Technology trends of Implementation of AES

Yongbeen Kwon * Hyeokdong Kwon * Hwajeong Seo *†
* 한성대학교 대학원 IT응용공학과

요 약

● 국제표준암호 AES의 최신 구현 기법들의 소개

연구 목적

● AES의 면적 효율성을 극대화 시키기 위한 비트-시리얼 구현 기법 “비트슬라이딩”

● AES의 처리율을 극대화 시키기 위한 캐시, 룩업테이블 활용 기법 “FACE”

연구 소개 1 비트 슬라이딩

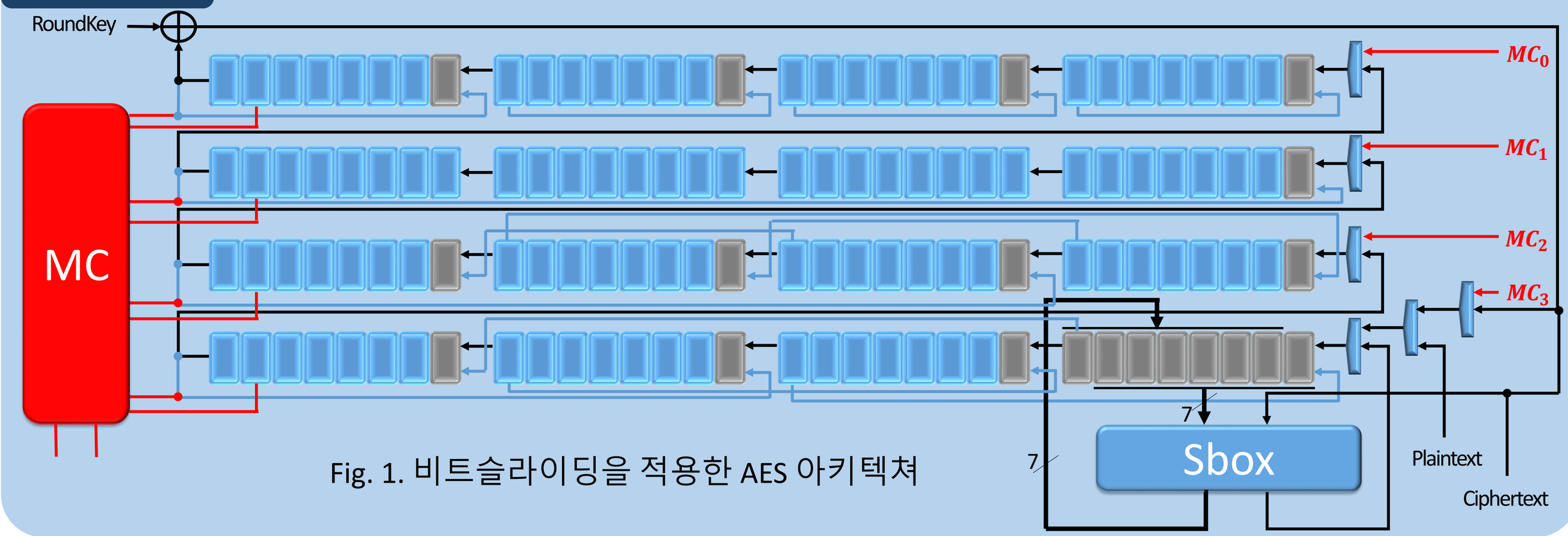

Fig. 1. 비트슬라이딩을 적용한 AES 아키텍쳐

연구 소개2 FACE(Fast AES Counter mode Encryption)

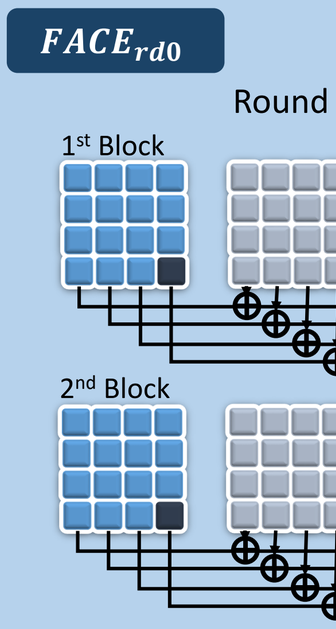

Fig. 2. FACE 기법1

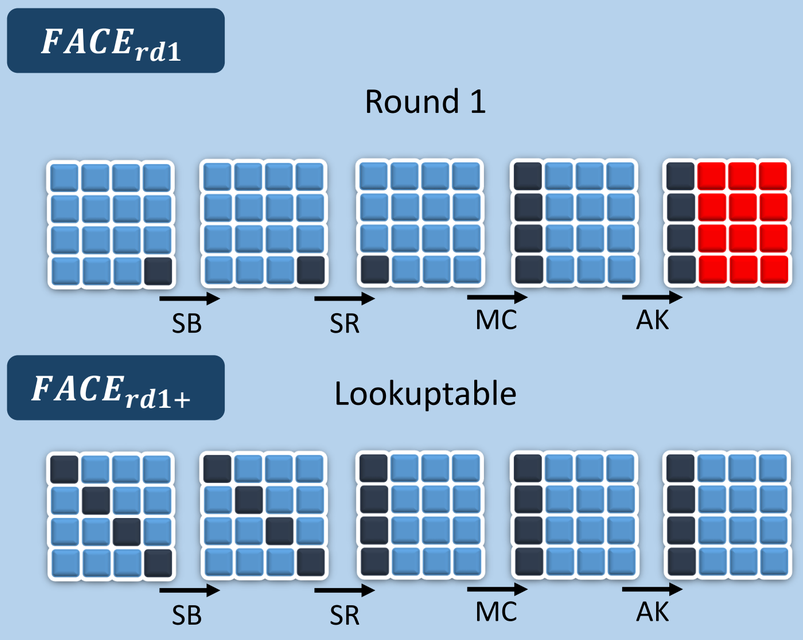

Fig. 3. FACE 기법2, 3

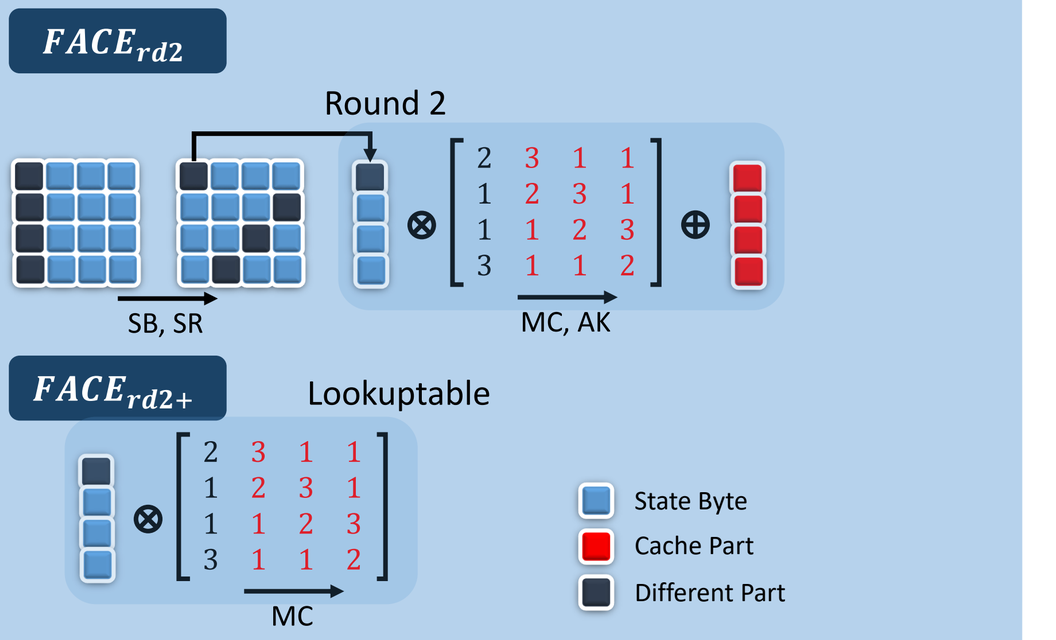

Fig. 3. FACE 기법4, 5

결 론

● 비트슬라이딩을 활용하여 알려진 기법 중 가장 작은 면적을 가지는 AES 구현
(Encryption, IBM130 : 1560 (2182) GE, Encryption/Decryption, IBM130 : 1738 (2402) GE)

● 캐시, 룩업테이블 기반의 FACE 기법을 적용하여 알려진 기법 중 가장 높은 처리율을 가지는 AES 구현
(Bitslice : 6.41 (7.59) cycle/byte, Intel Core 2 Q9550, AES-NI : 0.44 (0.55) cycles/byte, Intel Core i7, 8700K)