The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 22, No. 1, pp.1-6, Feb. 28, 2022. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2022.22.1.1
JIIBC 2022-1-1

저전력 AES 암호시스템을 위한 경량의 S-Box 설계

Design of Lightweight S-Box for Low Power AES Cryptosystem

이상홍*

Sang-Hong Lee*

요 약 본 논문에는 저전력 AES(Advanced Encryption Standard) 암호시스템을 구현하기 위한 합성체 기반의 경량 S-Box 구조 설계를 제안한다. 제안한 방법에서는 $GF(((2^2)^2)^2)$ 상에서 사용면적 및 처리속도의 개선을 위해서 x^2, λ, 그리고 $GF((2^2)^2)$ 등 3개의 모듈을 1개의 모듈로 통합한 단순 구조로 설계한다. 설계된 AES S-Box는 Verilog-HDL를 기반으로 하여 구조적 모델링을 하였으며, Xilinx ISE 14.7툴 상에서 Spartan 3s1500l FPGA 소자를 타켓으로 하여 논리합성을 수행하였다. 논리적인 동작을 검증을 위한 시뮬레이션은 Modelsim 10.3 툴을 이용하였으며, 시뮬레이션 결과를 통하여 설계된 S-Box가 정확히 동작함을 확인하였다.

Abstract In this paper, the design of lightweight S-Box structure for implementing a low power AES cryptosystem based on composite field. In this approach, the S-Box is designed as a simple structure by which the three modules of x^2, λ, and $GF((2^2)^2)$ merge into one module for improving the usable area and processing speed on $GF(((2^2)^2)^2)$. The designed AES S-Box is modelled in Veilog-HDL at structural level, and a logic synthesis is also performed through the use of Xilinx ISE 14.7 tool, where Spartan 3s1500l is used as a target FPGA device. It is shown that the designed S-Box is correctly operated through simulation result, where ModelSim 10.3. is used for performing timing simulation.

Keywords : Low power AES, encryption, lightweight S-Box, composite field, Verilog HDL

Ⅰ. 서 론

네트워크를 통한 정보의 양은 증가와 더불어 많은 종류의 보안 문제가 야기 되고 있다[1][2][3]. 최근 사물인터넷(IoT: Internet of Things)을 통한 다양한 서비스가 이루어지면서 저면적 및 경량화가 요구되는 보안 제품들이 많이 개발되고 있다[4]. 그러나 IoT는 개인정보의 유출이나 침해, 위조 및 변조, 해킹에 의한 사생활 침해 등 다양한 위협에 항상 노출되어 있다[4][5]. IoT 환경에서 안전한 보안 서비스를 제공하기 위해서는 무결성, 기밀성, 가용성 그리고 공격 및 장애로부터 모든 컴퓨팅 자원을 보호하는 보안 기술이 필요하다[5].

암호화 기술은 데이터 변조 또는 정보의 누설을 방지하기 위해서 사용된다. AES(Advanced Encryption

*정회원, 안양대학교 컴퓨터공학과
접수일자 2022년 1월 10일, 수정완료 2022년 1월 31일
게재확정일자 2022년 2월 4일

Received: 10 January, 2022 / Revised: 31 January, 2022 / Accepted: 4 February, 2022
*Corresponding Author: shleedosa@gmail.com
Dept of Computer Science & Engineering, Anyang University, Korea

Standard) 알고리즘에서 가장 중요한 요소는 S-Box의 구성방식이다[6-8]. S-Box는 암호화 중에 총 전력의 75%를 소비하며, 주로 3가지 방식을 사용하여 구현하게 된다[7]. LUT(look-up table) 이나 ROM 기반의 S-BOX에서는 이미 계산된 값을 일정한 주소에 저장하여 사용하는 방식이다. 이 방식은 특정 위치에서 데이터를 가져오기 위한 여분의 회로가 필요하며, 구현하는데 보다 많은 면적이 요구된다. 이러한 문제점을 개선하기 위하여 제안된 Modified LUT 방법은 제안 되었으며, 보다 빠른 계산을 위해 디코더와 멀티플렉서를 사용한. 합성체를 기반의 AES 구현은 바이트를 대체하여 계산하는 방식을 사용기 때문에 복잡한 계산이 필요하다[7].

AES 암호 시스템의 구현 방식에 있어서 소프트웨어 기반의 S-Box는 하드웨어 방식에 비해 보다 쉽게 구현이 가능 하지만 실시간 데이터 처리 및 해킹 등의 보안에 취약한 편이다[9][10].

본 논문에서는 저전력 AES 암호 시스템을 구현하기 위한 합성체 기반의 경량 S-Box 구조 설계를 제안한다. 제안한 방법에서는 $GF(((2^2)^2)^2)$ 상에서 사용 면적 및 처리속도를 개선하기 위해서 x^2, λ, 그리고 $GF(2^2)^2$ 등 3개의 모듈을 1개의 모듈로 통합한 구조로 설계한다. 또한, 체 역변환(δ^{-1}) 및 아핀(Affine) 연산 모듈도 1개로 통합하여 연산을 수행한다.

II. 관련 연구

1. AES 암호 알고리듬

AES 암호 알고리듬은 128 비트의 데이터 블록을 암호화하며, 킷(key) 값은 128비트, 192비트 그리고 256비트 등 3종류를 사용한다[8]. 본 논문에서는 128 비트를 기준으로 S-Box를 설계한다.

그림 1은 AES 알고리듬에서의 암호화 과정에 대한 의사 코드를 나타낸다. 이 알고리듬은 1단계로 128비트의 평문값과 라운드 키에 대해 덧셈 연산을 수행하고, 라운드 변환은 16바이트의 크기로 구성된다. 그림 1에서 알 수 있듯이 SubByte(), ShiftRow(), MixColumn() 및 Add_Round_Key() 함수가 순차적으로 수행된다.

라운드의 마지막 단계에서는 MixColumn 연산만 제외한 3종류의 변환을 수행하여 암호화된 결과를 얻게 된다. S-Box는 SubByte 연산을 실행하며, 8비트의 입력이 사용되고 8비트의 출력값을 얻게 된다[8][9].

```
AES_Cipher()
{
    byte state;
    state = input;
    Add_Round_Key(state, w[0, Num-1]);
    for (round = 1 step 1 to Num-1) {
      SubByte(state);
      ShiftRow(state);
      MixColumn(state);
      Add_Round_Key(state, (round+1)*Num-1]);
    }
    SubByte(state);
    ShiftRow(state);
    Add_Round_Key(state,w[Num*Nb, (Nr+1)*Num-1]);
    output = state;
}
```

그림 1. AES 암호 알고리듬
Fig. 1. AES encryption algorithm

AES-128에서 SubByte 연산은 1바이트를 $GF(2^8)$ 상에서의 역원을 구한 후 아핀 변환을 행하고, 8비트씩 치환 연산을 통하여 16회 반복 수행한다[8]. 이 연산은 하드웨어 구성 시 가장 큰 면적이 요구되므로 보다 효율적인 S-Box 구조 설계가 필요하다.

2. LUT 기반의 S-Box 구조

LUT 기반의 S-Box는 ROM이나 PROM으로 구현되므로 많은 양의 메모리가 필요하다. 메모리에 저장된 데이터를 읽기 위해서는 행과 열을 검색하여 원하는 데이터를 가져오게 된다. ROM 기반의 S-Box는 구현이 용이하지만 많은 메모리가 소모되는 단점이 있다. 이 방법은 데이터를 엑세스한는데도 많은 시간이 요구되므로 이러한 문제점을 개선하기 위해서디코더와 멀티플렉서를 이용한 개선된 방법이 제안 되었다[6][7].

3. 합성체 기반의 S-Box 구조

AES 알고리즘에서 곱셈역원(multiplicative inverse)을 구하기 위하여 합성체를 기반으로 한 S-Box 에 대한 많은 연구가 진행중이다. $GF(2^8)$ 상에서 곱셈역원을 구하기 위해서는 $GF(2^8)$을 계수가 $GF(2^4)$인 1차 다항식으로 변환하여 사용한다. $GF(2^8)$상의 임의의 다항식은 x^2+Ax+b 형태의 기약 다항식(irreducible polynomial)을 기반으로 $bx+c$의 형태로 표현 가능하다. 이때 $bx+c$의 곱셈역원은 식 (1)과 같이 정의된다[9][10].

$$(bx+c)^{-1} = b(b^2\lambda+c(b+c))^{-1}x + (c+b)(b^2\lambda+c(b+c))^{-1} \quad (1)$$

여기서, A=1, B=λ를 사용하며, 기약 다항식은 $x^2 = x + \lambda$를 사용한다.

그림 2는 $GF(2^4)$을 사용하여 $GF(2^8)$ 상에서 곱셈 역원을 구하기 위한 블록도를 나타낸다[9].

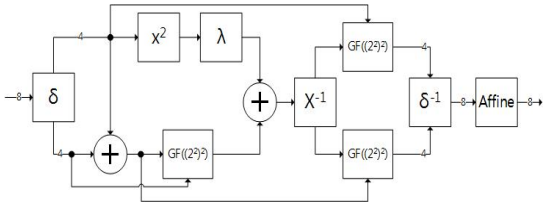

그림 2. 합성체 기반의 S-Box 블록도[9]
Fig. 2. Block diagram of Composite Field based S-Box[9]

합성체는 곱셈의 역원 계산이 수행되며 $GF(2^8)$는 보다 낮은 차수의 체 변환 즉, $GF(2), GF(2^2)$ 등 반복적으로 적용하여 구성이 가능하다. 이를 위해 식 (2)와 같은 기약 다항식을 사용할 수 있다.

$$\begin{aligned} &GF(2^2) &&: x^2 + x + 1 \\ &GF(2^2)^2) &&: x^2 + x + \phi \\ &GF(2^2)^2)^2) &&: x^2 + x + \lambda \end{aligned} \quad (2)$$

여기서 $\phi = 10_2, \lambda = 1100_2$ = $\{10\}_2$, 이다. 합성체에서 곱셈역원 계산은 $GF(2^8)$을 사용하는 소자로 직접 적용할 수 없다. 따라서 동형함수(isomorphic function) 인 δ를 통하여 해당 소자를 mapping 하여 체 변환후에 역원을 계산하고, 다시 역동형 함수(δ^{-1})를 사용하게 한다.

III. 경량 AES S-Box 설계

AES 128비트 알고리즘의 경우 SubByte 연산을 위해 16개의 S-Box가 참조되고, KeySchedule 에는 4개의 S-Box가 필요하므로 S-Box는 암호화에서 매우 큰 용량의 메모리가 요구된다[9].

SubByte 과정은 유한체 $GF(2^8)$ 상에서 곱셈 역원연산을 실행한 후, 아핀 변환(Affine Transformation)을 하게 된다. 그리고 InvSubByte 과정은 이와 반대로 수행하게 된다.

LUT 기반의 AES S-Box의 구현 방법은 입력에 대한 S-Box 출력값을 모두 LUT에 저장하기 때문에 메모리 낭비라는 문제가 있다[9][10].

기존의 곱셈역원 연산을 위한 S-Box 구조는 입력된 8비트의 입력 값은 체 변환 행렬에 의해 $GF(2^8)$에서 $GF((2^2)^2)$ 로 변환 후. 곱셈역원을 계산한다. 이때, 체 역변환 행렬 연산에 의해 다시 $GF(2^8)$의 형태로 변환되어 Affine 연산에 의해 최종 출력을 얻는다. $GF(((2^2)^2)^2)$ 상의 곱셈역원 연산을 위해 $GF((2^2)^2)$ 상의 곱셈 연산기($GF(2^4)$ 3개와 $GF(2^4)$ 상의 제곱(x^2 및 역원회로(x^{-1}), 그리고 XOR 연산회로가 필요하다[9].

역을 구하는 과정에서 $GF(2^4)$의 역원을 구하는 x^{-1}의 경우는 LUT를 이용하여 설계한다.

본 논문에서는 메모리 용량과 처리속도를 개선하기 위한 경량의 S-Box의 구조를 설계한다.

그림 3은 $GF(((2^2)^2)^2)$ 상에서 곱셈역원을 구하기 위한 경량의 S-Box 구조를 나타낸다.

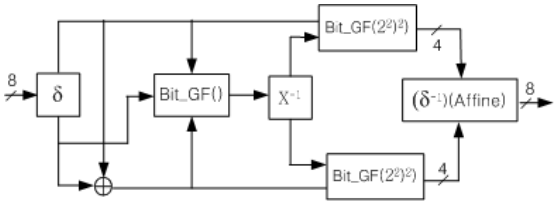

그림 3. 제안하는 합성체 기반의 경량 S_Box 구조
Fig. 3. Proposed lightweight S-Box structure based on Composit Field

제안한 방법에서는 $GF(((2^2)^2)^2)$ 상에서 저면적 설계 및 빠른 연산을 수행하기 위해 x^2, λ, $GF((2^2)^2)$ 등 3개의 모듈을 1개의 모듈인 *Bit_GF()* 모듈로 통합, 설계한다. 또한, 체 역변환(δ^{-1}) 및 아핀(Affine) 연산 모듈도 1개로 통합하여 연산을 수행하도록 설계한다.

$GF(((2^2)^2)^2)$상의 유한체 곱셈기를 설계하기 위해서 4비트의 출력 값을 $k = qw$ 로 정의한다. 여기서 $k = k(k_3k_2k_1k_0), q = q(q_3q_2q_1q_0), w = w(w_3w_2w_1w_0)$ 이다. 입력값 $x = 4$비트에서 상위 2비트는xH, 하위 4비트는 xL로 표기하고, 식 (3)을 얻는다.

$$\begin{aligned} k &= kHx + kL \\ &= (qHx + qL)(wHx + wL) \\ &= (qHwH)x^2 + (qHwL + qLwH)x + qLwL \end{aligned} \quad (3)$$

여기서$x^2 = x + \phi$ 일때 식 (3)을 정리하면 식 (4)와 같은 수식을 얻을 수 있다.

$$k=(qHwH)(x+\phi)+(qHwL+qLwH)x+qLwL \quad (4)$$
$$=(qHwH)+qHwL+qLwH)x+qHwH\phi+qLwL$$

식 (4)를 이용하면 $GF(((2^2)^2)^2)$의 곱셈 회로도를 구현할 수 있다. $GF(2^4)$ 상의 제곱연산(x^2) 을 계산하기 위한 수식은 식 (3)을 사용한다[9].

$$k_3=q_3$$
$$k_2=q_3\oplus q_2$$
$$k_1=q_2\oplus q_1$$
$$k_0=q_3\oplus q_1\oplus q_0 \quad (5)$$

또한, $\times\lambda$ 모듈은 식 (6)을 이용하여 설계한다.

$$k_3=q_2\oplus q_0$$
$$k_2=q_3\oplus q_2\oplus q_1\oplus q_0$$
$$k_1=q_3$$
$$k_0=q_2 \quad (6)$$

그림 4는 본 논문에서 제안하고 있는 경량 S_Box의 Main 모듈을 나타낸다.

```
module S_Box();
    delta d2(IN, del);
    assign b = del[7:4];
    assign c = del[3:0];
    Bit_GF(IN, tmp5);
    iinv_lut i1(tmp5, tmp6);
    mul_gf2_4 m4(b, tmp6, val[7:4]);
    mul_gf2_4 m5(b ^ c, tmp6, val[3:0]);
    del_and_aff daf1(val, OUT);
endmodule
```

그림 4. 제안하는 경량 S_Box의 Main 모듈
Fig. 4. Main module of proposed lightweight S-Box

결과적으로, 본 논문에서 제안하는 방법은 기존의 구조[5]의 $GF((2^2)^2)$ 곱셈 연산에 필요한 3개의 $GF(2^2)$ 곱셈기와 ϕ 연산 과정이 불필요하게 되어 메모리 용량 및 연산속도가 개선되어 경량의 AES S-Box를 구현이 가능하다. 또한, δ^{-1}과 Affine 연산도 하나의 모듈로 통합하는 방식을 취하여 전체 곱셈역원 연산과정에서 발생하는 회로지연을 줄일 수 있다.

IV. 시스템 구현 및 성능 평가

본 논문에서 제안한 AES 암호화를 위한 경량 AES S-Box는 Verilog-HDL을 사용하여 기술하였고, Xilinx ISE 14.7툴 상에서 Spartan 3s1500l FPGA 소자를 타깃으로하여 합성을 수행하였다. 그림 5는 합성결과를 캡쳐한 RTL schematic 뷰를 나타낸다.

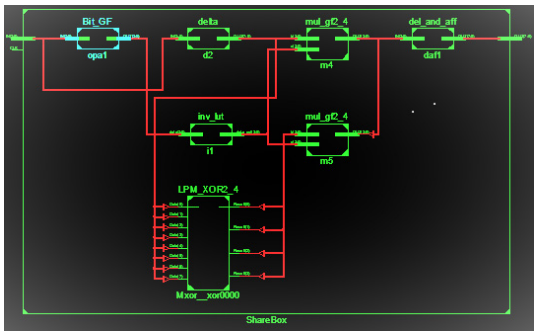

그림 5. 구현된 S-Box의 RTL 회로
Fig. 5. RTL schematic of Implemented S-Box

그림 5에 나타난 Bit_GF 모듈이 x^2, λ, 그리고 $GF((2^2)^2)$ 모듈이 통합된 회로를 나타내고 있다. 그리고 del_and-Aff 모듈이 체 역변환(δ^{-1}) 및 아핀(Affine) 연산 모듈이 1개로 통합된 연산회로이다. 설계된 S-Box에 대한 논리동작의 검증은 ModelSim PE 10.3을 이용하여 시뮬레이션을 수행하였다. 그림 6은 S-Box의 시뮬레이션 결과를 나타낸다.

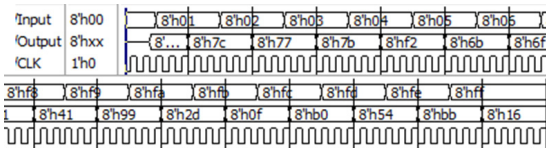

그림 6. S-Box의 시뮬레이션 결과
Fig. 6. S-Box simulation result

시뮬레이션 결과를 통하여 설계된 S-Box가 정확히 동작함을 확인하였다. 표 1은 조합회로로 구성된 기존의 방법들[9][10]과 제안한 방법에 대한 성능비교 결과를 나타낸다.

표 1. AES S-Box의 성능비교
Table 1. Performance comparison of AES S-Box

Items / Methods	No of Slices	No of LUTs	Max. path delay(ns)
Mui[9]	39	69	27.653
Saurabh[10]	44	76	32.388
Proposed1	42	74	26.822
Proposed2	44	78	25.459

공정한 성능 평가를 수행하기 위해 공히 Spartan xc3s1500L FPGA 를 사용하여 저자가 직접, 컴파일 및 합성을 수행하여 결과를 도출하였다. 표 1의 비교에서 알 수 있듯이 제안한 방법인 Proposed2는 최대 경로지연(Maximum path delay)의 비교에서 Saurabh[10] 방법 보다 약 21% 정도, 그리고 Mui[9]의 방법 보다 약 9% 정도 개선됨을 확인 하였다.

표 2는 2단계의 파이프라인(pipeline) 방식을 사용하여 기존의 방법과 제안한 방법[9][10]에 대한 성능을 비교한 것이다. 파이프라인 구성에서 사용된 레지스터는 각각 x^{-1}모듈의 앞단과 del_and-Aff 모듈의 앞단에서 사용하였다. 면적 사용량 비교에서 기존의 방법 보다 제안한 방법(Propose2)이 비교적 적은 면적을 요구한다.

표 2. 파이프라인으로 구성된 AES S-Box의 성능비교
Table 2. Performance comparison of pipelined AES S-Box

Items / Methods	No of Slices	No of FFs	No of LUTs	Minimum period(ns) (Freq[Mhz])
Mui[7] (2-pipes)	47	16	86	10.662 (93.791)
Saurabh[8] (2-pipes)	44	16	82	9.674 (103.370)
Propose2 (2-pipes)	43	12	80	7.931 (126.087)

구현된 경량 S-Box는 최대 126Mhz로 동작하며, 최소 지연시간은 기존의 방법[9]과의 비교할 때 약 18% 정도 개선되었다.

V. 결 론

본 논문에서는 저전력 AES 암호 시스템의 구현을 위한 합성체 기반의 경량 S-Box 구조를 제안하였다. 제안하는 방법1(Proposed1)에서는 LUT 기반의 기존 구현 방법과 달리 조합 논리를 사용하여 설계하여 설계 면적 및 처리 속도 면에서 최적화가 되도록 구성하였다. 또한, 제안하는 방법 2(Propose2(2-pipes))에서는 2단 파이프라인을 기반으로 하여 경량의 S-Box 구조를 설계하였고, 기존의 방법[9][10] 보다 비교적 적은 면적으로 처리속도가 개선됨을 확인 할 수 있다.

향후, 연구 과제로서 다양한 IOT 서비스 환경에서 개인정보의 유출이나 침해, 위조 및 변조, 해킹에 의한 사생활 침해 등을 방지하기 위하여 경량의 IOT 소자를 위한 최적의 AES 암호프로세서 개발이 필요하다.

References

[1] Min-Sup Kang, "Design of Real-Time CCTV Image Security Systems using Frame Partition Threads", Journal of KIIT, Vol. 19, No. 3, pp. 113-119, Mar 2021.
DOI: https://doi.org/10.14801/jkiit.2021.19.3.113

[2] Hong-Pil Kwon, Jae-Cheol Ha, "Power Analysis Attack of Block Cipher AES Based on Convolutional Neural Network", Journal of the Korea Academia-Industrial cooperation Society(JKAIS), Vol. 21, No. 5, pp. 14-21, 2020.
DOI: https://doi.org/10.5762/KAIS.2020.21.5.14

[3] Su-Bong Ryu, Min-Sup Kang, "Implementation of Image Security System for CCTV Using Analysis Technique of Color Informations", The Journal of the Institute of Internet, Broadcasting and Communication, Vol. 12, No. 5, pp. 219-227, Oct 2021.
DOI: https://doi.org/10.7236/JIWIT.2012.12.5.219

[4] CISCO, "IoT", https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html#~stickynav=1(accessed Jan., 10, 2017.

[5] M. Katagi and S. Moriai, "Lightweight Cryptography for the Internet of Things", sony corporation, 2011. 3.

[6] Abhishek Kumar and Sokat Tejani, "S-BOX Architecture" : Futuristic Trends in Network and Communication Technologies, :Springer Singapore, 2019.
DOI: https://doi.org/10.1007/978-981-13-3804-5_2

[7] Pammu, A.A., Chong, K.-S., Gwee, B.-H.: Secured low power overhead compensator Look-Up-Table(LUT) Substitution Box (S-Box) Architecture, IEEE International Conference on Networking, Architecture, and Storage (NAS), August 2016, pp. 1-7, 2016.

[8] FIPS 197, "Advanced Encryption Standard (AES)", November 26, 2001.

[9] Edwin NC Mui, "Practical Implementation of Rijndael S-Box Using Combinational Logic", Custom R&D Engineer Texco Enterprise Pvt.Ltd, 2007.

[10] Saurabh Kumar, V.K. Sharma and K. K. Mahapatra, "Low Latency VLSI Architecture of S-Box for AES Encryption" IEEE International Conference on Circuits, Power and Computing Technologies (ICCPCT), March 2013.
DOI: https://doi.org/10.1109/ICCPCT.2013.6528906

저 자 소 개

이 상 홍(정회원)

- 1999년 2월 : 경원대학교 전자계산학과(공학사)
- 2001년 2월 : 경원대학교 일반대학원 전자계산학과(공학석사)
- 2012년 2월 : 경원대학교 일반대학원 전자계산학과(공학박사)
- 2013년 3월 ~ 현재 : 안양대학교 컴퓨터공학과 조교수

•관심분야 : neuro-fuzzy system을 이용한 전문가 시스템