PIPO 블록암호

유튜브 주소 : https://youtu.be/EJb-MsPWBOY

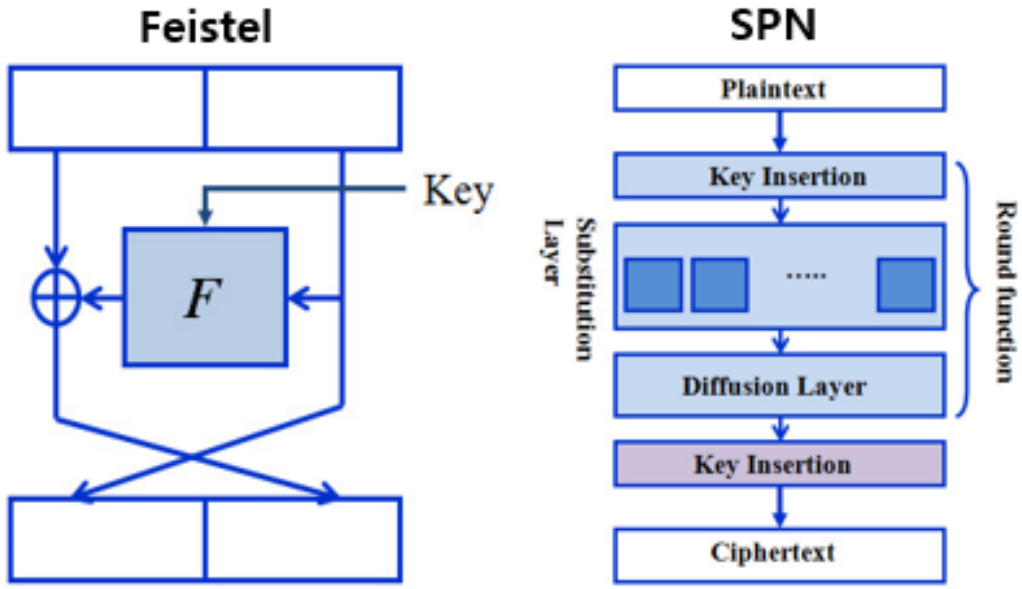
PIPO 개요

PIPO 알고리즘

구현 코드 분석

PIPO 개요

- PIPO : 국산 경량 블록암호(ISISC'20)
- PIPO-64/128, PIPO-64/256
- SPN((Substitution-Permutation Network) 구조 사용
  - Substitution(치환)과 permutation(전치)
  - Substitution된 S-box 출력을 p-box로 permutation하는 과정을 반복하는 구조



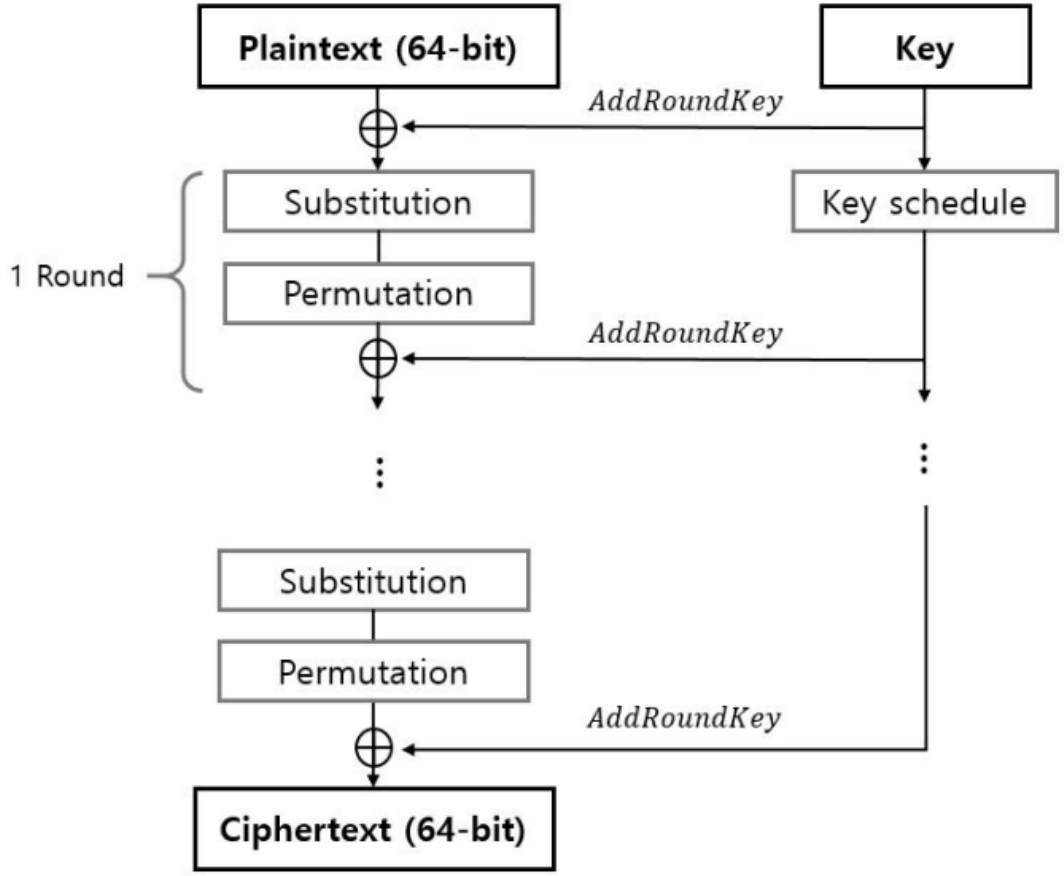
PIPO 개요

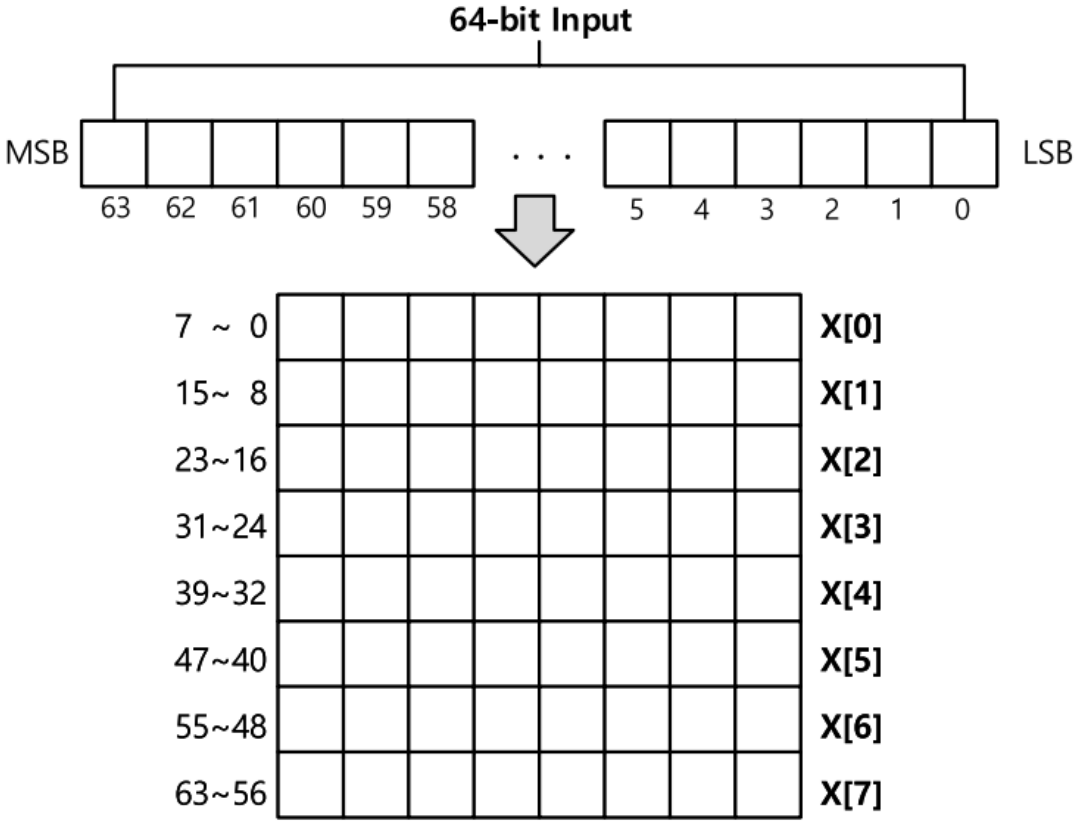
type	block size	key size	round
64/128	64 bit	128 bit	13
64/256	64 bit	256 bit	17

- 블록 길이 : 64bit
- 키 길이 : 128/256 bit
- 라운드 : 13/17
- 구현 방식 : TLU / bitslice
  - TLU – look up table 이용
  - Bitslice – 효율적인 s-box 연산 가능 -> 높은 성능으로 구현 가능

PIPO 알고리즘

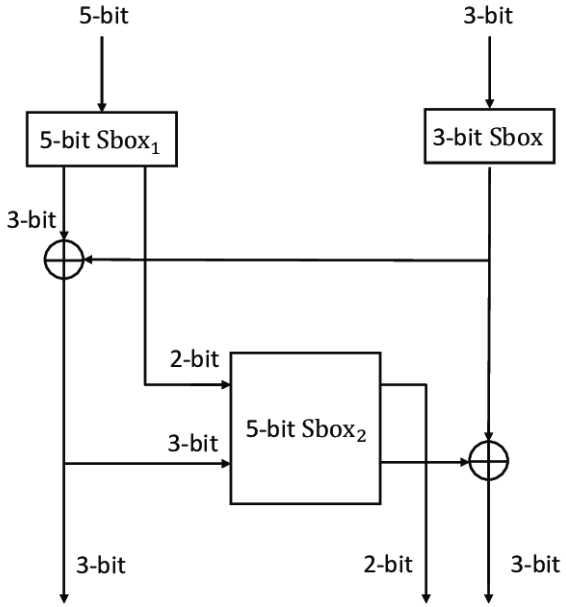
- PIPO 알고리즘 구조

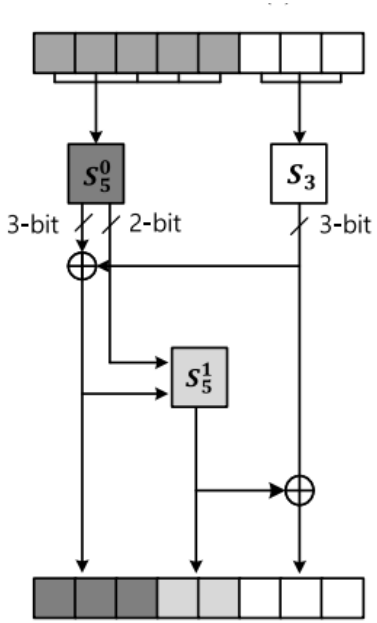




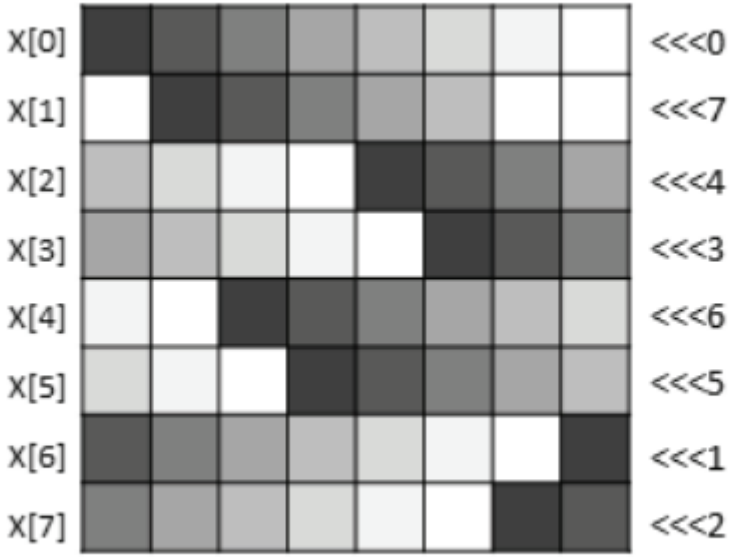
PIPO 알고리즘

- S-layer





R-layer



Q & A