IDEC Chip Design Contest

AES–128 알고리즘을 이용한 암호화 프로세서 구현

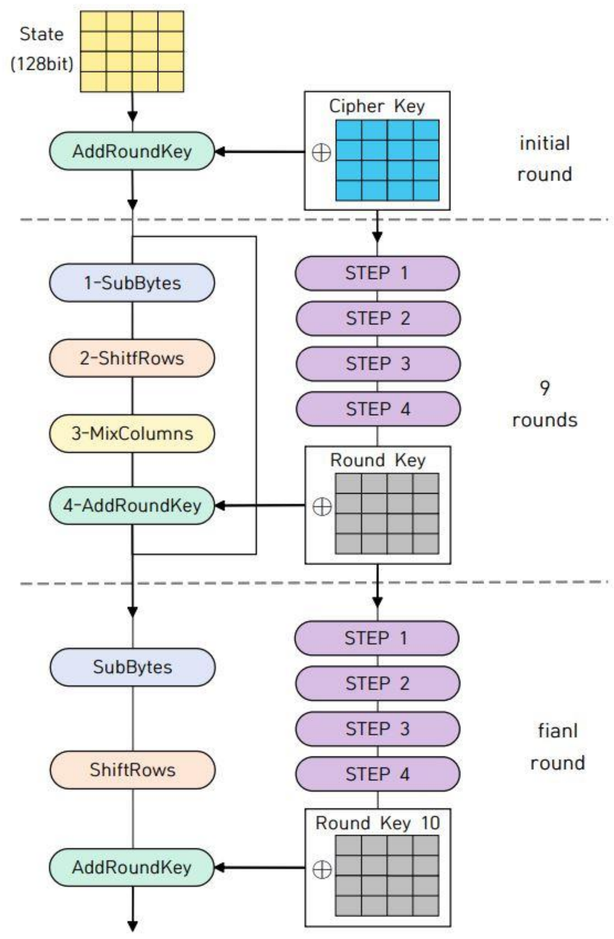
김보미, 신주인, 정진균
전북대학교 전자공학부

Introduction

정보통신기술의 융합으로 이뤄지는 4차 산업 혁명이 도래함에 따라 더 많은 정보를 다룰 수 있게 되었다. 그로 인해 데이터를 송수신하는 과정에서 타인에게 알려지지 말아야 할 개인적인 정보와 중요한 정보가 가로채어지거나 노출되고, 해당 정보들을 악용하는 경우도 증가하였다. 이러한 피해를 예방하고, 중요한 정보들을 보호하기 위한 암호화 기술이 필요하게 되었다 [1]-[3]. AES(Advanced Encryption Standard) 알고리즘은 대칭형 블록 암호 알고리즘으로 미국 국립표준기술연구소에서 컴퓨터의 계산 능력 향상으로 인해 안전성 저하 문제가 대두된 DES (Data Encryption Standard) 알고리즘을 대체하기 위해 채택되었다 [4]-[6]. DES보다 보안성능이 우수해 차세대 암호표준으로 제안된 AES는 벨기에의 Joan Daemen과 Vincent Rijmen이 개발한 Rijndael를 기반으로 하며 보안성, 효율성, 융통성의 동작 특성 또한 갖추고 있다 [7]. 본 논문에서는 정보의 암호화에 있어 AES-128 알고리즘을 사용하며, 이를 MATLAB으로 먼저 검증한 후, Verilog- HDL을 이용하여 암호화 프로세서를 기술하고 CMOS 180nm 공정을 이용하여 구현한다.

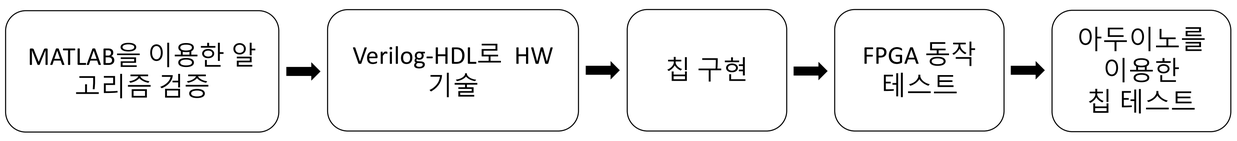
AES-128 알고리즘

AES-128은 암호화할 데이터(State)와 암호화 키(Cipher Key)를 4×4바이트 행렬 형태로 구성하여 암호화를 수행하는 알고리즘으로 먼저 암호화할 데이터와 Cipher Key를 입력으로 하여 AddRoundKey를 하는 initial round를 진행한다. 이후 1-SubBytes, 2-ShiftRows, 3-MixColumns, 4-AddRoundKey의 순서로 이루어진 round를 10번 반복하는데 마지막 10번째 final round에서는 3-MixColumns을 제외하고 진행한다. 그 결과 암호화된 값이 출력된다.



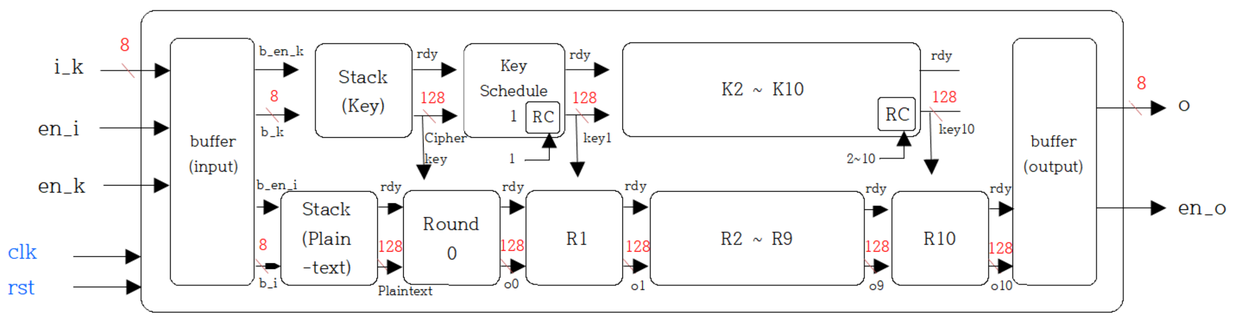
[AES-128 알고리즘 플로우]

알고리즘 검증은 MATLAB을 이용하여 모델링 한후, 그 결과와 Verilog 로 기술하고 FPGA 를 이용하여 AES-128 암호화 와 복화화 동장을 비교 검증하였다. 검증 후 CMOS 180nm 공정을 통해 Synopsys 사의 Design Compiler로 합성하고 Astro 을 이용하여 P&R 을 진행하였다.

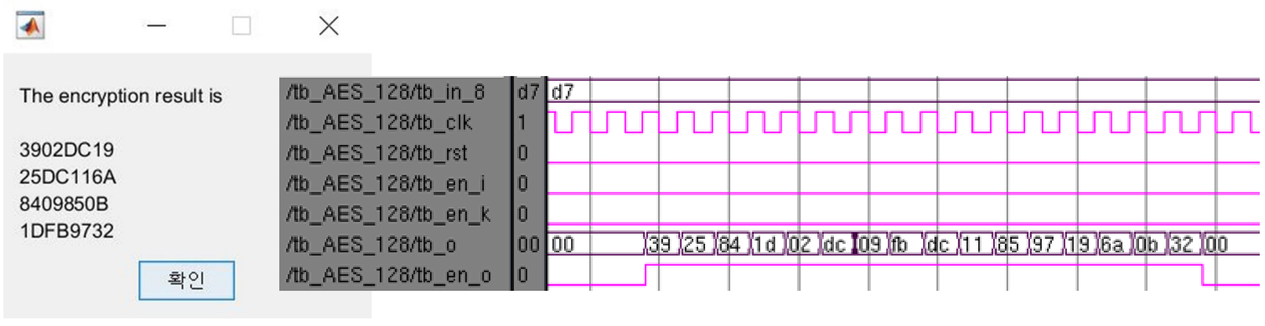


[AES-128 프로세서 설계 검증 플로우]

AES-128 아키텍처

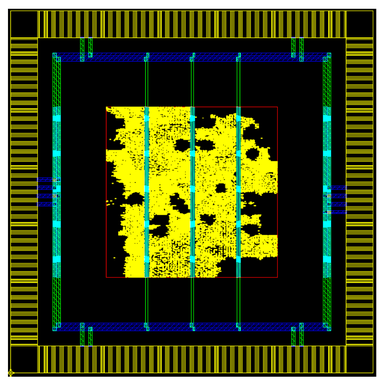


[AES-128 프로세서 구조]

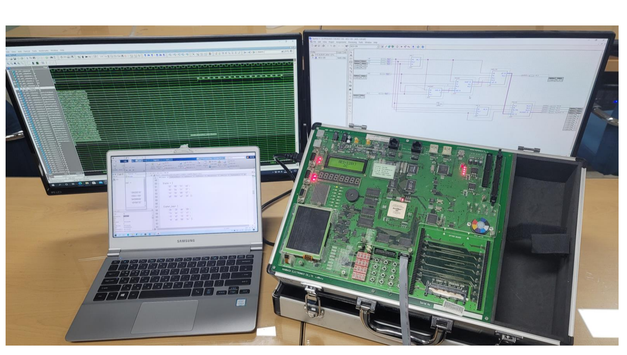


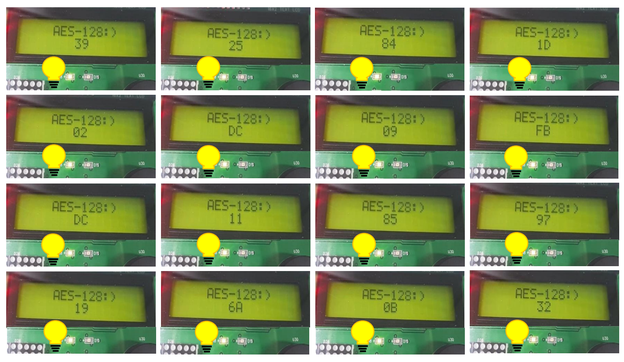
[시뮬레이션 결과]

ITEM	CONTENT
SIZE [GC]	147709 GC
POWER	37.1492mW
CORE SIZE [μm^2]	1495×1491μm^2
INPUT PORT	clk, rst, en_i, en_k
OUTPUT PORT	en_o
DATA PORT	i_k, o



[구현 결과]





[테스트 결과]

Conclusions

본 논문에서는 대칭형 블록 암호 알고리즘으로 블록 길이와 키 길이가 128비트인 AES-128 알고리즘을 하드웨어 프로세서로 구현하였다. 그 과정에서 이 알고리즘을 MATLAB을 이용하여 검증하고, 하드웨어 기술 언어인 Verilog-HDL로 설계한 후, 합성과 P&R을 하여 하드웨어를 설계 및 구현하였다. 구현한 프로세서는 FPGA로 동작 테스트를 하였고, 테스트 결과는 MATLAB을 이용한 검증 결과와 일치하였다. 본 논문에서 구현한 암호화 프로세서는 사물인터넷과 임베디드 시스템 같은 소형, 경량, 저전력, 실시간 수행 등의 제약이 있는 환경에서 활용이 가능하다.

References

[1] Jin Hyung Park, “AES-CTR-C : Efficient Implementation of AES CTR Mode”, 2011.
[2] Ashwini M. Deshpande, Mangesh S. Deshpande and Devendra N. Kayatanavar, “FPGA Implementation of AES Encryption and Decryption”.
[3] Atul M. Borkar, R. V. Kshirsagar and M. V. Vyawahare, “FPGA Implementation of AES Algorithm”.
[4] HK Ahn, KH Park and KW Shin, “A Cryptoprocessor for AES-128/192/256 Rijndael Block Cipher Algorithm”, Journal of the Korea Institute of Information and Communication Engineering, pp. 427-433, 2002.05
[5] Chih-Chung Lu and Shau-Yin Tseng, “Integrated Design of AES (Advanced Encryption Standard) Encrypter and Decrypter”.
[6] Sung-Ho Shin and Jae-Heung Lee, “The Hardware Implementation of AES-128 Rijndael Cipher Algorithm”, 한밭대학교 정보통신전문대학원 논문집, 2004.
[7] Myung-Yong Choi, Chang-Soo Park and Gyeong-Yeon Cho, “Modified AES Algorithm for Implementation of Efficient Hardware”, 한국멀티미디어학회 학술발표논문집, pp. 484-487, 2005.05.
[8] Beomsik song, “Observation on the Cryptologic Properties of the AES Algorithm”, 2004.

2021 IDEC Congress CDC
The chip fabrication and EDA tool were supported by the IC Design Education Center(IDEC), Korea.
반도체설계교육센터 IC DESIGN EDUCATION CENTER