# bcrypt

융합보안학과 윤세영

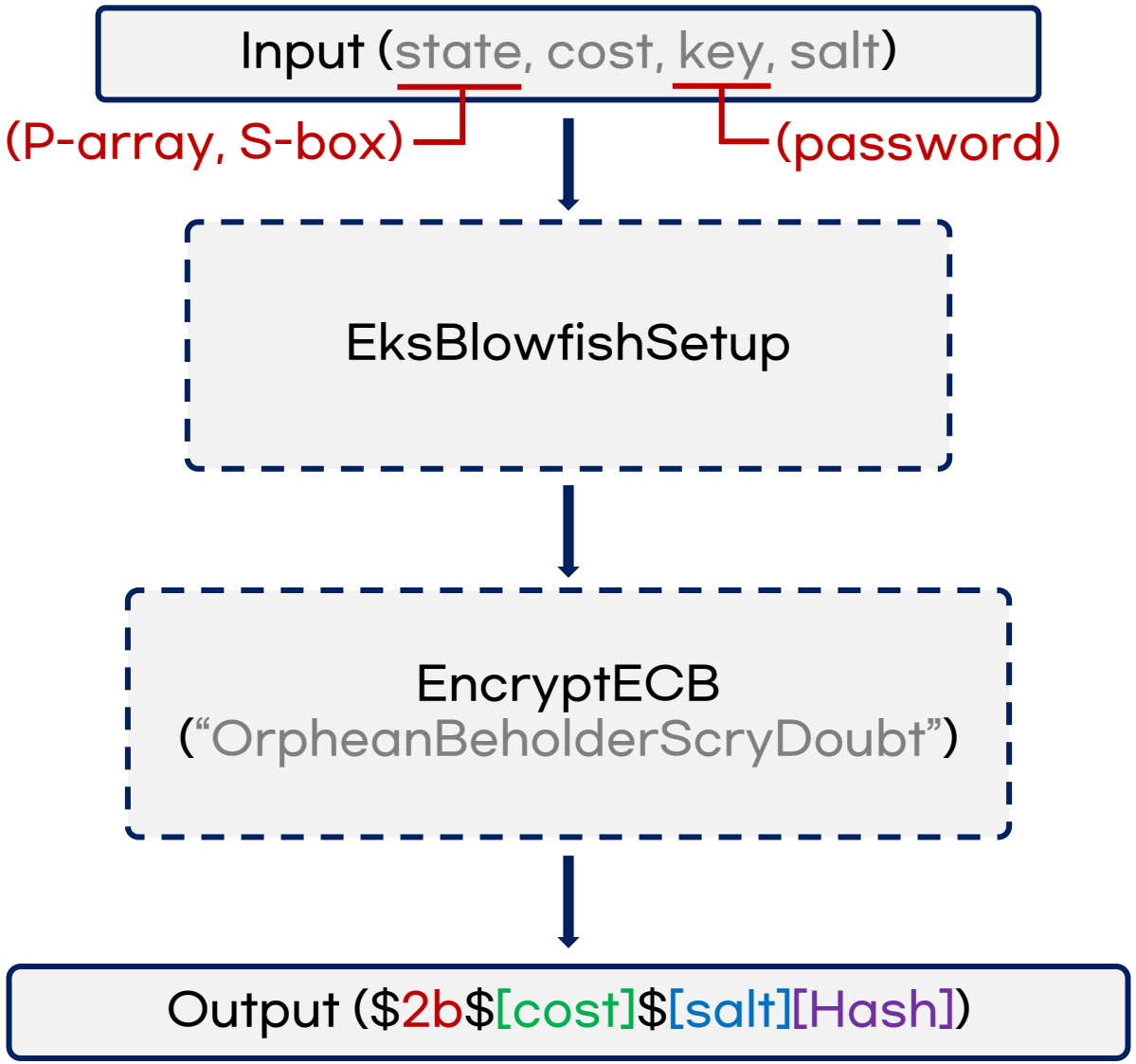
유투브 주소:
https://youtu.be/jUSMov0trVs

# bcrypt

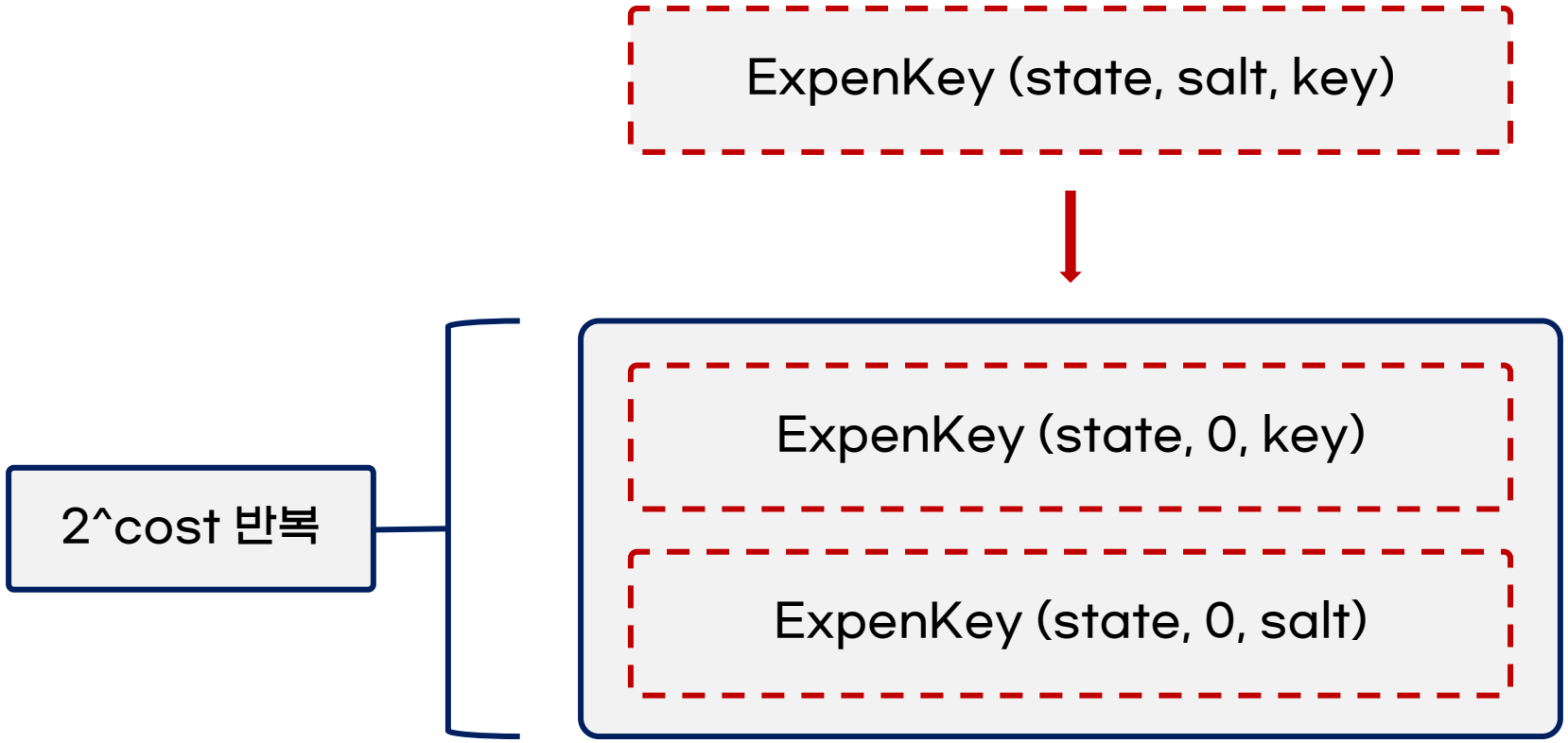
- 비밀번호 해시 함수: 비밀번호를 안전하게 저장하고 검증하기 위해 사용함
- 단방향 해시 함수: 입력값(비밀번호)을 해시값으로 변환하지만, 해시값에서 원래 값을 복원할 수 없음
- Salt 사용: 해시를 생성할 때 무작위로 생성된 값(Salt)을 추가해 동일한 비밀번호라도 다른 해시값이 생성됨
- Cost 사용: 연산 복잡도를 조절할 수 있어, 해시 생성이 느려지도록 할 수 있음 (보안 강화)

- 비밀번호 입력 -> Salt 생성 -> 비밀번호, Salt, Cost 를 사용하여 해시값 생성
- (생성된 해시값을) 데이터베이스에 저장 -> 로그인 시 기존 해시값과 비교하는 방식으로 사용

# bcrypt algorithm



# EksBlowfishSetup



# ExpenKey

1. key XOR P-array

```
"P_array": [
    0x243f6a88, 0x85a308d3, 0x13198a2e, 0x03707344,
    0xa4093822, 0x299f31d0, 0x082efa98, 0xec4e6c89,
    0x452821e6, 0x38d01377, 0xbe5466cf, 0x34e90c6c,
    0xc0ac29b7, 0xc97c50dd, 0x3f84d5b5, 0xb5470917,
    0x9216d5d9, 0x8979fb1b
],
```

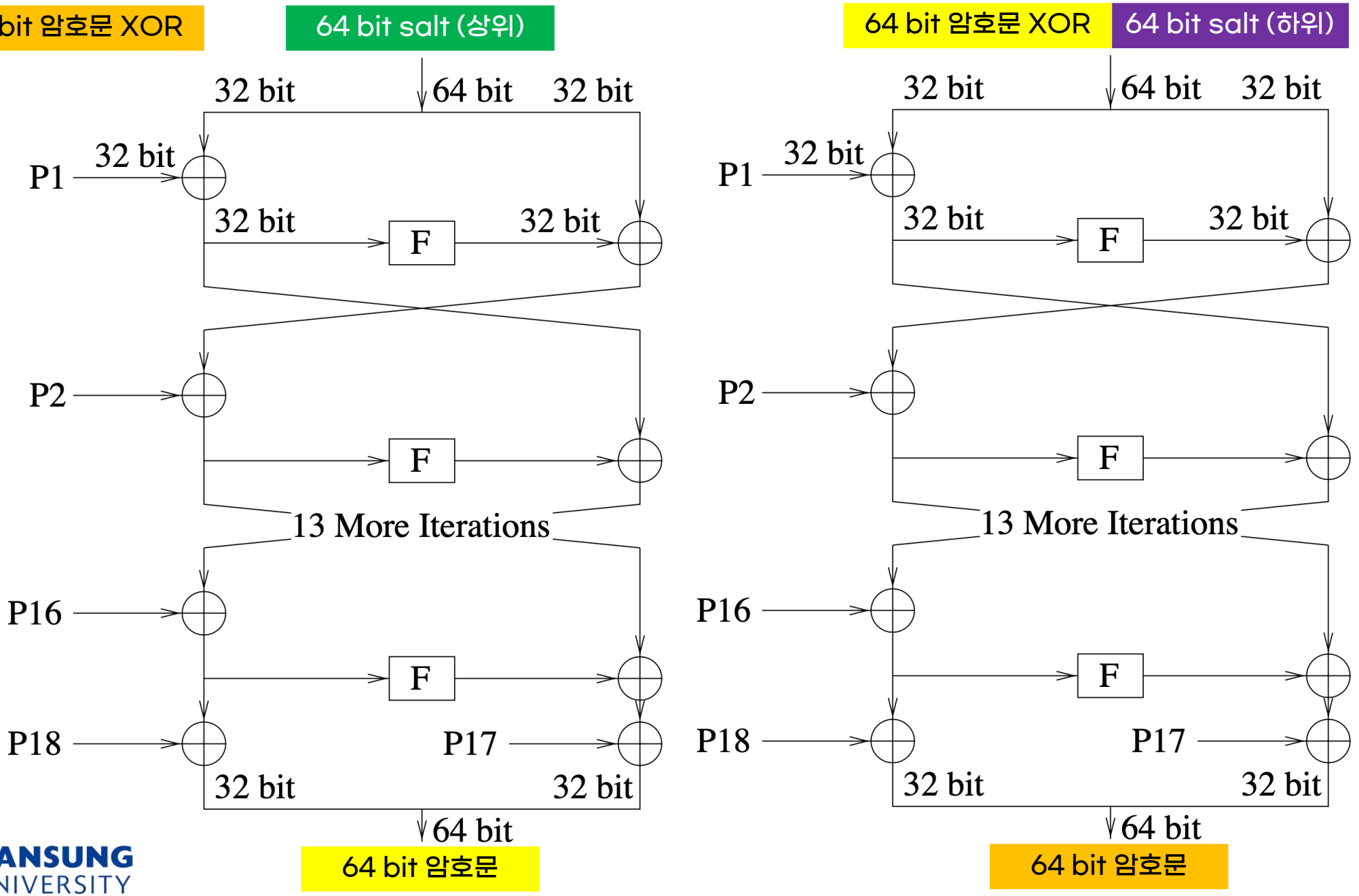
abcd / efab / cdef / abcd / efab / cdef ···

2. Blowfish (salt, P-array, S-box)

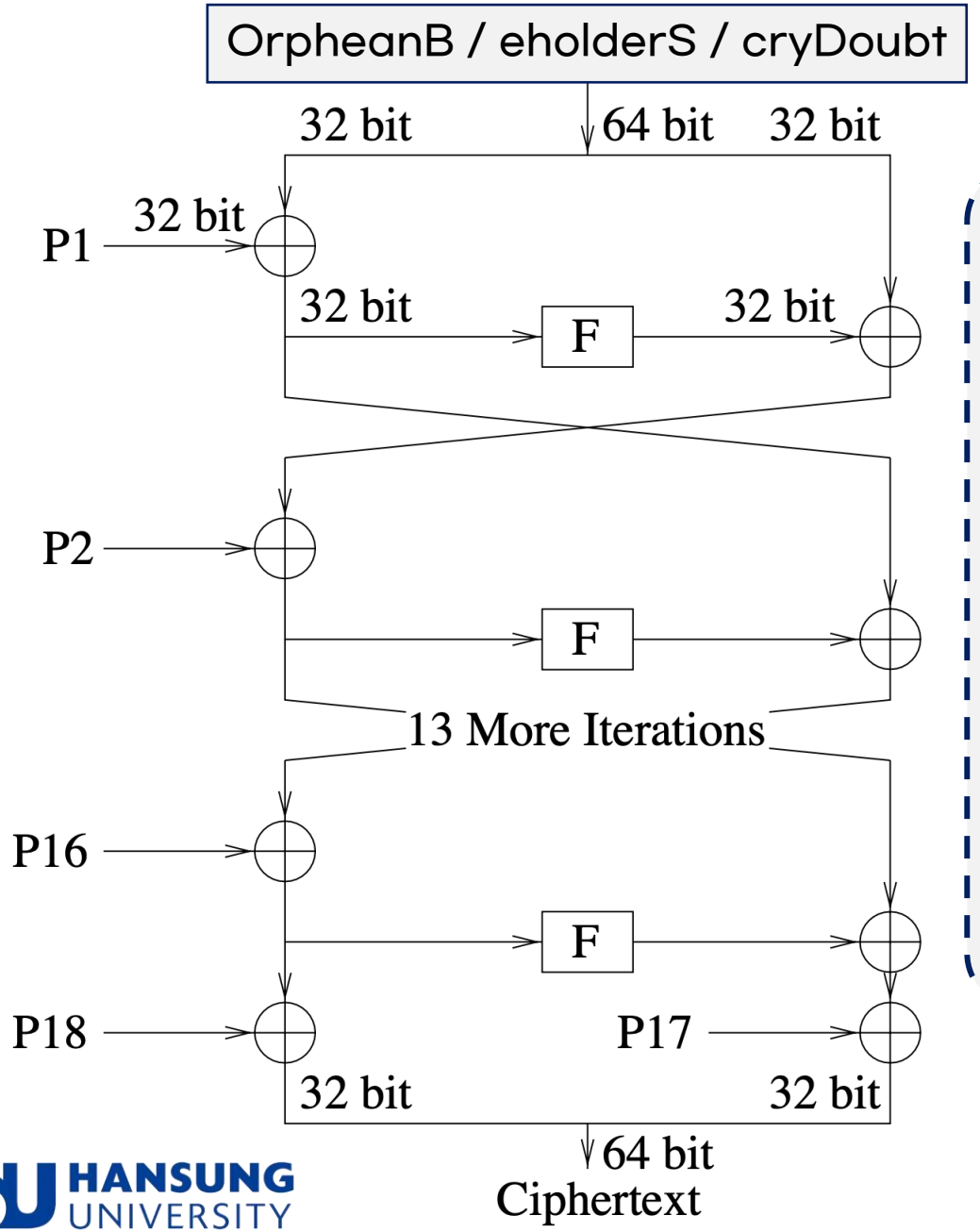
```
"P_array": [
    0x243f6a88, 0x85a308d3, 0x13198a2e, 0x03707344,
    0xa4093822, 0x299f31d0, 0x082efa98, 0xec4e6c89,
    0x452821e6, 0x38d01377, 0xbe5466cf, 0x34e90c6c,
    0xc0ac29b7, 0xc97c50dd, 0x3f84d5b5, 0xb5470917,
    0x9216d5d9, 0x8979fb1b
],
```

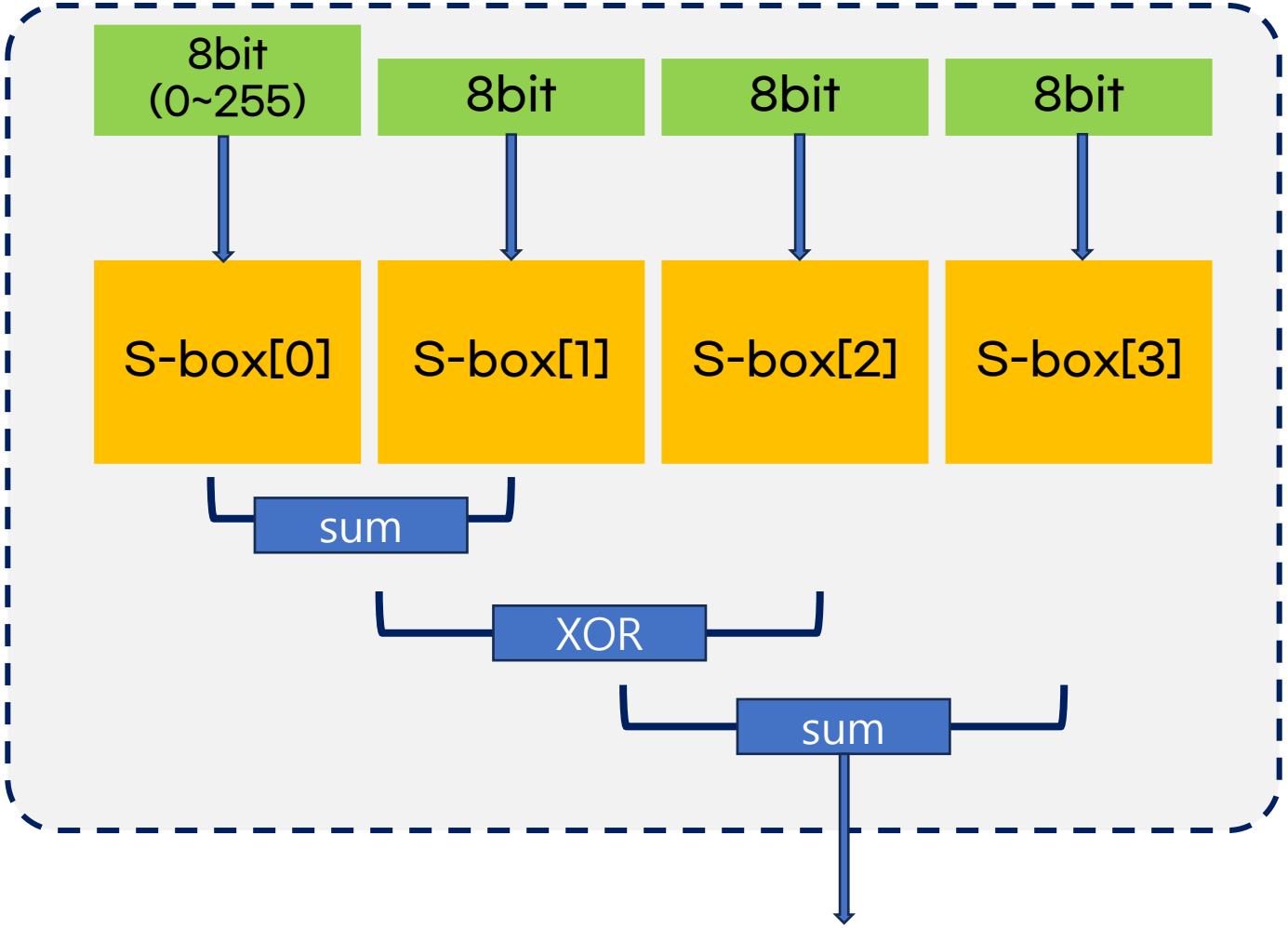
```
"S_box": [
    [
        0xd1310ba6, 0x98dfb5ac, 0x2ffd72db, 0xd01adfb7,
        0xb8e1afed, 0x6a267e96, 0xba7c9045, 0xf12c7f99,
        0x24a19947, 0xb3916cf7, 0x0801f2e2, 0x858efc16,
        0x636920d8, 0x71574e69, 0xa458fea3, 0xf4933d7e,
        0x0d95748f, 0x728eb658, 0x718bcd58, 0x82154aee,
```

# Blowfish (salt, P-array, S-box)



# Blowfish (EncryptECB)



# 감사합니다