고급 소프트웨어 공학

Proposal

- 경량 AES 알고리즘(Light AES)에 대한 검증 -

KONKUK University

IT convergence security

신민용 smy11go@konkuk.ac.kr

안정현 aa9922@konkuk.ac.kr

목차

논문 주제

SPIN을 이용한 경량 AES 알고리즘에 대한 검증

- 경량 AES*(Light ASE) 알고리즘 – LAS

  - 보안성이 강화된 경량 AES 알고리즘

- Model Checker **SPIN**을 이용하여 기존 **AES**와 **LAS**의 **Avalanche Effect**을 비교하여 검증을 수행

*AES(Advanced Encryption Standard): 블록 암호 알고리즘

동기

SPIN을 이용한 경량 AES 알고리즘에 대한 검증

- 미디어 콘텐츠 등을 전송하는 스트리밍 서비스의 품질 저하를 최소화하고 미디어 콘텐츠를 안전하게 보호 할 수 있는 블록 암호 알고리즘이 필요
- 블록 암호 알고리즘 중, 안전하면서도 연산 과정이 단순화된 'AES' 알고리즘의 경량버전이 필요
- AES의 경량화는 주로 round의 축소로 이루어지지만 Related Key Attack 공격기법이 가능
  - Related Key Attack란 연관된 라운드 키의 일부를 가지고 평문과 암호문을 얻을 수 있는 조건이 성립한 상태에서 실시하는 이론적인 공격. 라운드가 축소된 AES를 해독하는 최상의 공격 기법
- 이에 Related Key Attack에 취약하지 않도록 라운드 동작횟수와 Key Schedule수를 수정하여 Avlanche Effect가 충분히 강한 경량화된 AES인 LAS를 검증

배경지식 (1)

AES(Advanced Encryption Standard)

- Rijndael 알고리즘, SPN(Substitution-Permutation Network) 구조를 사용

  - S-BOX, P-BOX를 이용하여 치환(Substitution)하고 섞는(Permutation) 과정으로 암· 복호화를 수행

- 128bit의 블록 암호 알고리즘

	블록 크기	비밀키 길이	라운드 횟수
AES-128	128bit	128bit	10 Round
AES-192	128bit	192bit	12 Round
AES-256	128bit	256bit	14 Round

배경지식 (2)

AES(Advanced Encryption Standard)

- State: 암·복호화 과정에서 생성되는 모든 128bit 데이터 블록

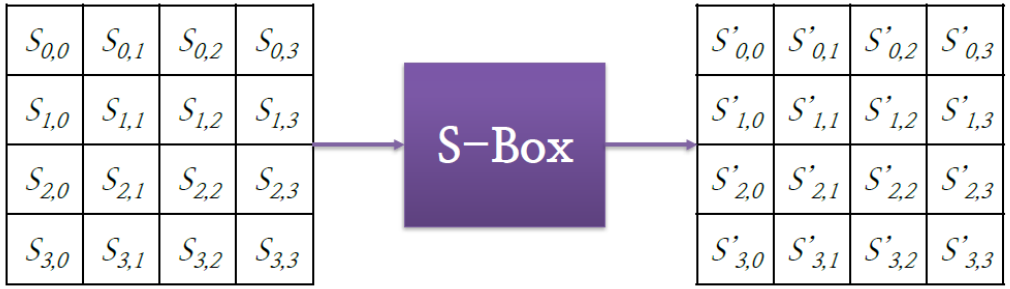
$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

함수명	기능	동작위치
AddRound	128bit State와 128bit 라운드 키를 이용하여 E-OR 연산을 수행하는 함수	라운드 내부
SubBytes	1byte값(0~255 중 어떤값)을 index로 S-Box로부터 1개의 값을 얻는 처리(치환)	
ShiftRows	SubBytes의 출력을 규칙에 따라 byte단위로 섞음	
MixColumns	4byte값을 비트연산을 통해 다른 4byte값으로 변환	
KeySchedules	각 round에서 생성되는 128bit round key 생성	라운드 외부

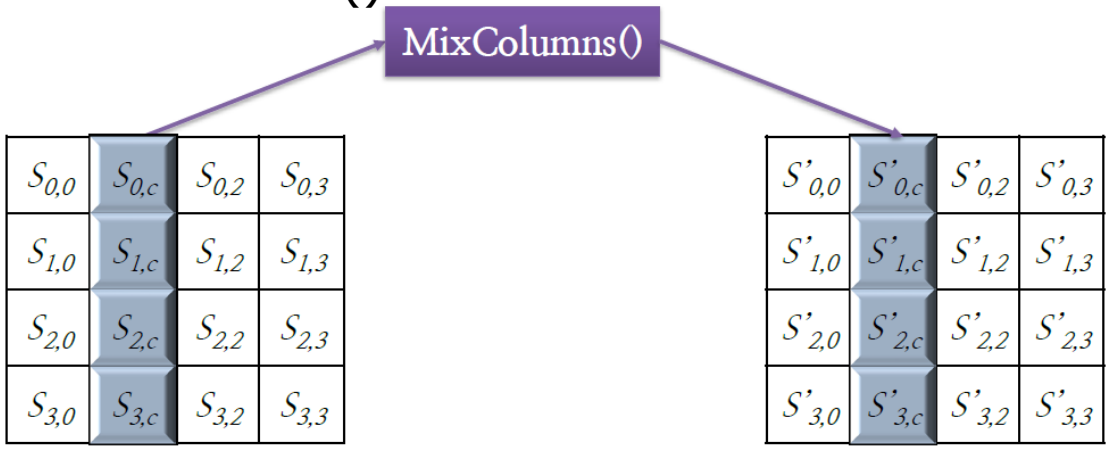
배경지식 (3)

AES(Advanced Encryption Standard)

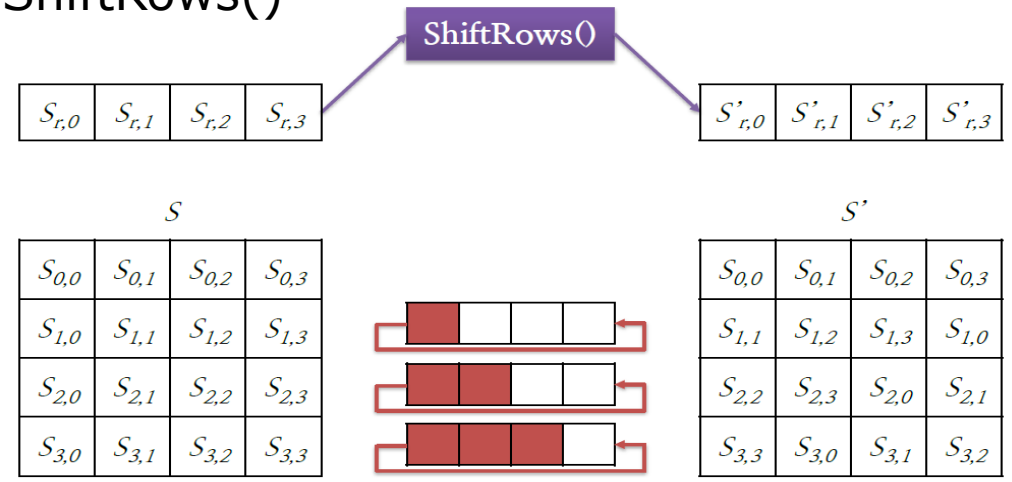
- SubBytes()



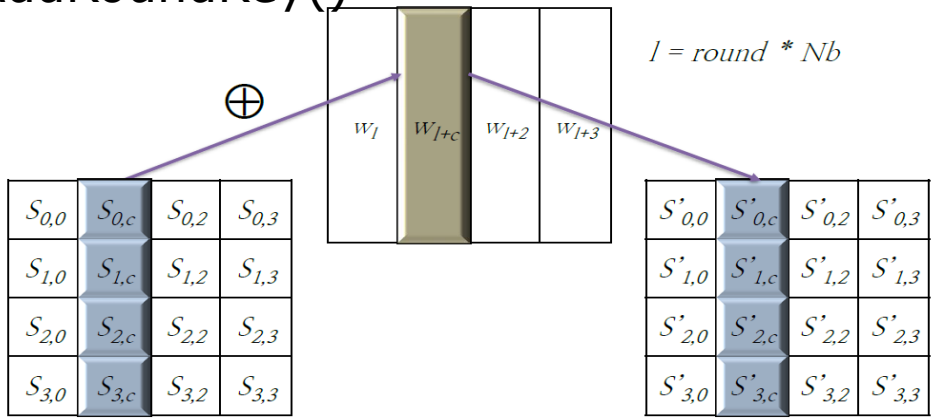
- MixColumns()



- ShiftRows()

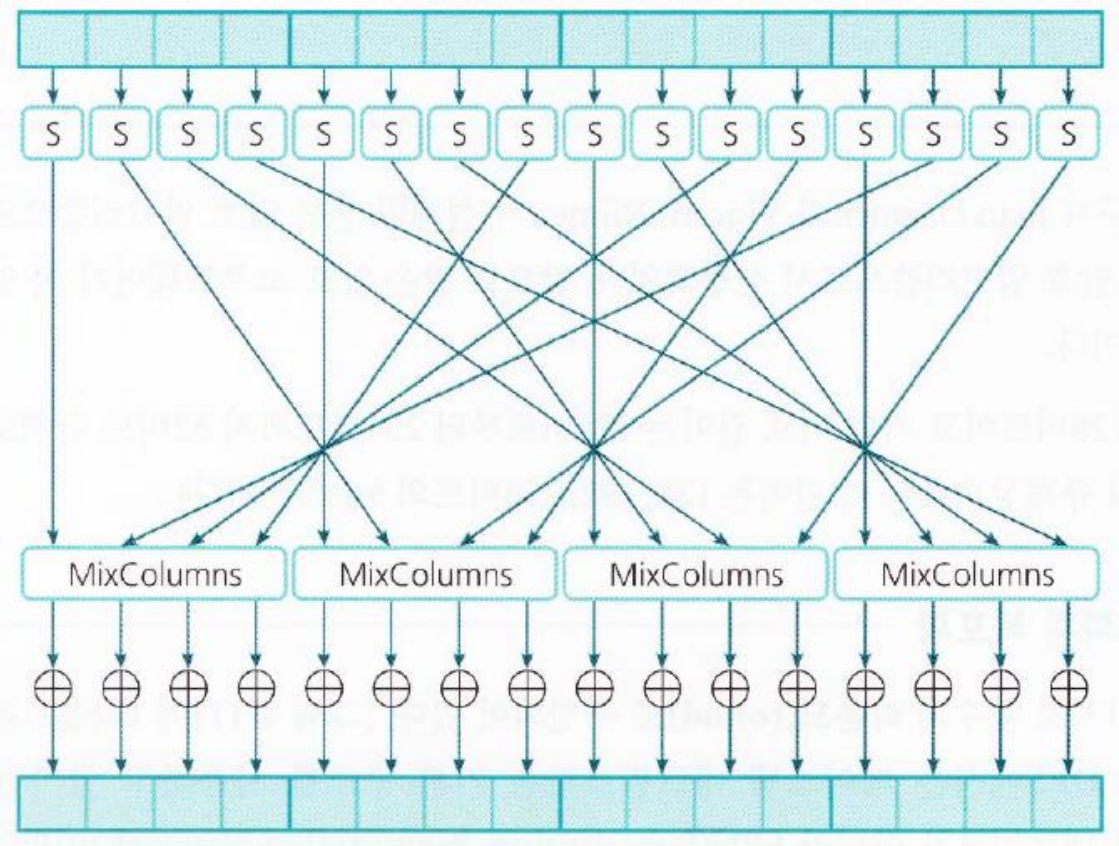


- AddRoundKey()



배경지식 (4)

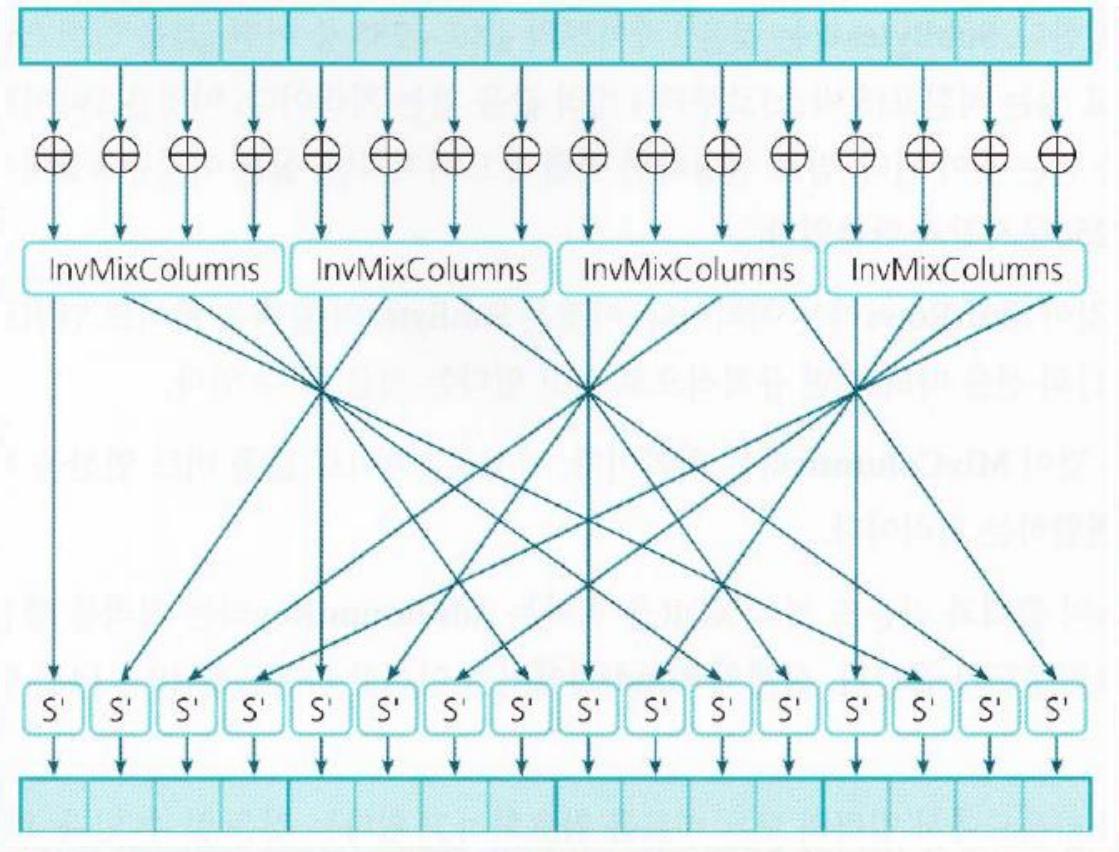
AES(Advanced Encryption Standard)



- 입력 및 출력 : 128bit = 16byte
- 암호화(Encryption) 과정
  - SubBytes(byte치환) →ShiftRows(행이동) → MixColumns(열이동) → AddRoundKey(round key와XOR)

배경지식 (5)

AES(Advanced Encryption Standard)



- 입력 및 출력 : 128bit = 16byte
- 복호화(Decryption) 과정
  - AddRoundKey(round key와XOR) → InvMixColumns(열역순이동) → InvShiftRows(행역순이동)→ InvSubBytes(byte 치환(역순))

배경지식 (6)

LAS(Lightweight AES) 알고리즘

- AES-256 기반의 경량 블록 암호 알고리즘, 경량 AES(Light ASE) 알고리즘

	블록 크기	비밀키 길이	라운드 횟수	KeySchedule 동작 횟수
LAS	128bit	256bit	14 Round → 7 Round	7번 → 8번

- AddRoundKey 함수 2개 = FirstAddRoundKey 함수 + SecondAddRoundKey 함수(라운드키 256bit)
  - •FirstAddRoundKey : 128bit State와 128bit 홀수 Column의 라운드 키를 E-OR 연산을 수행하는 함수
  - •SecondAddRoundKey : 128bit State와 128bit 짝수 Column의 라운드 키를 E-OR 연산을 수행하는 함수
- 암호화과정 : FirstAddRoundKey → SubBytes(byte치환) →ShiftRows(행이동) → MixColumns(열이동) → SecondAddRoundKey
- 복호화과정 : SecondAddRoundKey → InvMixColumns(열역순이동) → InvShiftRows(행역순이동)→ InvSubBytes(byte 치환(역순)) → FirstAddRoundKey

배경지식 (7)

LAS(Lightweight AES) 알고리즘

- 효과

1) 라운드 동작 횟수 축소 + KeySchedule함수 동작 횟수 확대
2) 기존과 비슷한 수준의 차분 확산 효과
3) 암·복호화 속도가 최대 53% 향상
4) 256bit 비밀키를 사용함으로써 Brute-Force Attack 보안
5) AES-256과 같은 수준의 Avalanche Effect를 가짐

검증 계획

SPIN을 이용한 경량 AES 알고리즘에 대한 검증

- LAS 알고리즘의 Avalanche Effect를 검증

  - Avalanche Effect:어떠한 알고리즘의 입력 값에 미세한 변화를 줄 경우 출력 값에 상당한 변화가 일어나는 성질

  - Avalanche Effect로 인해 키 또는 평문에서 생긴 변화의 크기가 암호문에서 나타나, 암호문을 통해 평문을 찾아낼 수 있는 확률이 높아져 알고리즘의 안전성이 떨어지는 문제가 발

  - 암호 알고리즘의 안전성을 위해서는 충분한 Avalanche Effect가 필요

- Model Checker **SPIN**을 이용하여 기존 **AES**와 **LAS**의 **Avalanche Effect**을 비교하여 검증을 수행

*AES(Advanced Encryption Standard): 블록 암호 알고리즘

검증 계획

SPIN을 이용한 경량 AES 알고리즘에 대한 검증

- ‘AES 및 LAS 알고리즘에 동일한 크기의 비밀키를 사용하여 검증하는 알고리즘’을 모델링

  1)구현된 AES와 LAS 알고리즘

  2)AES와 LAS 알고리즘의 Avalanche Effect를 검증하기 위해 동일한 크기의 비밀키를 입력하여 비교

검증 계획

SPIN을 이용한 경량 AES 알고리즘에 대한 검증

- Property
  - AES와 LAS의 입력값과 출력값이 반드시 128bit로 같아야 한다.
  - 똑같은 비밀키를 가져도 반드시 2번째 라운드부터는 State의 변화된 bit값들이 AES와 LAS가 같지 말아야 한다.
  - AES와 LAS의 Avalanche Effect의 편차가 특정 값 이상 차이나지 않는다.

참고 문헌

[1] NIST.FIPS.197 – Advanced Encryption Standard(AES)

[2] 김준태(2017), “스트리밍 서비스 보호를 위한 경량 블록 암호 알고리즘 연구”

Q & A

Thanks you!