4가지 운영모드를 지원하는 ARIA 암호/복호 코어의 FPGA 구현

김동현* · 신경욱**

국립금오공과대학교

FPGA Implementation of ARIA Encryption/Decrytion Core Supporting Four Modes of Operation

Dong-Hyeon Kim* · Kyung-Wook Shin**

School of Electronic Eng., Kumoh National Institute of Technology

E-mail : kdh137@kumoh.ac.kr

요 약

본 논문에서는 국내 표준(KS)으로 제정된 블록암호 알고리듬 ARIA의 하드웨어 구현을 제안한다. 제안된 ARIA 암·복호 코어는 표준에 제시된 세 가지 마스터 키 길이128/192/256-비트를 모두 지원하도록 설계되었으며, ECB, CBC, CTR, OFB와 같은 4개의 암호 운영모드를 지원한다. 회로의 크기를 줄이기 위해 키 확장 초기화 과정과 암복호 과정에 사용되는 라운드 함수가 공유되도록 설계를 최적화 하였다. 설계된 ARIA 암·복호 코어를 FPGA로 구현하여 하드웨어 동작을 검증하였으며, 1.07 Gbps@167 MHz의 성능을 갖는 것으로 평가되었다.

ABSTRACT

This paper describes an implementation of ARIA crypto algorithm which is a KS (Korea Standards) block cipher algorithm. The ARIA crypto-core supports three master key lengths of 128/192/256-bit specified in the standard and the four modes of operation including ECB, CBC, CTR and OFB. To reduce hardware complexity, a hardware sharing is employed, which shares round function in encryption/decryption module with key initialization module. The ARIA crypto-core is verified by FPGA implementation, the estimated throughput is about 1.07 Gbps at 167 MHz.

키워드

ARIA 알고리듬, 블록암호, 정보보안, 암호화, 암호 운영모드

Ⅰ. 서 론

암호기술은 과거에는 군사적인 용도 등의 비밀통신을 위해 주로 사용되었으나 현재는 인터넷 기반의 사회, 경제 활동의 안전성, 신뢰성, 프라이버시 보호 등을 위한 필수 기술로서 메일전송 사용자 인증, 전자상거래 등에 광범위하게 사용되고 있다. 암호기술은 특정분야에서 사용하는 특수기술에서 차세대 정보환경의 기반기술로 변화하고 있으며 중요성이 증대되고 있다[1].

국가보안기술연구소에서는 정보통신 서비스의 다변화 및 전자정부 구현 등으로 인한 국가기관과 민간(G2C)간 소통 자료에 안전성과 효율성을 제공하기 위한 정보보안 알고리듬으로 ARIA를 제안하였으며, 2004년 12월 국내 표준(KS)으로 제정되었다[2]. ARIA 블록암호 알고리듬은 미국 연방표준 알고리듬인 AES(Advanced Encryption Standard)[3]와 입·출력 크기 및 사용 가능한 키 길이가 동일하며, 속도와 안전성 측면에서 유사하여 동급 경쟁 기술로 평가를 받고 있다. ARIA 블록암호 알고리듬은 시스템의 요구에 맞는 다양한 구현 방법들이 연구되고 있다. 대용량 데이터의 고속처리에 초점을 맞춘 하드웨어 구현을 비롯해서 스마트카드나 RFID와 같은 휴대용 장치에 적합한 소면적, 저전력 위주의 하드웨어 구현 결과도 발표되고 있다[4,5]. 고속 처리에 초점을 맞춘 하드웨어 구조는 높은 throughput을 갖는 장점이 있지만, 회로의 면적이나 전력소모 측면에서 휴대용

기기에 적합하지 않다. 반면 소면적, 저전력 위주의 구조는 회로의 면적이나 전력소모 측면에서는 뛰어난 성능을 보이지만, 높은 throughput을 가지지는 못한다. ARIA 알고리듬의 하드웨어 구현을 위해서는 회로의 면적을 최소화하면서도 동시에 높은 throughput을 얻기 위한 다양한 설계 최적화가 요구된다.

본 논문에서는 ARIA 알고리듬의 키 초기화 모듈과 암·복호 모듈에서 사용하는 라운드 함수를 공유하여 설계 하였다. 설계된 ARIA 암·복호 코어는 ECB, CBC, OFB, CTR과 같은 4가지 암호 운영모드를 지원하도록 설계하였으며, 이를 FPGA로 구현하여 기능을 검증하였다.

Ⅱ. ARIA 블록암호 알고리듬

ARIA 알고리듬은 평문(암호문)을 128-비트의 블록 단위로 분할하여 암호(복호)화 하며, 128/192/256-비트의 마스터 키 길이에 따라12/14/16의 라운드 변환을 갖는 involution substitution-permutation network 구조의 블록암호 시스템이다. 전체적인 ARIA 알고리듬의 암호화 및 복호화 과정은 그림 1과 같다. 첫 라운드와 마지막 라운드를 제외한 나머지 라운드들은 모두 동일한 형태를 가지며, 홀수 라운드(F_o)와 짝수 라운드(F_e)에 각기 다른 치환계층이 사용된다. 마지막 라운드(F_f)에서는 확산계층을 라운드 키 덧셈으로 대체한다. 각 라운드 함수는 그림 2와 같이 라운드 키 가산, 치환계층, 그리고 확산계층의 세 부분으로 구성된다. 라운드 키 가산은 128-비트의 라운드 키를 라운드 입력 128-비트와 비트 단위로 XOR한다. 치환계층은 그림 3과 같이 두 가지 유형으로 구분되며, "유형1"은 홀수 라운드에 사용되고, "유형2"는 짝수 라운드에 사용된다. 각 유형은 8-비트 입·출력을 갖는 두 가지 S-box S_1, S_2와 그 역치환 S_1^{-1}, S_2^{-1}로 구성된다. 확산계층은 16×16 involution 이진 행렬을 이용한 바이트 단위의 확산함수로 구성되며, 확산함수는 입력 16-바이트에 대해 식(1)과 같이 바이트 단위의 행렬 곱셈을 수행하여 16-바이트의 결과를 출력으로 한다.

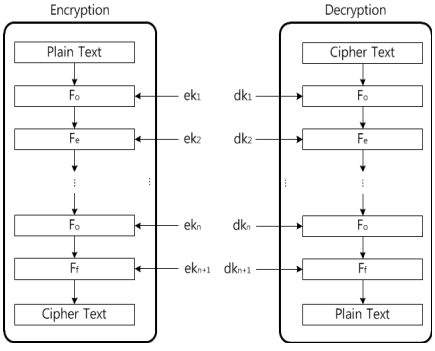


그림 1. ARIA 알고리듬의 암호화 및 복호화 과정

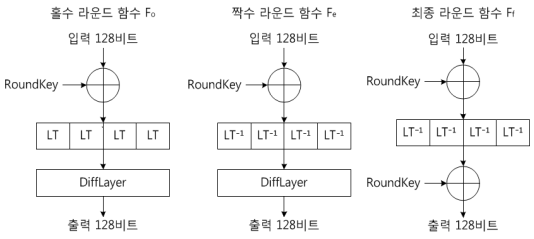
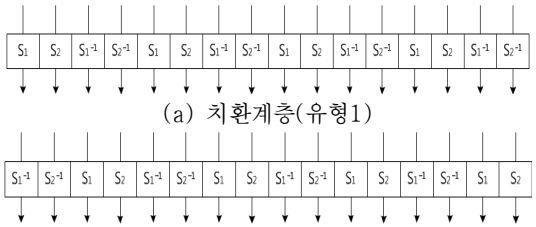


그림 2. ARIA 알고리듬의 라운드 함수



(a) 치환계층(유형1)

(b)치환계층(유형2)

그림 3. ARIA 알고리듬의 치환계층

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \\ y_9 \\ y_{10} \\ y_{11} \\ y_{12} \\ y_{13} \\ y_{14} \\ y_{15} \end{pmatrix} = \begin{pmatrix} 0&0&0&1&1&0&1&0&1&1&0&0&0&1&1&0 \\ 0&0&1&0&0&1&0&1&1&1&0&0&1&0&0&1 \\ 0&1&0&0&1&0&1&0&0&0&1&1&1&0&0&1 \\ 1&0&0&0&0&1&0&1&0&0&1&1&0&1&1&0 \\ 1&0&1&0&0&1&0&0&1&0&0&1&0&0&1&1 \\ 0&1&0&1&1&0&0&0&0&1&1&0&0&0&1&1 \\ 1&0&1&0&0&0&0&1&0&1&1&0&1&1&0&0 \\ 0&1&0&1&0&0&1&0&1&0&0&1&1&1&0&0 \\ 1&1&0&0&1&0&0&1&0&0&1&0&0&1&0&1 \\ 1&1&0&0&0&1&1&0&0&0&0&1&1&0&1&0 \\ 0&0&1&1&0&1&1&0&1&0&0&0&0&1&0&1 \\ 0&0&1&1&1&0&0&1&0&1&0&0&1&0&1&0 \\ 0&1&1&0&0&0&1&1&0&1&0&1&1&0&0&0 \\ 1&0&0&1&0&0&1&1&1&0&1&0&0&1&0&0 \\ 1&0&0&1&1&1&0&0&0&1&0&1&0&0&1&0 \\ 0&1&1&0&1&1&0&0&1&0&1&0&0&0&0&1 \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \\ x_{14} \\ x_{15} \end{pmatrix} \quad (1)$$

ARIA의 키 확장은 키 초기화 과정과 라운드 키 생성 과정으로 나뉜다. 초기화 과정에서는 그림 4와 같이 3라운드의 Feistel 구조를 이용하여 마스터 키 MK로부터 4개의 128-비트 초기화 키 값 W_k (단, $0 \le k \le 3$)를 생성한다.

마스터 키 MK는 128/192/256-비트이므로, 그림 4의 키 초기화 과정 입력에 필요한256-비트 (KL, KR)을 구성해야 한다. MK의 길이가 128-비트인 경우에는 KL에 마스터 키를 할당하고 KR은 0으로 채운다. MK의 길이가 192-비트인 경우에는 MK의 상위 128-비트를 KL에 할당하고, MK의 남은 64-비트를 KR의 상위 비트에 할당하고, 나머지는 0을 채운다. MK의 길이가 256-비트인 경우

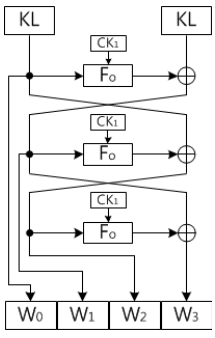


그림 4. ARIA 알고리듬의 키 초기화 과정

에는 KL과 KR에 각각 MK의 상위, 하위 128-비트씩 할당한다. 그림 4에서 128-비트의 초기화 상수 CK는 표준문서에 정의된 128-비트의 상수를 이용하여 키의 길이에 따라 결정된다.

라운드 키 생성 과정에서는 4개의 128-비트 초기화 키 값 W_k를 조합하여 암호화에 사용되는 라운드 키 ek_i와 복호화에 사용되는 라운드 키 dk_i를 생성한다. 라운드 변환은 마스터 키 길이에 따라 12/14/16로 구성되고 마지막 라운드에는 키 가산이 두 번 이루어지므로 각각 13/15/17개의 라운드 키가 생성되어야 한다. 암호화 라운드 키는 식(2)의 연산으로 생성된다.

$$
\begin{aligned}
ek_1 &= (W_0)\oplus(W_1^{\gg 19}), & ek_{10} &= (W_1)\oplus(W_2^{\ll 61}),\\
ek_2 &= (W_1)\oplus(W_2^{\gg 19}), & ek_{11} &= (W_2)\oplus(W_3^{\ll 61}),\\
ek_3 &= (W_2)\oplus(W_3^{\gg 19}), & ek_{12} &= (W_3)\oplus(W_0^{\ll 61}),\\
ek_4 &= (W_3)\oplus(W_0^{\gg 19}), & ek_{13} &= (W_0)\oplus(W_1^{\ll 31}),\\
ek_5 &= (W_0)\oplus(W_1^{\gg 31}), & ek_{14} &= (W_1)\oplus(W_2^{\ll 31}),\\
ek_6 &= (W_1)\oplus(W_2^{\gg 31}), & ek_{15} &= (W_2)\oplus(W_3^{\ll 31}),\\
ek_7 &= (W_2)\oplus(W_3^{\gg 31}), & ek_{16} &= (W_3)\oplus(W_0^{\ll 31}),\\
ek_8 &= (W_3)\oplus(W_0^{\gg 31}), & ek_{17} &= (W_0)\oplus(W_1^{\ll 19})\\
ek_9 &= (W_0)\oplus(W_1^{\ll 61}),
\end{aligned}
\qquad (2)
$$

복호화 라운드 키는 암호화 라운드 키의 역순이 되며, 식(3)과 같이 암호화 라운드 키 ek_i가 확산함수 A를 거쳐 복호화 라운드 키 dk_i로 생성된다. 단, 처음과 마지막 라운드 키는 확산계층을 거치지 않고 직접 사용된다. 식(3)에서 n은 마스터 키 길이에 따른 라운드 수(12/14/16)를 나타낸다.

$$
\begin{aligned}
&dk_1 = ek_{n+1},\ dk_2 = A(ek_n),\\
&dk_3 = A(ek_{n-1}),\ \cdots,\ dk_n = A(ek_2),\ dk_{n+1} = ek_1
\end{aligned}
\qquad (3)
$$

Ⅲ. ARIA 암·복호 코어 설계

본 논문에서는 ECB, CBC, OFB, CTR 4가지 암호 운영모드를 지원하며, 3가지 마스터 키 길이 128/192/256-비트를 지원하는 ARIA 암·복호 코어를 설계하였다.

4가지 암호 운영모드를 지원하는 ARIA 하드웨어 전체 구조는 그림 5와 같다. 2개의 XOR와 6개의 멀티플렉서에 의해 4가지의 모드가 선택적으로 동작한다. ECB 모드의 암·복호화는 평문을 입력으로 ARIA 코어에 인가하고 라운드 수만큼 암·복호화된 데이터를 출력한다. CBC 모드의 암호화는 첫 번째 암호화의 경우 평문과 IV(Initialization Vector)를 XOR 연산하여 ARIA 코어의 입력으로 인가하여 라운드 수만큼 암호화 된 데이터

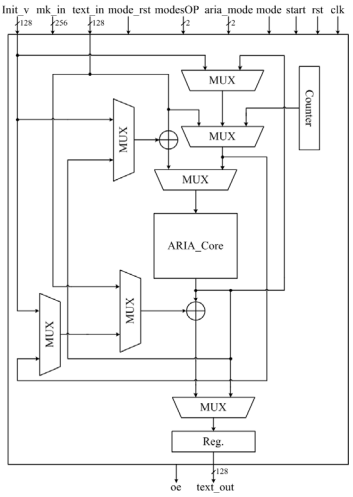


그림 5. 4가지 암호 운영모드를 지원하는 ARIA 하드웨어 전체 구조

를 출력한다. 첫 번째 이후의 암호화는 IV 대신 이전 ARIA 코어의 출력을 평문과 XOR하여 준다. CBC 모드의 복호화는 첫 번째 복호화의 경우 암호문을 입력으로 받아 ARIA 코어의 입력으로 인가하고 라운드 수만큼 복호화된 데이터를 IV와 XOR 연산하여 출력한다. 첫 번째 이후의 복호화는 IV 대신 이전 복호화에 사용하였던 암호문을 ARIA 코어의 출력과 XOR 연산한다. OFB 모드의 암·복호화는 첫 번째 암·복호화의 경우 IV를 ARIA 코어의 입력으로 인가하여 라운드 수만큼 암·복호된 데이터를 평문(암호문)과 XOR 연산하여 출력한다. 첫 번째 이후의 암·복호화는 IV 대신 이전 ARIA 코어의 출력을 현재 ARIA 코어의 입력으로 인가하여 준다. CTR 모드의 암·복호화는 암·복호가 진행될 때 마다 1씩 증가하는 카운터를 ARIA 코어의 입력으로 인가하고 라운드 수만큼 암·복호화된 데이터를 평문(암호문)과 XOR 연산하여 출력한다.

설계된 ARIA 암·복호 코어는 단일 라운드 구조를 가지며, 그림 6와 같이 키 스케줄러 모듈과 암·복호 모듈로 구성된다. 키 스케줄러 모듈은 키 초기화 모듈과 라운드 키 생성 모듈로 구성된다. 설계된 ARIA 암·복호 코어는 키 초기화 모듈에서 초기 5 클록 사이클을 소모하며, 암·복호 모듈에서는 마스터 키의 길이에 따라 각각 13/15/17 클록 사이클을 소모한다. 키 초기화 모듈의 라운드 함수는 초기 5 클록 사이클 이후 라운드 키가 생성되면서 암·복호 모듈에서 암·복호가 이루어지는 동안은 사용하지 않는다. 따라서 그림 6의 구조와 같이 멀티플렉서를 이용하여 초기 5 클록 사이클 동안은 라운드 함수에 키 초기화 모듈의 입력값을 넣어주고, 나머지 클록 사이클 동안은 암·복호 모듈의 입력값을 넣어준다.

모듈별 동작을 설명하면 다음과 같다. 암·복호 모듈은 단일 라운드 구조로서 MK의 길이에 따라 각각 12/14/16 라운드가 진행된다. 최종 라

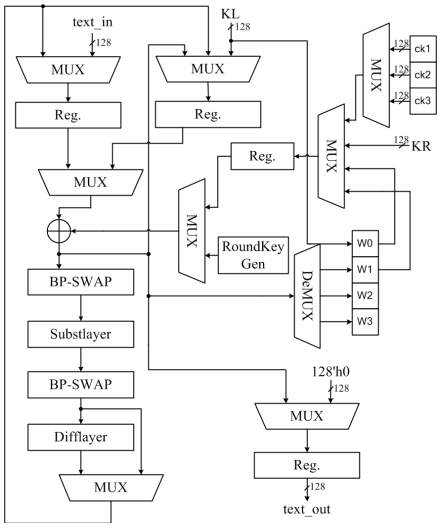


그림 6. ARIA 암·복호 코어의 구조

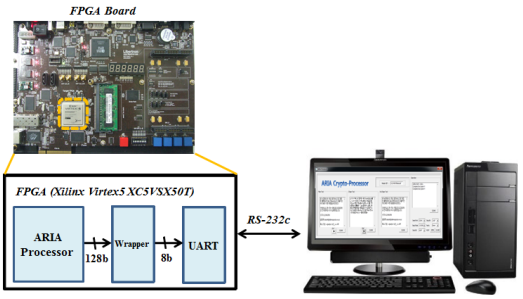
운드에서는 확산계층 대신 라운드 키 가산이 이루어지므로, 라운드 출력에 멀티플렉서를 달아 선택적으로 확산계층을 거치지 않은 치환계층의 출력이 라운드 입력으로 피드백 되도록 하였다 홀수와 짝수 라운드의 치환계층은 S-box의 배열이 다르므로 BP-SWAP 블록을 이용하여 입력과 출력의 포트를 재배치함으로써 홀수와 짝수 라운드의 치환계층이 공유되도록 하였다. 확산계층 블록에는 공통되는 XOR 연산을 묶어서 간략화 함으로써 90개의 8-비트 XOR를 60개의 8-비트 XOR로 구현하였다.

키 초기화 모듈은 라운드 함수와 XOR 연산의 3회 반복으로 동작되며, 멀티플렉서를 이용하여 Feistel구조에 있는 XOR 연산과 라운드 함수의 XOR 연산을 공유하여 사용하였다. 라운드 키 생성 모듈은 두개의 멀티플렉서와 시프트 회로로 구성되며, 키 초기화 모듈에서 생성된 W_k 값을 이용하여 on-the-fly 방식으로 라운드 키를 생성한다.

Ⅳ. 기능 검증 및 성능 평가

ARIA 암·복호 코어는 Verilog HDL로 설계되었으며, FPGA 구현을 통해 하드웨어 동작과 성능을 평가하였다. 설계된 ARIA 암·복호 코어는 그림 7(a)와 같이 FPGA 구현을 통해 하드웨어 동작을 확인하였다. 그림 7(b)는 FPGA 검증 결과이며, 평문을 암호화하여 암호문이 출력되고, 암호문을 다시 복호화 하면 원래의 평문이 출력됨을 확인할 수 있으며, 따라서 설계된 ARIA 암·복호 코어가 정상적으로 동작함을 확인하였다.

설계된 ARIA 암·복호 코어의 FPGA 합성 결과 11,146 slice로 구현되었으며, 167 MHz로 동작하여 1.07 Gbps의 성능을 갖는 것으로 평가되었다.



(a) FPGA 검증 시스템 구성도

(b) FPGA 검증 결과

그림 7. 설계된 ARIA 코어의 FPGA 검증

Ⅴ. 결 론

128-비트 입·출력과 128/192/256-비트의 마스터 키를 지원하며, ECB, CBC, OFB, CTR 4가지 암호 운영모드를 지원하는 ARIA 암·복호 코어를 FPGA로 구현하여 동작을 확인하였다. 회로의 면적을 줄이기 위해 키 초기화 모듈과 암복호 모듈의 라운드 함수를 공유하였다. FPGA 합성 결과 11,146 slice로 구현되었으며, 167 MHz로 동작하여 1.07 Gbps의 암·복호 성능을 갖는 것으로 평가되었다. 설계된 ARIA 암·복호 코어는 대량의 데이터를 고속으로 처리해야 하는 장치에서 보안성을 높이기 위한 시스템으로 응용이 가능하다

참고문헌

[1] 임용진, 홍진, 지성택, “스트림 암호의 발전 방향,” 한국정보과학회, 정보과학회지, 제23권, 제1호, pp. 40-45, 2005.

[2] 국가보안기술연구소, 민관겸용 블록 암호 알고리즘 ARIA 알고리듬 명세서, http://www. nsri.re.kr/ARIA, 2004.

[3] FIPS Publication197, “Advanced Encryption Standard (AES),” U.S. Doc/NIST

[4] 하성주, 이종호, “블록 암호 ARIA를 위한 고속 암호기/복호기 설계,” 전기학회논문지, 제57권, 제9호, pp. 1652-1659, 2008.

[5] 유권호, 구본석, 양상운, 장태주, “경량화된 확산계층을 이용한 32-비트 구조의 소형 ARIA 연산기 구현,”정보보호학회논문지, 제16권, 제6호, pp. 15-24, 2006.