파이프라인 구조 기반의 고속 ARIA 암호 프로세서의 하드웨어 구현

*하준수, *최현준, **서영호,*김동욱
*광운대학교 전자재료공학과
**한성대학교 정보통신공학과
e-mail : *truemind@kw.ac.kr, dwkim@kw.ac.kr*

Hardware Implementation of fast ARIA cipher processor based on pipeline structure

*Joon-Soo Ha, *Hyun-Jun Choi, **Young-Ho Seo, *Dong-Wook Kim
*Department of Electronic Materials Engineering
Kwangwoon University
** Department of Information and Communication Engineering
Hansung University

Abstract

This paper presented a hardware implementation of ARIA, which is Korean standard block ciphering algorithm. In this work, we proposed a improved architecture based on pipeline structure and confirmed that the design operates in a clock frequency of 101.7MHz and in throughput of 957Mbps in Xilinx FPGA XCV-1600E.

I. 서론

오늘날 멀터미디어 컨텐츠의 질이 급격하게 향상하고, 여러 가지 통신 매체를 통해서 전송하는 스트림 서비스가 발달함에 따라서 저작권 보호를 위해 대용량의 컨텐츠를 실시저작권을 보호할 수 있는 고속의 암호 프로세서의 필요성이 대두되고 있다. 본 논문에서는 기존의 ARIA 프로세서에 비하여 성능을 향상시키기 위해서 라운드 함수 블록 내부에 4단 파이프라인 구조를 제안하였고, 이를 Verilog-HDL을 이용하여 Xilinx FPGA상에서 구현하였다.

II. 본론

ARIA 알고리즘의 라운드 함수의 기본 구조는 ISPN(Involution SPN) 구조이고 키 확장의 초기화 과정에서는 Feistel 구조를 이용한다. 입/출력 크기는 128-비트이고, 키 크기는 128, 192, 256-비트의 세 가지 모드를 지원하며, 라운드 키 크기는 128-비트이고, 라운드 수는 키 크기에 따라 12, 14, 16 라운드인 구조를 갖는다. 라운드 함수는 128-비트 라운드 키를 라운드 입력 128-비트와 비트별 XOR하는 라운드 키 덧셈, 두 유형의 치환 계층이 있으며 각각은 2종의 8비트 입/출력 S-box와 그들의 역변환으로 구성된 치환 계층, 간단한 16 × 16 involution 이진 행렬을 사용한 바이트 간의 확산 함수로 구성된 확산 계층의 세부분으로 구성되어 있다. ARIA의 키 확장은 초기화 과정과 라운드 키 생성 과정 두 가지로 나뉜다. 초기화 과정에서는 Feistel 암호를 이용하여, 암호키 MK로부터 네 개의 128-비트 값 W_0, W_1, W_2, W_3를 생성하고, 라운드 키 생성 과정에서는 W_0, W_1, W_2, W_3를 조합하여 암호화 라운드 키 ek_i와 복호화 라운드 키 dk_i를 생성한다. 복호화 라운드 키는 암호화 라운드 키로부터 유도되며 키의 순서가 바뀌고, 처음과 마지막 라운드 키를 제외하고 암호화 라운드 키를 입력으로 하는 확산 함수 A의 출력이 복호화 라운드 키가 된다.

III. 구현

본 논문에서는 한 라운드 함수 블록만을 하드웨어로

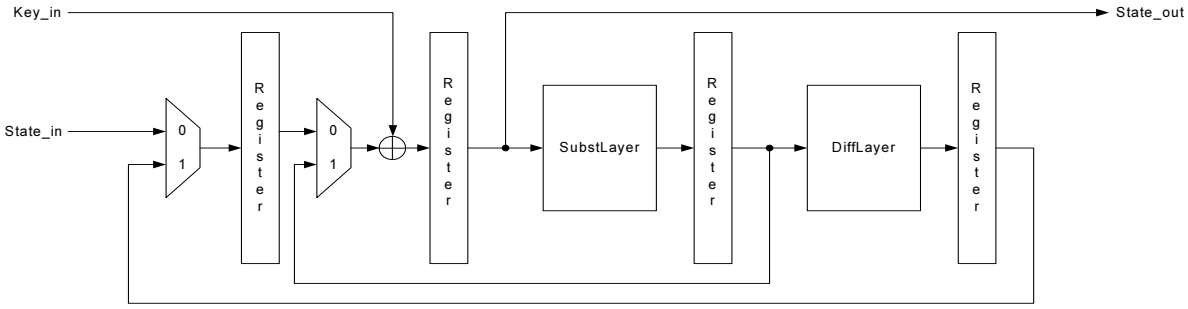

그림 1. 라운드 함수 블록의 4단 파이프라인 구조

구현하고, 라운드 함수 블록 내부에 4개의 파이프라인 레지스터를 삽입하여, 동작 속도와 성능을 향상시킨 4단계 파이프라인 구조를 제안하였다. 블록 암호 알고리즘은 라운드 연산의 특성상 한 블록의 연산이 모두 끝나기 전에는 다른 블록의 연산을 수행할 수가 없기 때문에, 한 번에 파이프라인 단계 수만큼의 블록씩 파이프라인 연산을 수행하도록 설계하였다.

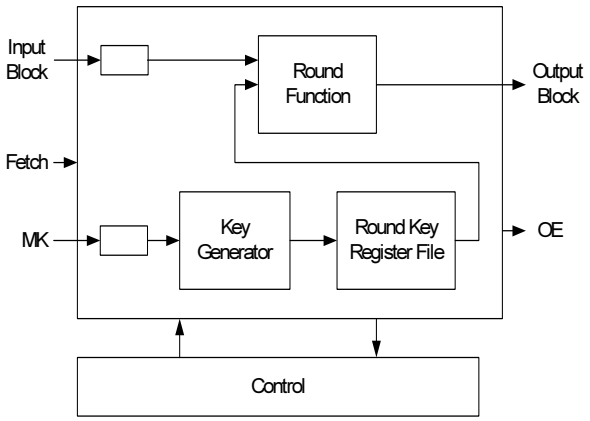

그림 2. 전체 구조

그림 1은 개선된 라운드 함수 블록의 파이프라인 구조를 보여주고 있고, 그림 2는 본 논문에서 구현한 하드웨어의 전체 구조를 보여주고 있다. 제안된 구조의 성능 평가를 위하여 Xilinx FPGA XCV1600E를 타겟으로 합성을 하여 성능을 평가하였고, 기존의 ARIA 프로세서와 비교하여 이를 표 1에 정리하였다.

표 1. 성능 평가표

	Opera-tion	Device	Frequency	Throughput
Previous ARIA-1	En/De	XCV-1600E	46.5MHz	496Mbps
Previous ARIA-2	En/De	XCV-1600E	47.5MHz	405Mbps
Our ARIA	En/De	XCV-1600E	101.7MHz	957Mbps

Ⅳ. 결론

본 논문에서는 기존의 대한민국 표준 128비트 블록 암호 알고리즘 ARIA 프로세서를 고속의 데이터 처리를 위해서 라운드 함수 모듈을 파이프라인 기반의 구조로 개선함으로써 기존에 구현된 프로세서보다 성능을 2배 이상 향상시켰다. 본 논문에서 구현한 ARIA 프로세서는 대용량의 멀티미디어의 보안이나 네트워크 보안를 위해서 사용되어질 수 있을 것으로 기대된다.

참고문헌

[1] 민관겸용 블록 암호 알고리즘 ARIA의 알고리즘 명세서, 국가보안기술연구소, 2004.

[2] 박진섭, 윤연상, 김용대, 양상운, 장태주, 유영갑, “ARIA 암호 알고리듬의 하드웨어 설계 및 구현”, 전자공학회 논문지, 제 42권 SD 제 4호, pp. 253~260, 2005년 4월

[3] Xinmiao Zhang and Keshab K. Parhi, “High speed VLSI Architectures for the AES Algorithm”, IEEE Trans. on VLSI Systems, vol.12, no. 9, pp. 957~967, Sept. 2004

[4] 김종현, 서영호, 김동욱, “블록 암호알고리즘 SEED의 면적 효율성을 고려한 FPGA구현”, 정보과학회 논문지, 제7권 제4호, pp.372~381, 2001년 8월

[4] W. Stallling, Cryptography and Network Security, Pearson Education, 2003

Ⅴ. Acknowledgement

본 연구 보고서는 정보통신부의 출연금으로 수행한 IT SoC 핵심 설계 인력 양성 사업의 수행결과입니다.