ISSN:1226-7244 (Print)
ISSN:2288-243X (Online)
논문번호 18-01-16
104
j.inst.Korean.electr.electron.eng.Vol.22,No.1,104~109,March 2018
http://dx.doi.org/10.7471/ikeee.2018.22.1.104

High Throughput을 위한 블록 암호 알고리즘 ARIA의 하드웨어 설계 및 구현

Hardware Design and Implementation of Block Encryption Algorithm ARIA for High Throughput

유 흥 렬*, 이 선 종*, 손 영 득*★

Heung-Ryol Yoo*, Sun-Jong Lee*, Yung-Deug Son*★

Abstract

This paper presents a hardware design for the block encryption algorithm of ARIA which is used for standard in Korea. It presents a hardware-efficient design to increase the throughput for the ARIA algorithm using a high-speed pipeline architecture. We have used ROM for the S-box implementation. This approach aims to decrease the critical path delay of the encryption. In this paper, hardware was designed by VHDL, realized RTL level by Synplify which is synthesis tool and verified simulation by ModelSim. The ARIA algorithm is shown 68.3 MHz (Maximum operation frequency) to use Xilinx VertxE XCV Series device.

요 약

본 논문에서는 국내 표준으로 제정된 ARIA 알고리즘을 High Throughput을 위한 하드웨어 구조를 제안하고 구현하였다. 치환 계층의 고속 처리를 위하여 ROM table 구성과 라운드 내부의 파이프라인 방식을 이용하며, 12 라운드를 확장된 구조로 설계하여 병렬 특성을 활용 가능한 설계 방법을 제안한다. 본 논문은 VHDL을 이용하여 RTL 레벨로 설계 되었으며, 합성 툴인 Synplify를 이용하였으며, 시뮬레이션을 위해 ModelSim을 이용하였다. 본 논문에서 제시한 하드웨어 구조는 Xilinx VertxeE Series 디바이스를 이용하였으며 68.3 MHz의 주파수 및 674Mbps의 Throughput을 나타낸다.

Key words : ARIA, Block Encryption Algorithm, Hardware, Pipeline, VHDL

* Dept. of Mechanical Facility Control Engineering, Korea University of Technology and Education

★ Corresponding author

E-mail: ydson@koreatech.ac.kr, Tel: +82-41-560-1297

Manuscript received Mar. 9, 2018; revised Mar. 26, 2018 ; accepted Mar. 28, 2018

Ⅰ. 서론

대칭키 암호 방식은 변환하는 방법에 따라 블록 암호 알고리즘과 스트림 암호 알고리즘으로 구분되며, 많은 정보기술과 상호 운용이 쉽고 데이터 처리량도 강력한 장점을 갖는다. 블록 암호 알고리즘은 고정된 크기의 입력 블록을 고정된 크기의 출력 블록으로 변형하는 암호 알고리즘으로 출력 블록의 각 비트는 입력 블록과 키의 모든 비트의

영향을 받아 결정된다. 현대 블록 암호 알고리즘은 대부분 Shannon의 이론에 근거하여Confusion과 Diffusion의 반복에 의하여 강력한 암호 알고리즘으로 설계 되었다. 대칭키 알고리즘의 내부 구조가 간단한 치환과 순열의 조합으로 되어 있어서 시스템 환경에 맞는 적절한 암호 알고리즘을 쉽게 개발 할 수 있다. 대표적인 대칭키 암호 알고리즘으로 DES, IDEA, AES, SEED 그리고 ARIA 알고리즘을 사용하고 있다. ARIA 알고리즘은 현재 국가 표준 암호 알고리즘인 SEED와 함께 국가 암호 알고리즘으로 사용 될 차세대 암호 알고리즘으로 개발 되었다. ARIA는 미국 ·유럽 등의 새로운 표준 제정 시 고려된 안전성 및 효율성 기준에 부합되도록 설계되었다[1]-[4].

본 논문에서는 파이프라인 구조의 내부 라운드 함수, S-BOX의 Lookup table 구현 그리고 전체 라운드의 확장된 구조로 클럭 속도의 향상과 병렬 처리가 가능하게 구현하였다.

Ⅱ. 본론

1. ARIA 알고리즘[3]

그림 1, 그림 2와 같이 ARIA 알고리즘은 암호화와 복호화를 수행하는 라운드 함수와 키 확장으로 구성되어 있다. ARIA 라운드 함수의 기본 구조는 Involution SPN 구조이다. 입, 출력의 크기는 128비트이며, 키의 크기는 128, 192 그리고 256비트 가변 크기를 암호 강도에 의해 선택 할 수 있다. 키의 크기에 따라 12, 14 그리고 16 라운드 함수를 반복 수행한다. 그림 1은 라운드 키 덧셈, 치환 계층 그리고 확산 계층의 세 부분으로 구성되는 라운드 함수를 나타내고 있다. 라운드 키 덧셈은 128비트 라운드키를 라운드 입력 128비트와 비트별 XOR한다. 치환계층은 두 유형으로 구성되며, 32비트 단위로 4종의 S1, S2 그리고 역치환으로 구성된 S-BOX를 사용한다. 확산계층은 16×16 이진행렬을 사용한 입력 16바이트에 대하여 바이트 단위의 행렬 곱을 수행한 결과를 16바이트 출력하는 구조를 가지고 있다. 키 확장은 초기화 과정과 라운드 키 생성과정의 두 부분으로 나뉜다. 초기화 과정에서는 3 라운드 256비트 Feistel 알고리즘을 이용하여 마스터키로부터 W0, W1, W2, W3을 생성하며 네 개의 W값을 조합하여 라운드 키를 생성한다. 그림 2는 ARIA 알고리즘의 전체 암호화와 복호화 과정을 나타낸다.

2. 2 제안하는 하드웨어 구조

라운드함수의 내부는 라운드 키 덧셈, 치환 계층 그리고 확산계층으로 구성 되어 있다. 따라서 클럭 속도를 높이기 위하여 각 계층 사이에 레지스터를 삽입하여 파이프라인 구조를 가진다.

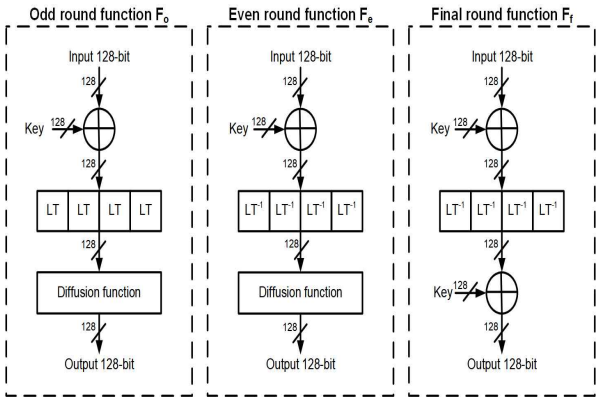

Fig. 1. Round function.
그림 1. 라운드 함수

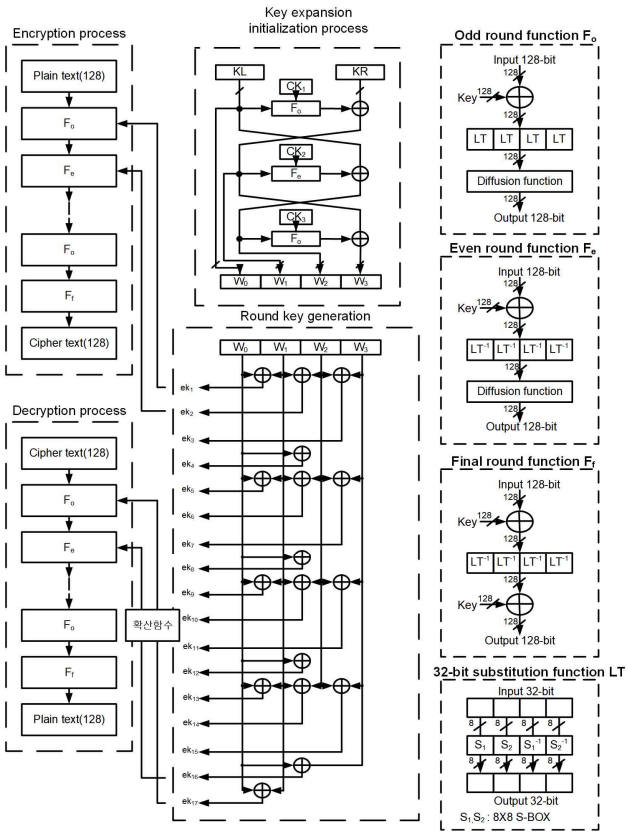

Fig. 2. Encryption and Decryption process
그림 2. ARIA의 암호화와 복호화 과정

S-BOX는 미리 계산 가능하기 때문에 ROM TABLE을 사용하여 입력 데이터가 어드레스가 되어 해당 어드레스의 데이터를 출력하게 된다. 또한 두 종류의 확산계층을 MUX를 통하여 공용으로 사용하게 하였다. 그림 3은 제안하는 라운드 내부의 파이프라인 구조를 나타내며 본 논문에서 구현하는 각 라운드 내부는 라운드 키 덧셈 후에 하나, 치환계층 다음에 하나 그리고 최종 데이터 출력 전에 레지스터를 구성하여 3단 파이프라인으로 구성하고 있다. 암·복호화 알고리즘을 수행하는 라운드 함수는 하나의 라운드 함수를 반복하지 않고 전체 라운드가 펼쳐진 구조로 각각의 라운드에서 생성된 데이터는 다음 라운드의 입력으로 사용된다. 그림 4는 제안하는 S-BOX의 구조를 나타낸다. S-box의 구현에 대한 연구에는 S-box의 값을 계산하는 On-the-fly 방식과 ROM에 S-box의 값을 저장하는 두 가지 접근 방법이 있다. 첫 번째 방법인 On-the-fly 방식은 하드웨어의 복잡도를 줄이는데 목적이 있다. 그러나 이러한 접근은 암·복호화 시 임계 경로(Critical Path) 지연 시간을 증가시킨다. ROM에 S-box의 값을 저장하는 접근은 암·복호화 시 임계 경로 지연을 감소시키는데 목적이 있다. ARIA의 규격에 S-box의 값은 상수이다. 암·복호화 프로세스 동안에 S-box의 값은 변화하지 않는다. 그러므로 On-the-fly 방식으로 값을 계산하는 대신에 저장할 수 있다.

본 논문에서는 설계의 용이성과 고속 처리를 위하여 미리 계산 가능한 치환 함수 S-box를 Look up table을 이용하였다. 입력 데이터가 어드레스가 되어 해당 어드레스의 데이터를 출력하게 된다. 또한, ROM 구현에 따른 설계 면적의 최소화를 위하여 LT 함수와 LT^{-1}함수를 공유하는 수정된 LT 함수를 사용한다. 수정된 LT 블록은 입력단과 출력단에 각각 Rotate를 사용하여 하나의 치환계층으로 구성하였다[6][7]. 마지막으로 반복되는 라운드를 확장된 구조를 이용하여 12개의 라운드가 배치되어 병렬처리가 가능하도록 설계하여 High Throughput을 가능하도록 하였다. 제어신호에 의해 키 초기화 과정을 거친 후 라운드 키 생성과 동시에 각 라운드 함수를 통해 각 라운드를 거쳐 암호문을 생성하는 과정으로 진행한다. 그림 5는 전체 ARIA 알고리즘의 블록도를 나타낸다. ARIA 알고리즘의 동작을 제어하는 제어부, 키 확장을 위한 키 초기화 부, 라운드 키 생성을 위한 라운드 키 생성부 그리고 암·복호의 라운드를 생성하는 라운드 모듈로 구성 되어 있다.

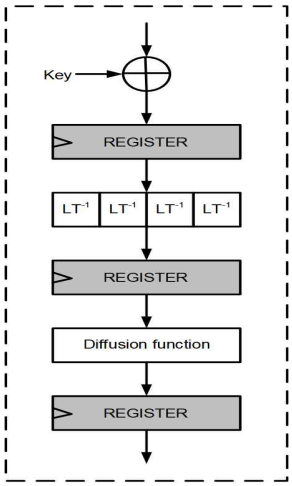

Fig. 3. Inner round pipelining
그림 3. 내부 라운드의 파이프라인

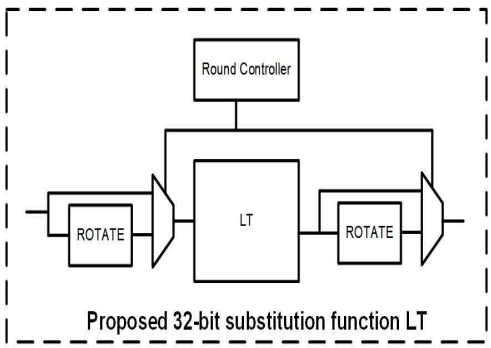

Fig. 4. Architecture of diffusion layer
그림 4. 확산 계층의 구조

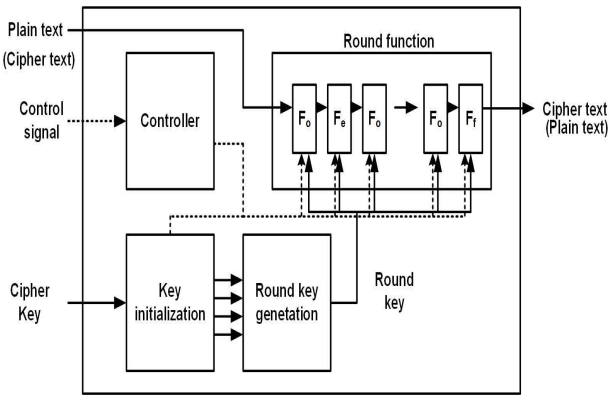

Fig. 5. Proposed overall block diagram
그림 5. 전체 블록도

2.3 Simulation 결과 및 성능 결과

ARIA 알고리즘은 VHDL을 이용하여 설계하였으며, 그림 6은 테스트 벡터를 이용하여 암호문이 생성과정을 나태내고 있다. 초기화 과정이 완료되면 초기화 종료 신호를 제어 블록에서 입력 신호로 받으면 라운드 키 생성 블록과 암·복호화를 수행하는 라운드 블록으로 시작 신호를 출력하여 암·복호화가 진행하게 된다[8]. 암호화 과정은 평문 “00112233445566778899aabbccdde eff”과 암호키 값“000102030405060708090a0b0c0d0 e0f”을 입력 받고 암호/복호 과정을 구분하는 enc 신호 ‘1’을 입력 받고 암호 과정 종료 신호와 함께 암호문 “d718fbd6ab644c739da95f3be6451778”을 출력한다. 그림 7은 암호화 과정의 시뮬레이션 파형을 나타낸다. 복호화 과정은 암호화 과정과 동일하며 암호화 라운드 키로 유도된 복호화 라운드 키를 사용하고 암호/복호 신호인 enc를 ‘0’으로 입력한다. 암호문 “d718fbd6ab644c739da95f3be64 51778”을 입력 받아 평문을 출력하는 시뮬레이션파형을 그림 8에서 확인 할 수 있다.

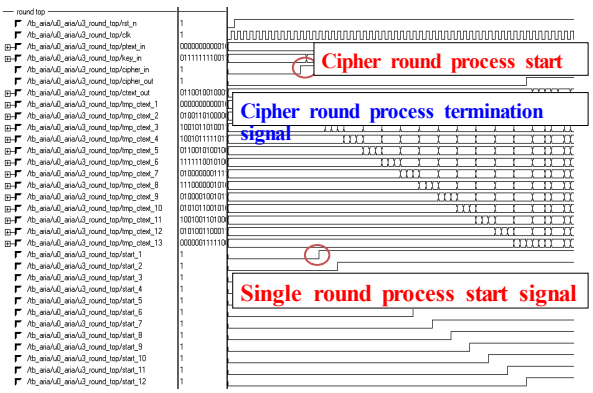

Fig. 6. Simulation result
그림 6. 시뮬레이션 결과

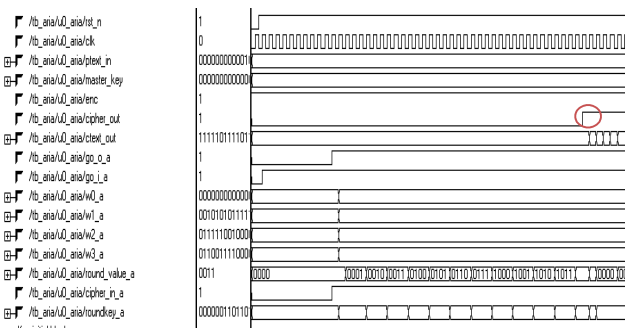

Fig. 7. Simulation of the encryption process
그림 7. 암호화 과정의 시뮬레이션

그림 8는 라운드 함수 내부 및 전체 라운드 함수의 심플리파이를 통하여 합성 결과를 보여 주고 있다. 라운드 함수의 파이프라인 된 하드웨어 합성 결과를 나타낸다. 합성 결과 라운드 키 덧셈, 치환 계층 그리고 확산 계층 출력단에 레지스터로 구성되어 3단 파이프라인 구조를 가지고 있다.

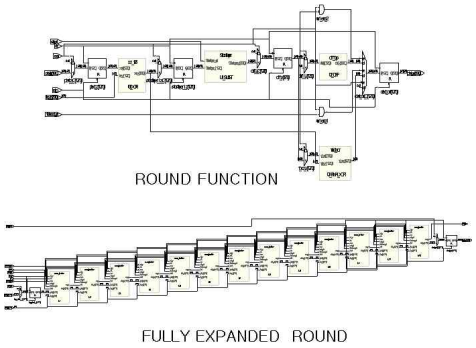

Fig. 8. Synthesis result
그림 8. 합성 결과

2.4 성능 분석

본 논문에서 구현한 ARIA 알고리즘의 분석을 위해 Xilinx사의 FPGA VertxeE XCV Series를 사용하였으며 표 1에서 성능 평가표를 통하여 기존방법과 비교 분석하였다. 기존의 1번째 방법은 S-box를 공유할 수 있는 구조와 적은 면적에 빠른 키 생성을 위한 구조로 ARIA 블록은 1 라운드 반복 구조로 구현하였다. 설계된 ARIA 블록은 1,491 slice와 128 BRAM을 사용하여 동작 주파수 30 MHz의 동작을 보인다. 기존의 2번째 방법은 S-box를 On-the-fly 방식을 이용하여 면적을 최소화 할 수 있는 방법으로 Smart Card에 적합하게 설계되었다. 설계된 ARIA 블록은 1,492 slice와 동작 주파수 46.5 MHz의 동작을 보인다. 기존 방법과 비교하여 라운드 내부의 파인프라인 구조와 전체 암·복호화 라운드를 확장된 구조를 사용하여 한 라운드 종료 시 다음 암·복호화를 진행할 수 있도록 설계하였다. 제안하는 방법의 ARIA 블록은 23,551 slice와 동작 주파수 68.3 MHz, 처리율 674Mbps의 동작을 보인다. slice의 크기는 전체 라운드의 확장된 구조로 인하여 증가하였지만 1라운드 반복하는 구조를 가지는 기존 논문에 비해 파이프라인 처리로 인하여 12라운드 이후에는 결과가 출력 되므로 연산 속도에서 차이를 나타낸다.

Table 1. Efficiency Analysis.
표 1. 성능분석

Method	Device	Slice	Frequency (MHz)
Conventional method Ⅰ	XCV Series	2,202	30.056
Conventional method Ⅱ	XCV Series	1,492	46.5
Proposed method	XCV Series	23,551	68.3

Ⅲ 결론

본 논문에서는 128비트의 블록 암호 알고리즘 ARIA의 하드웨어를 효율적 설계방법을 제안한다. 암호과정의 임계 경로 지연을 감소시키며 높은 쓰루풋의 성능을 유지하기 위하여 미리 계산 가능한 치환 계층은 메모리 기반의 look up table로 구현하였으며, 또한 클럭 속도 또는 샘플 속도를 증가시키거나 같은 속도에서 저 전력을 위하여 라운드 함수의 내부 파이프라인 및 128비트 암호키를 위한 12라운드를 위하여 라운드 함수 전체를 확장된 라운드 구조로써 설계 하였다. 본 논문은 최종 데이터 경로를 설계하기 전에 각 블록의 구현을 bottom-up 설계 방식을 이용하였다. 하드웨어 설계는 VHDL을 이용하였으며 합성툴인 Synplify를 통하여 RTL 레벨에서의 구현하였고 ModelSim 툴을 사용하여 시뮬레이션 검증을 하였다. ARIA 암호 알고리즘은 Xilinx VertxeE XCV Series를 디바이스를 사용하여 최대 동작 주파수 68.3 MHz, 674Mbps의 처리율로 동작하는 성능을 보인다. 암호 알고리즘인 AES, SEED등이 고속 처리를 위하여 파이프라인 처리로 높은 쓰루풋의 결과를 나타내고 있으며, ARIA 암호 알고리즘도 본 논문에서 제시한 하드웨어 구조를 통하여 충분한 성능 향상을 보이고 있다. 따라서 제시한 구조를 바탕으로 일대 다 통신에 적용하면 유용 할 것이며 향후 192/256 비트에 대해서도 연구가 필요하며, 병렬처리 기법을 적용하면 더 나은 성능을 낼 수 있을 것이라 기대한다.

References

[1] Martin P.J. and Kratz, *Information systems security*, Van Nostrand Reinhold, 1993

[2] Telecommunication Technology Associate, 128-bits Block Encryption Algorithm (SEED), Jun. 1999.

[3] http://www.nsri.re.kr/ARIA, National Security Research Institute ,ARIA Algorithm Specification

[4] H.R.Yoo, B.S.Chea, K.Y. Kim, Y.B.Cho, “Hardware Design and Implementation for SEED Cipher Processor of Dynamic Scheduling Architecture,” *IDEC(IC Design Education Center*, 2003.

[5] C.E.Shanon. *Communication Theory of Secrecy System. Bell System Technical Journal*, vol.30, pp.50-64, 1951.

[6] KESHAB K. PARHI, *VLSI Digital Signal Processing,* JOHN WILEY & SONS,INC, 1999.

[7] D.H. Youn, Modrn CRYTOGRAPHY, Green, 2004.

[8] Y.C. Kim, Y.M. Jung, J.H.Cho, Y.S. Hong Reunong, *VHDL for digital design* , Hg Science Publisher, 2001

[9] J.S. Park, Y.S Yun, Y.D Kim, “Design and Implementation of ARIA Cryptic Algorithm,” *The Institute of Electronics Engineers of Korea.*, vo. 42, no. 4, pp 29-36, 2005.

[10] K.B.Kim, K.W.Shin, "A Unified ARIA-AES Cryptographic Processor Supporting Four Modes of Operation and 128/256-bit Key Lengths," *Journal of the Korea Institute of Information and Comm.*, vol. 21, no. 4, pp 795-803, 2017. DOI:10.6109/jkiice.2017.21.4.795

BIOGRAPHY

Heung-RyolYoo(Member)

2002 : BS degree in Electrnics Egineering, SoonChengHang University.

2007: MS degree in Electrnics Egineering, Kunkuk University.

2016~ : MS degree in Mechanical Facility Control Engineering, Korea University of Technology and Education.

2004~2013 : Senior Research Engineer, SEMES. Co,.LTD

Sun-Jong Lee (Member)

2003 : BS degree in Electrical Engineering, Namseoul University.
2016~ : MS degree in Mechanical Facility Control Engineering, Korea University of Technology and Education

2001~Present : Senior Research Engineer, SunKyung E&I Co,.LTD

Yung-Deug Son (Member)

1997 : BS degree in Control and Instrumentation Engineering, Korea Maritime University.
2001 : MS degree in Ocean Electro-Mechanical Engineering, Kobe University.
2015 : PhD degree in Electrical Engineering, Pusan National University.
1998 : Research student, Tokyo Institute of Technology
2001~2009 : Senior Research Engineer, Hyundai Heavy Industries Co,.LTD
2016~Present : Assistant Professor, Korea University of Technology and Education.