최신 블록 암호 구현 기법

비트슬라이딩

Jean, Jérémy, et al. "Bit-Sliding: A Generic Technique for Bit-Serial Implementations of SPN-based Primitives." *International Conference on Cryptographic Hardware and Embedded Systems*. Springer, Cham, 2017.

SPN(Substitution-Permutation Networks)

- 비선형 요소(S)와 선형 요소(P)로 이루어진 암호 구조

구현 타협점 – 고려 요소

- 처리율
- 면적

구현 타협점 – 구현 방법

- 라운드 기준 구현
- 전체 구현
- 시리얼 구현

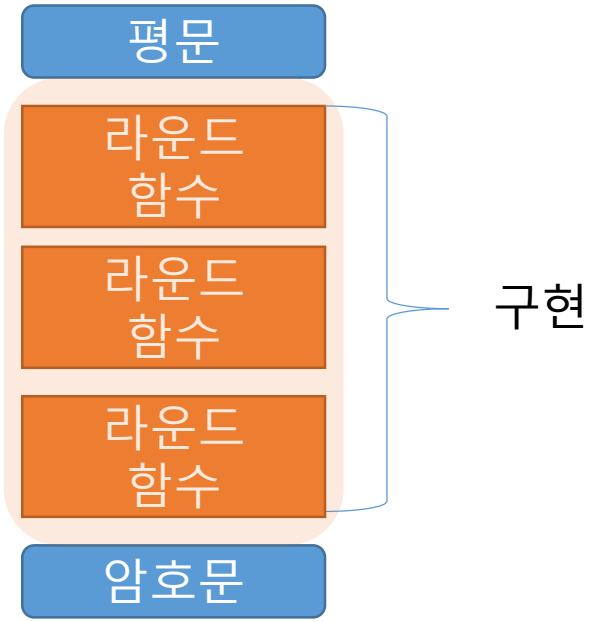
구현 타협점 – 구현 방법

- **라운드 기준 구현**

처리율	준수
면적	준수

구현 타협점 – 구현 방법

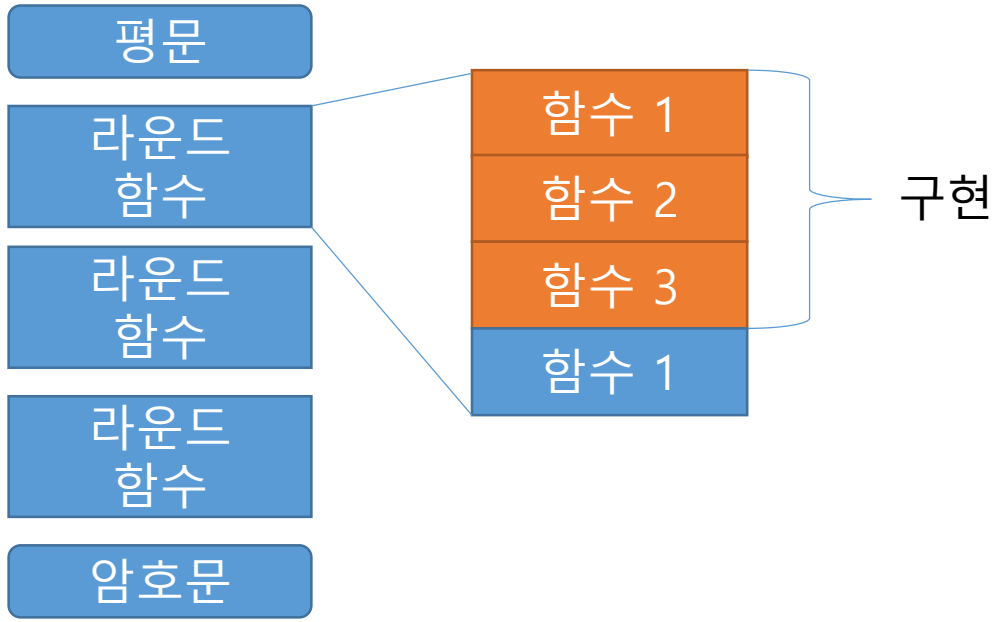
- **전체 구현**



고려 요소	
처리율	극대화
면적	-

구현 타협점 – 구현 방법

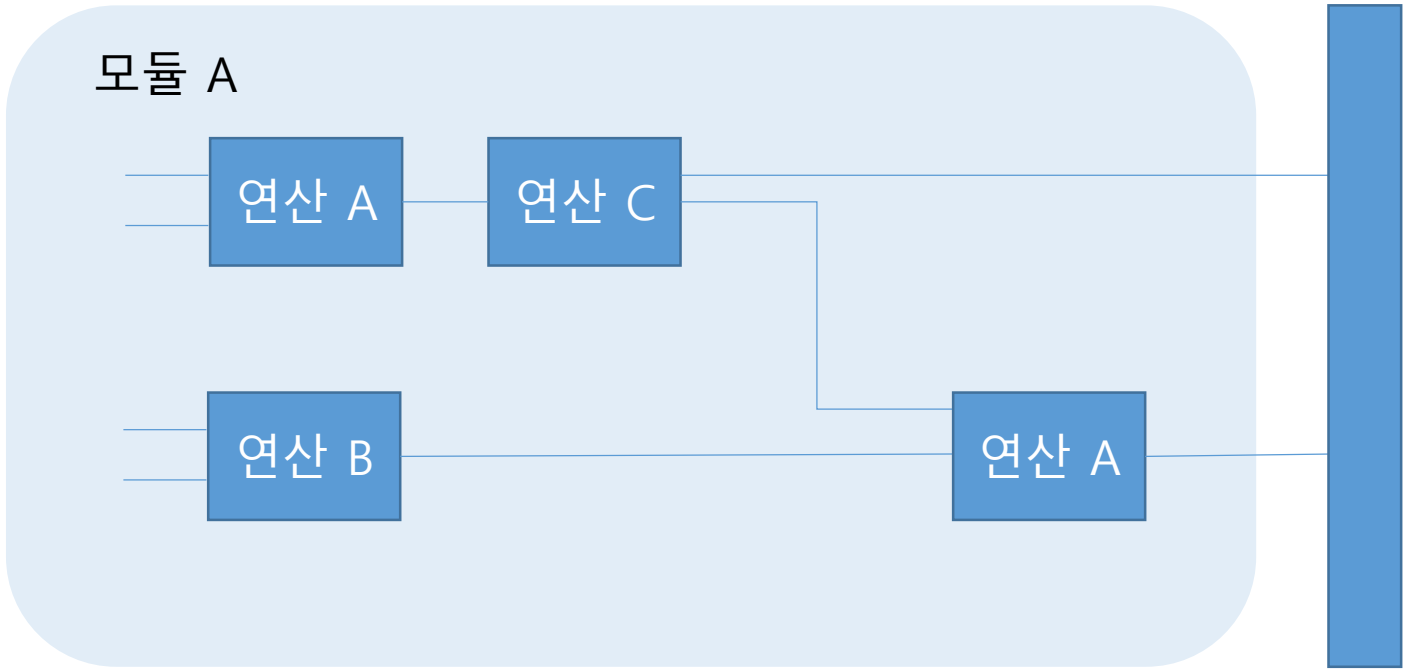
- **시리얼 구현**



고려 요소	
처리율	-
면적	극대화

데이터 이동 경로

가장 느린 데이터 경로



플립-플롭(Flip-Flop)

- 게이트 출력 값을 유지하기 위해 만들어진 장치

- 특정 신호가 변화할 때 입력을 이용하여 출력을 생성 (입력을 기억)

멀티플렉서(MUX)

- 여러 입력 중 하나를 출력

스캔 플립-플롭

- 플립플롭 + 멀티플렉서
  (FF + MUX)

- 데이터 입력, 스캔 입력 중 선택하여 데이터를 저장

플립-플롭 vs 스캔 플립-플롭

- 비트들의 복잡한 연결 -> 스캔 플립-플롭의 사용

- 일반 플립-플롭의 사용을 극대화
  -> 비트슬라이딩

비트슬라이딩

- 암호문의 첫 비트에 의해 복잡한 비트 연결을 다룸
- 첫 비트(스캔 플립-플롭에 저장)
  나머지 비트(플립-플롭에 저장)
- 순차적으로 S박스 출력 비트들을 밀어냄(스캔 플립-플롭 사용)
  출력 비트의 저장에는 기존의 회로를 사용

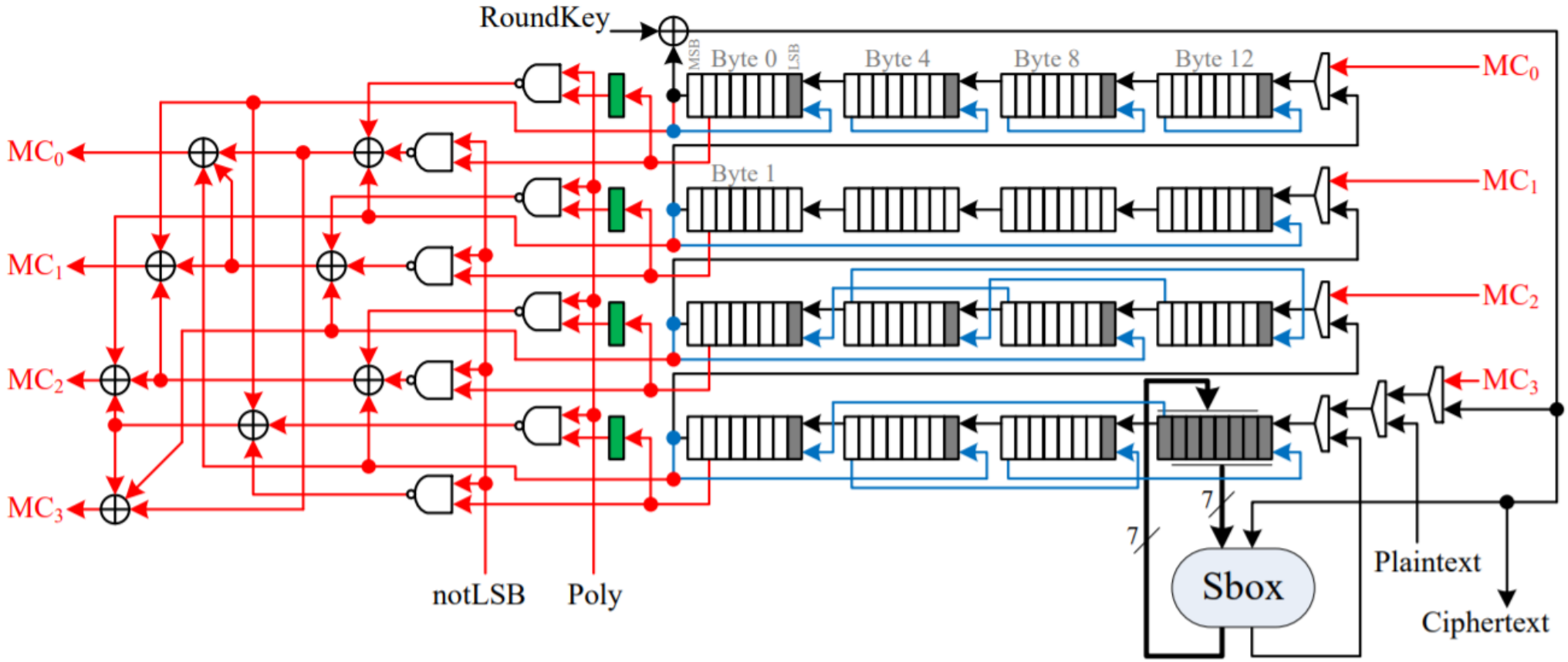
AES(Advanced Encryption Standard)-128

- SPN 구조의 표준화 암호

- 128비트 키 버전

- AK(AddRoundKey)
- SB(SubBytes)
- SR(ShiftRow)
- MC(MixColumns)

비트슬라이딩을 AES-128에 적용



결과

종류	알려진 최소 면적 구현	비트슬라이딩 구현
암호화	2182GE	1563GE
암호화/복호화	2413GE	1744GE

- 같은 라이브러리 사용 기준 (IBM 130nm Library)
- ASIC 구현 기준