]

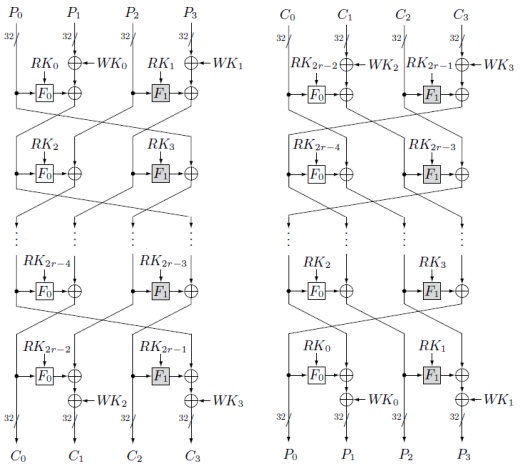
정보보안 기술의 다양한 응용분야들 중 DRM (Digital Rights Management) 보안기술은 모바일 단말기를 이용한 디지털 콘텐츠 이용이 보편화됨에 따라 중요성이 부각되고 있다. DRM은 디지털 콘텐츠를 패키지 형태의 암호화된 데이터로 변환하여 유통하고, 인증절차를 걸쳐 허가된 수신자만 암호화된 데이터의 해석이 가능하도록 하는 보안기술의 한 형태이다.[2] CLEFIA는 DRM 시스템을 위해 소니에 의해 개발된 블록암호 알고리듬이며[3], 경량 구현이 가능하고 128/192/256-비트 마스터키를 사용하여 AES(Advanced Encryption Standard)와 호환이 가능하다는 장점을 갖는다. CLEFIA는 선형공격, 불능 차분공격 등의 보안공격에 대한 안전성이 입증되었고, 경량 구현이 가능하여 RFID, IoT(Internet of Things)의 보안에 적합한 것으로 평가되고 있다.

본 논문에서는 IoT 환경에 적합하도록 최적화된 CLEFIA 암호 코어를 설계하였으며, FPGA 구현을 통해 하드웨어 동작을 검증하였다. 저면적 구현을 위해 암호화 및 복호화, 라운드 키 생성을 위한 데이터 프로세싱 블록의 하드웨어 자원을 최대한 공유하도록 최적화 하였다.

II. CLEFIA 블록암호 알고리듬[3]

CLEFIA는 128-비트 평문(암호문)을 암호화(복호화)하여 128-비트 암호문(평문)을 생성하는 대칭키 방식의 블록암호 알고리듬이다. CLEFIA는 그림 1과 같은 4-branch GFN(Generalized Feistel network)을 기반으로 하며, 마스터키 길이(128/192/256-비트)에 따라 18/22/26 라운드의 변환을 통해 암호화(복호화)가 이루어진다. CLEFIA의 암호화와 복호화 과정은 역순으로 이루어지며, 라운드 키 가산 순서와 순환이동 방향이 반대로 이루어진다. GFN은 2개의 F-함수(F_0, F_1), XOR 연산 그리고 32 비트 단위의 순환이동으로 구성되며, 32-비트 단위로 데이터를 처리한다. GFN은 라운드 변환과 라운드 키 생성에 공통적으로 사용된다. 마스터키를 GFN으로 변환하여 생성된 중간키 L과 마스터키 K에 상수값을 연산하여 라운드키 RK_r가 생성된다.

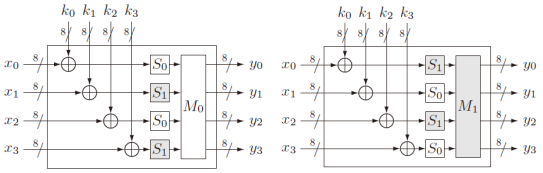
F-함수 F_0, F_1은 각각 그림 2-(a),(b)와 같이 구성되며, 라운드 키 가산, 4개의 비선형 S-Box, 확산 매트릭스 M_0, M_1의 곱셈으로 구성된다. F_0와 F_1에는 두 종류의 S-Box S_0, S_1이 서로 다른 순서로 적용되며, S-Box 출력과 M_0, M_1의 곱셈은 기약다항식 $p(z) = z^8 + z^4 + z^3 + z^2 + 1$으로 정의되는 유한체 $GF(2^8)$에서 연산된다.



(a) encryption (b) decryption

그림 1. CLEFIA의 4-branch GFN

Fig. 1. 4-branch GFN of CLEFIA



(a) F_0 (b) F_1

그림 2. F-함수 F_0, F_1

Fig. 2. F-function F_0, F_1

III. CLEFIA-128 코어 설계

본 논문에서는 128-비트의 마스터키를 지원하는 CLEFIA-128 암호/복호 프로세서를 설계하였다. CLEFIA-128 코어는 그림 3과 같이 데이터 프로세싱 블록과 키 스케줄링 블록으로 구성되며, 128-비트의 라운드 키를 받아 18번의 라운드 변환을 통해 암호화/복호화를 수행한다. 4개의 32-비트 레지스터 R_i (단, $0 \le i \le 3$)는 입력되는 평문(암호문)과 라운드 변환 중간값을 저장한다. 키 스케줄링 블록은 4개의 32-비트 레지스터 L_i (단, $0 \le i \le 3$)와 Double Swap 회로 그리고 상수값 생성회로로 구성된다. L_i 레지스터는 라운드 키 생성을 위한 중간값 L을 저장한다.

중간값 L의 생성과 라운드 변환 연산은 각각 독립적인 데이터 프로세싱 블록을 통해 이루어진다. 본 논문에서는 하드웨어 복잡도를 최소화하기 위해 하나의 데이터 프로세싱 블록을 사용하여 중간값 L의 생성과 라운드 변환이 처리되도록 하였다. 또한, 하나의 F-함수 회로를 이용하여 F_0 함수와 F_1 함수가 선택적으로 연산되도록 설계하여 경량 하드웨어 구현을 실현했다.

F-함수 회로는 바이트 단위의 치환(Sub-byte)을 수행하는 S-BOX 블록, 확산 매트릭스 곱셈을 연산하는 Matrix MULT 블록으로 구성된다.

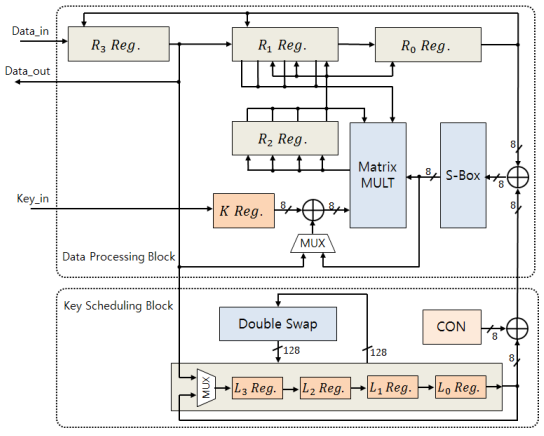


그림 3. CLEFIA-128 암호 코어

Fig. 3. CLEFIA-128 crypto core

그림 1에서 볼 수 있듯이, CLEFIA의 암호화와 복호화의 라운드 변환은 데이터 순환이동이 반대 방향으로 이루어진다. 본 논문에서는 암호화와 복호화의 데이터 순환이동이 동일한 방향으로 이루어지고, 라운드 키 RK_i^*의 생성을 마스터키 K와 분리시킨 MGFN(Modified GFN) 구조[4]를 적용하여 설계하였으며, 이를 통해 데이터 프로세싱 블록과 키 스케줄링 블록의 회로를 단순화시켰다.

Ⅳ. 기능검증 및 FPGA 검증

Verilog HDL로 설계된 CLEFIA-128 코어의 기능검증 결과는 그림 4과 같으며, 128-비트의 평문 “00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F”와 128-비트의 마스터키 “FF EE DD CC BB AA 99 88 77 66 55 44 33 22 11 00”을 입력으로 사용하였다. 그림 4에서 암호화 결과로 128-비트의 암호문 “DE 2B F2 FD 9B 74 AA CD F1 29 85 55 45 94 94 FD”가 출력되고, 이를 다시 복호한 결과는 암호화 입력으로 사용된 평문 “00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F”이 출력됨을 확인함으로써 논리기능이 정상적으로 동작함을 확인하였다.

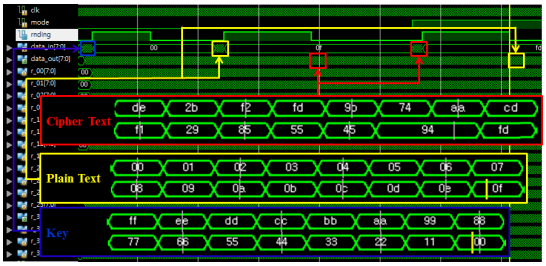


그림 4. CLEFIA-128 코어의 기능검증 결과
Fig. 4. Simulation result of CLEFIA-128 core

시뮬레이션이 완료된 CLEFIA-128코어는 FPGA 구현을 통해 하드웨어 동작을 검증하였다. 검증 시스템은 FPGA 보드, PC, UART 인터페이스 등으로 구성되며, FPGA 디바이스는 Xilinx Virtex5 XC5VSX50T가 사용되었다. 그림 5는 FPGA 검증 결과 화면이며, 평문을 암호화한 후 이를 다시 복호화하여 원래의 평문이 출력되어 CLEFIA-128 코어가 정상적으로 동작함을 확인하였다.

표 1. 설계된 CLEFIA-128 코어의 특성
Table 1. Summary of CLEFIA-128 core

Device	Virtex5 XC5VSX-50T
Maximum clock frequency	145 MHz
Throughput	105 Mbps
Slices	823

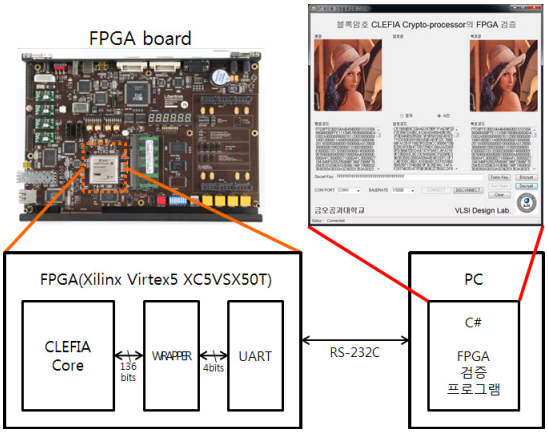


그림 5. CLEFIA-128 코어의 FPGA 검증 결과
Fig. 5. FPGA verification result of CLEFIA-128 core

검증이 완료된 Verilog HDL 모델은 Xilinx ISE에서 합성 결과 Xilinx Vertex5 XC5VSX50T 칩에서 최대 145 MHz 클록으로 동작 가능하며, 표 1과 같은 성능을 가지는 것으로 평가되었다.

Ⅴ. 결 론

ISO/IEC 국제표준으로 승인된 128-비트 블록 암호 알고리듬 CLEFIA를 하드웨어로 구현하여 동작을 확인하였다. 암호화/복호화 라운드 연산과 라운드 키 생성을 위한 하드웨어 자원의 공유를 극대화하여 저면적 구현을 실현했다. 설계된 CLEFIA-128 코어는 Virtex5 XC5VSX50T FPGA 디바이스에서 823 slices의 초경량으로 구현되었으며, 스마트폰, IoT, RFID 환경 등과 같이 경량화가 요구되는 응용분야의 정보보호 코어로 활용이 가능하다.

감사의 글

※ 반도체설계교육센터(IDEC)의 CAD Tool 지원에 감사드립니다.

참고문헌

[1] W. Stalling, *Cryptography and Network Security*, Prentice Hall, 1999.
[2] 한국교육학술정보원, *교육 · 학술 컨텐츠 보호를 위한 DRM 구축 방안 수립*, 2003.
[3] Sony Corporation, *The 128-bit Blockcipher CLEFIA : Algorithm Specification*, 2007.
[4] Sony Corporation, *Very Compact Hardware Implementations of the Blockcipher CLEFIA*, 2011.