2025 전자공학 공학설계 페스티벌

51.2 Gbps 4-Parallel Pipeline AES-GCM 암호화 가속기

◐ 참 가 팀 소속 : 국민대학교 창의공과대학 전자공학부 (지도 교수 : 민경식)
◐ 참 가 팀 이름 : Courtist (김현욱, 김승현, 김유성, 추지훈)

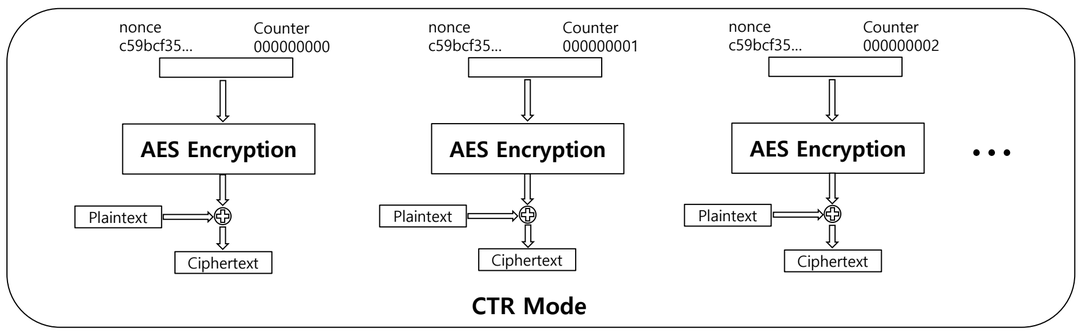
1. Abstract

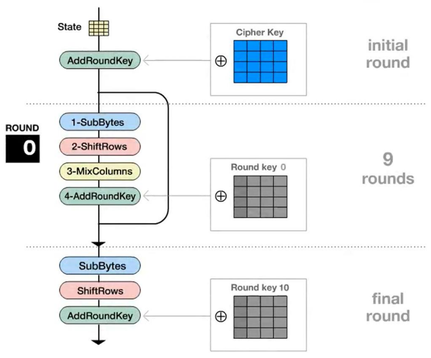
CPU 기반 하드웨어 연산은 직렬 연산 중의 Latency로 인해 기가비트급 대역폭 처리 시 병목 현상이 발생하며 전력 효율성과 처리속도 측면에서도 물리적 한계를 가진다. 본 설계에서는 Xilinx Artix-7과 Xilinx Vivado Design Suite을 활용하여 100MHz 시스템 클럭에서 단일 암호화 모듈의 전력, 면적을 최적화하고, 병렬 및 파이프라인 설계를 도입해 대역폭을 극대화한다. 이를 통해 대량의 스트림 데이터를 암호화하고, 취약점을 보완하기 위해 GHASH 인증 태그로 데이터 무결성 검증을 수행하는 AES-GCM를 구현한다. 4-병렬 파이프라인 AES-128 암호화 모듈 설계를 통해 Pipeline Register Stalling 이후 10ns마다 512-bit IV Counter를 한번에 암호화하여 51.2 Gbps의 처리량을 달성하였다.

2. Methods

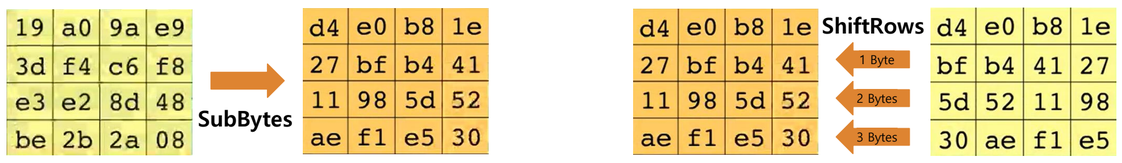
AES-128 + GCM(CTR + AEAD) Mode

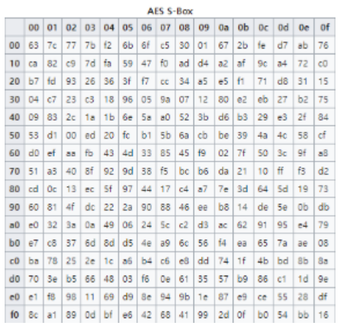
AES-128은 데이터를 128비트 단위로 처리하는 128비트 키 길이의 대칭키 알고리즘
AES-CTR은 IV Counter의 AES 암호화를 통한 Key Stream으로 평문과 XOR 연산해 암호문을 출력
모든 카운터 값은 독립적이며, 병렬 처리가 가능
AES-GCM은 암호문과 Galois Field 연산을 통해 인증 태그를 생성해 무결성 및 인증을 제공



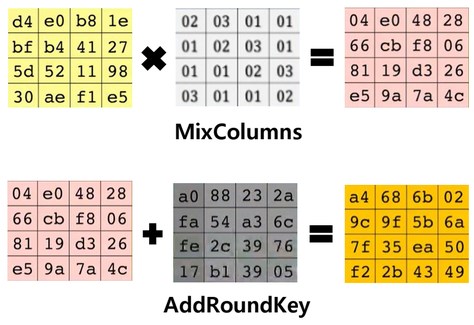


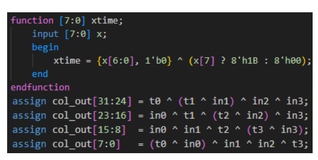
- Initial Round: 128비트 고유 counter block을 1 byte 4×4 행렬(State)로 구성하고 Initial Round key와 XOR 연산
- Main Round: 128비트의 경우 9회 반복
  1. SubBytes: 치환 상자(S-Box)를 이용하여 State 치환
  2. ShiftRows: State의 행이 왼쪽으로 0,1,2,3 바이트씩 이동
  3. MixColumns: State의 각 열을 특정 행렬 곱셈 연산
  4. AddRoundKey: State에 해당 Round Key를 XOR
- Final Round: Main round에서 Mixcolumns 단계가 제외되며 이 결과와 평문을 XOR하면 최종 암호문 출력





S-BOX

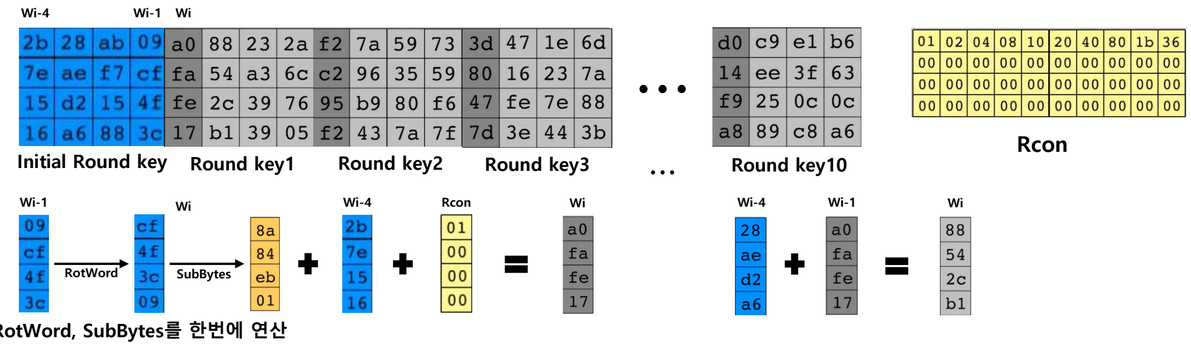




GF(2) 갈루아 필드 연산 함수 재활용으로 면적, 전력 절감

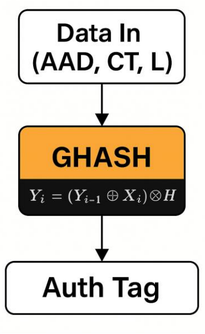
Key Expansion

AES는 여러 번의 Round를 반복하여 암호화를 수행하며, 각 Round는 서로 다른 128비트의 Round Key가 필요
따라서 Initial Key로부터 각 Round에 사용되는 Round Key를 다음 연산을 통해 확장



AEAD(Authenticated Encryption with Additional Data)

GHASH 함수로 생성된 AEAD 인증 태그는 데이터의 무결성과 인증을 보장하여 데이터의 무결성과 인증을 동시에 제공



Karatsuba Algorithm

$$A = A_H \cdot x^{64} + A_L$$
$$B = B_H \cdot x^{64} + B_L$$

$$A \times B = (A_H \cdot x^{64} + A_L)(B_H \cdot x^{64} + B_L)$$
$$= A_H B_H \cdot x^{128} + (A_H B_L + A_L B_H) x^{64} + A_L B_L$$ 곱셈기 4개 소모

XOR XOR XOR XOR

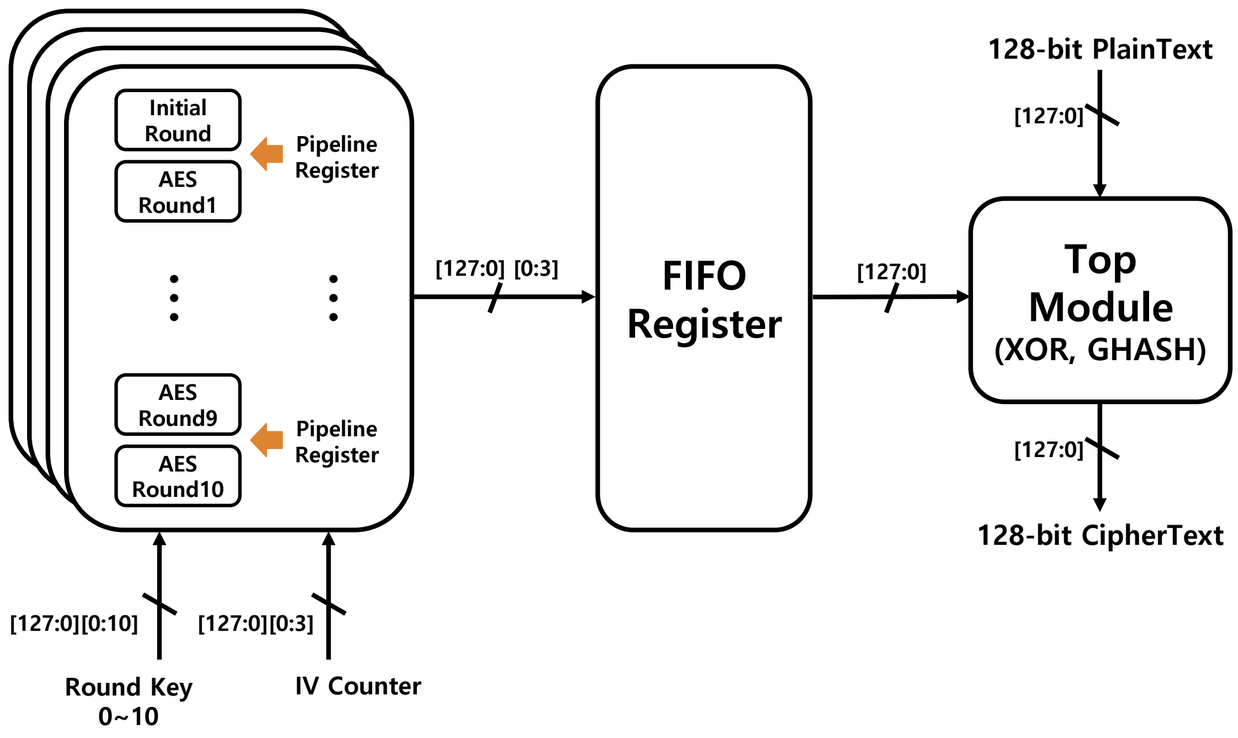
$$A_H B_L + A_L B_H = (A_H + B_L)(B_H + A_L) - A_H B_H - A_L B_L$$ 곱셈기 3개 소모

면적, 전력 감소, Timing 유리

H: 0으로 채워진 128비트 블록을 암호화한 결과
Xi: Data In(AAD, Ciphertext, Length)
Yi: GHASH 연산 결과(누적), 초기 값은 0

송신자는 IV, 암호문에 더해 AAD와 인증 태그를 첨부하여 전송
수신자는 동일한 알고리즘으로 태그를 재생성하고(1 clk만에 연산 가능), 이를 수신된 태그 값과 비교(Compare)함으로써 전송 중 발생할 수 있는 위·변조 탐지 가능

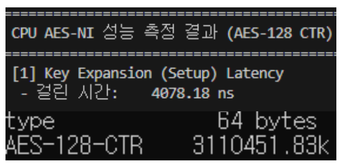
암호화 병렬 및 파이프라인 구조

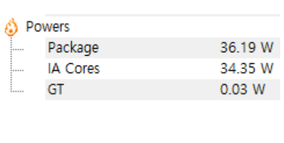


3. Result

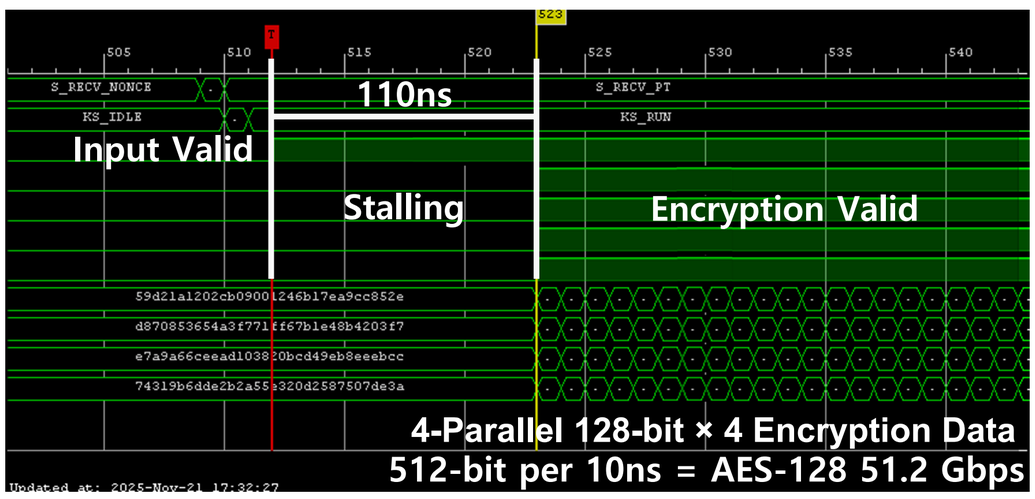
※암호화 검증을 위해 UART 사용

FPGA vs AES-NI 비교 (Xilinx Artix-7 vs 12th Gen Intel(R) Core(TM) i5-12600K)

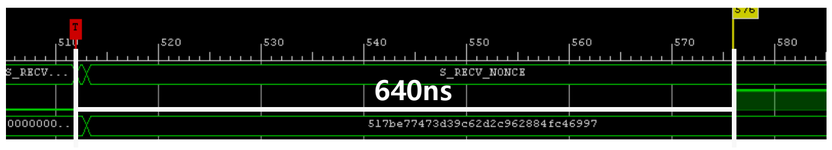




AES-NI OpenSSL 벤치마크 결과
Key Expansion : 4078.18ns
3110451.83KB/s = 25.48 Gbps
전력 : 약 18.35W (기본 전력 제외)



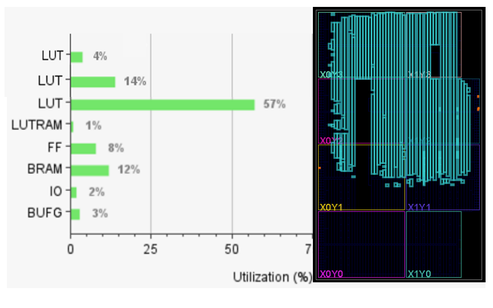
<Data Encryption>

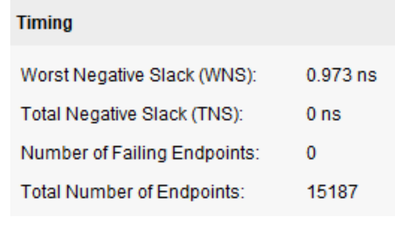


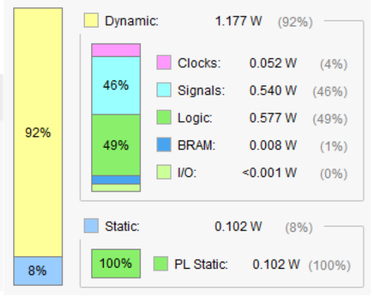
<Key Expansion>

Key Expansion : 약 6.37배
Throughput : 약 2.01배
Power : 약 14.35배 효율적

FPGA 사용량







단일 모듈 재활용시 : LUT 4%
단일 파이프라인 구조 : LUT 14%
4-병렬 파이프라인 구조 + AEAD
: LUT 57%로 저면적 고효율 활용

100Mhz Clock 9.73%의 Timing Margin 확보

1.279W의 On-Chip Power 소모로 저전력 특성 달성