Cryptanalysis
(암호분석)

Chapter 7 – Part 1

2020.6

Contents

- Differential probability
- Differential Cryptanalysis (DC)
- Variants of DC

차분(difference)

- XOR(Exclusive OR) 연산
  - 비트 단위의 XOR 연산
    $\mathrm{XOR}: \{0,1\} \times \{0,1\} \to \{0,1\}$
  - n비트 단위의 XOR 연산
    $\mathrm{XOR}: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$

입력		출력
x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

- 차분: 주어진 $x, y \in \{0,1\}^n$ 에 대하여 $x \oplus y$를 x, y의 **차분(difference)**이라 한다.

- 예제:
  - $x = 1101, y = 1011 \rightarrow x \oplus y = 0110$
  - $x = 1001, y = 1111 \rightarrow x \oplus y = 0110$

x, y의
차분

선형 함수의 차분 전파

- 선형 함수와 차분 특성
  - 선형 함수 $f\colon \{0,1\}^n \to \{0,1\}^m$는 모든 x, y에 대하여
    $$f(x \oplus y) = f(x) \oplus f(y).$$
  - 동일한 입력차분에 대한 출력차분은 항상 같다(일정하다).
    입력차분 $x \oplus y = \alpha$ 인 모든 x, y에 대하여
    출력차분 $f(x) \oplus f(y) = \beta$는 항상 일정하다.
  - 이를 간단히 표기하면, **차분특성 $\boldsymbol{f}\colon \boldsymbol{\alpha} \to \boldsymbol{\beta}$ (확률 1)**

- 예: $\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_0 \oplus x_2 \oplus x_3 \\ x_0 \oplus x_1 \oplus x_3 \\ x_0 \oplus x_1 \oplus x_2 \end{pmatrix}$ 차분특성 $\boldsymbol{f}\colon 0110 \to 0110$ **(확률 1)**

  - $x = 1101,\ y = 1011 : x \oplus y = 0110 = \alpha$
    $$f(x) \oplus f(y) = 0010 \oplus 0100 = 0110 = \beta$$
  - $x = 1001,\ y = 1111 : x \oplus y = 0110 = \alpha$
    $$f(x) \oplus f(y) = 1001 \oplus 1111 = 0110 = \beta$$

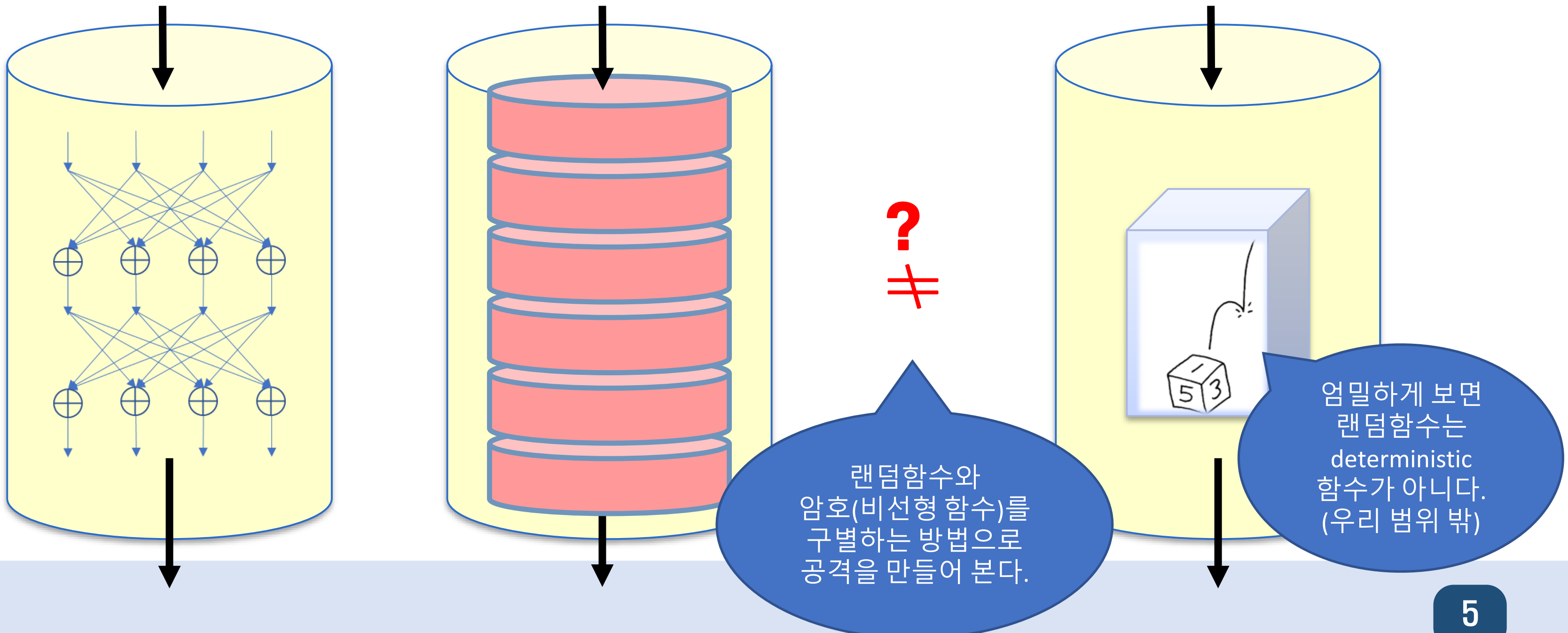
비선형 함수의 차분 전파

- 비선형 함수와 특징
  - 비선형 함수 $f: \{0,1\}^n \to \{0,1\}^m$는 모든 x, y 에 대하여
    $f(x \oplus y) = f(x) \oplus f(y)$ 을 보장할 수 없다.
  - 동일한 입력차분에 대하여 출력차분은 일정하지 않다.
    입력차분 $x \oplus y = \alpha$ 인 x, y에 따라
    출력차분 $f(x) \oplus f(y) = \beta$는 달라진다.

- 비선형 함수의 차분 전파 특성
  - 입력차분 $x \oplus y = \alpha$ 에 대응하는 출력차분이 $f(x) \oplus f(y) = \beta$는 확률적으로 성립한다.
  - 이를 간단히 표기하면, **차분특성 $f: \alpha \to \beta$ (확률 p)**
  - 확률 p가 큰 α, β 를 얻으면
    차분특성 $f: \alpha \to \beta$이 선형 함수와 비슷해진다.

차분 전파 특성의 비교

- 입력 차분이 $x \oplus y = \alpha$ 인 경우 출력차분 $f(x) \oplus f(y) = \beta$은?
  - 선형 함수: 항상 일정한 출력차분
  - 비선형 함수: 특정한 출력차분 β 가 얻어질 확률이 존재
  - 랜덤 함수: 특정한 출력차분 β가 될 확률은 2^{-n} (n비트 출력)



차분 특성의 계산

- 부울함수 $S: \{0,1\}^n \rightarrow \{0,1\}^m$
  - 입력차분이 α인 모든 입력 x, y를 모두 찾으면?
    $\{(x, y) |\ x \oplus y\ = \alpha, x, y \in \{0,1\}^n\}\ = \{(x, x \oplus \alpha) |\ x \in \{0,1\}^n\}$
  - 입력차분이 α인 입력 x, y 는 모두 몇 쌍인가? 2^n

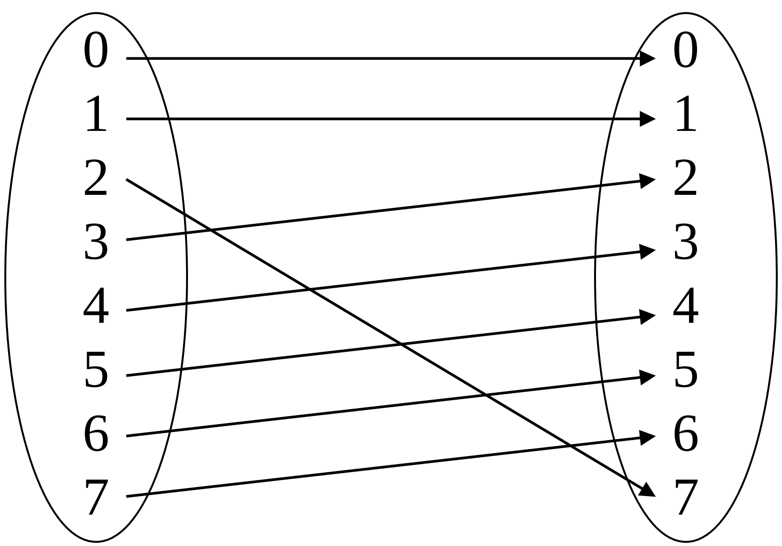
- 주어진 입력차분에 대한 출력차분 계산
  - 입력차분이 α인 모든 입력 x, y 쌍에 대하여 출력차분이 β 가 되는 쌍의 개수는?
    $\delta(\alpha, \beta) =\ \#\{x |\ S(x) \oplus S(x \oplus \alpha) = \beta\}$. (#: 원소의 개수)
  - 입력차분이 α 일 때, 출력차분이 β 일 확률은?

$$\mathrm{P}[\alpha \rightarrow \beta] = DP(\alpha, \beta) = \frac{\delta(\alpha, \beta)}{2^n}$$

예제1: 3비트 부울 함수 S

- S: 3비트 입출력의 부울 함수(Boolean function)

$S: \{0,1\}^3 \rightarrow \{0,1\}^3$



테이블 표현 | 0 1 7 2 3 4 5 6

S[0] = 0
S[1] = 1
S[2] = 7
S[3] = 2
S[4] = 3
S[5] = 4
S[6] = 5
S[7] = 6

3비트 Sbox로 생각할 수 있다.

예제1: 3비트 부울 함수 S

- 입력차분 α, 출력차분 β에 대하여 $\delta(\alpha,\beta)$를 구하면?
  - 예: $\delta(0,0) = 8$ (입력차분 $\alpha = 0$ 의 의미: 같은 입력)
  - 예: $\delta(1,1) = 2$
  - 예: $\delta(1,2) = 0$ (입력차분 $\alpha = 1$인 경우 출력차분 $\beta \neq 2$)
- S의 차분분포표

출력차분 β

입력차분 α

	0	1	2	3	4	5	6	7
0	8	0	0	0	0	0	0	0
1	0	2	0	2	0	2	0	2
2	0	0	2	2	0	0	2	2
3	0	2	2	0	0	2	2	0
4	0	0	2	2	2	2	0	0
5	0	2	2	0	2	0	0	2
6	0	0	0	0	2	2	2	2
7	0	2	0	2	2	0	2	0

최대차분확률은?

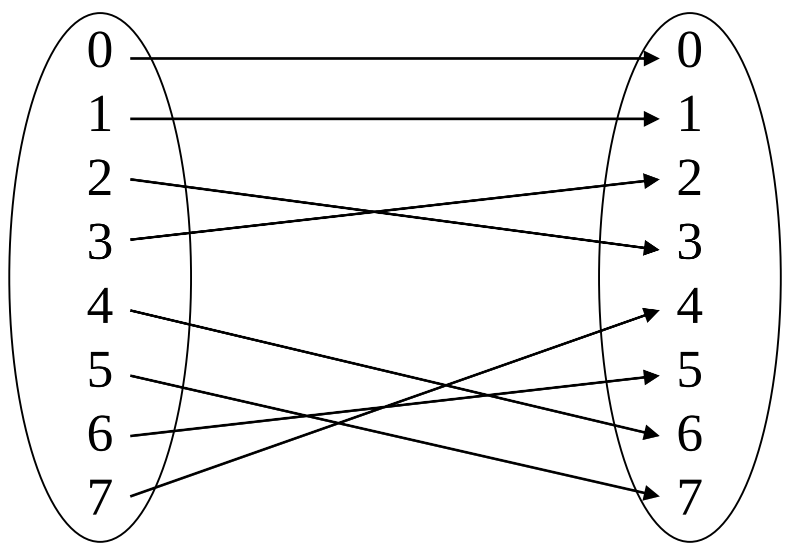
$$\mathrm{P}[\alpha \to \beta] = DP(\alpha,\beta) = \frac{\delta(\alpha,\beta)}{2^n} = \frac{2}{8}$$

최대차분확률이 되는 경우가 다수 존재한다.
$\alpha = 1, \beta = 1$
$\alpha = 3, \beta = 1$
…

예제2: 3비트 부울 함수 T

- T: 3비트 입출력의 부울 함수(Boolean function)

$T: \{0,1\}^3 \rightarrow \{0,1\}^3$



테이블 표현 | 0 1 3 2 6 7 5 4

T[0] = 0
T[1] = 1
T[2] = 3
T[3] = 2
T[4] = 6
T[5] = 7
T[6] = 5
T[7] = 4

예제2: 3비트 부울 함수 T

▶ T의 차분분포표

출력차분
β

입력차분 α 에
대한 출력차분
β 는 1가지
경우뿐이다.

입력차분
α

	0	1	2	3	4	5	6	7
0	8	0	0	0	0	0	0	0
1	0	8	0	0	0	0	0	0
2	0	0	0	8	0	0	0	0
3	0	0	8	0	0	0	0	0
4	0	0	0	0	0	0	8	0
5	0	0	0	0	0	0	0	8
6	0	0	0	0	0	8	0	0
7	0	0	0	0	8	0	0	0

S[0] = 0
S[1] = 1
S[2] = 7
S[3] = 2
S[4] = 3
S[5] = 4
S[6] = 5
S[7] = 6

T[0] = 0
T[1] = 1
T[2] = 3
T[3] = 2
T[4] = 6
T[5] = 7
T[6] = 5
T[7] = 4

최대차분확률은?

$$\mathrm{P}[\alpha \rightarrow \beta] = DP(\alpha,\beta) = \frac{\delta(\alpha,\beta)}{2^n} = \frac{8}{8}$$

두 함수의
근본적인 차이는
무엇인가?

차분분포표 만들기

```python
import random

# 테이블 초기화
DTable = []
for i in range(len(S)):
    DTable.append( [ 0 for j in range(len(S))])

# 입출력 차분표
for x1 in range(len(S)):
    y1 = S[x1]
    for dx in range(len(S)):
        x2 = x1 ^ dx
        y2 = S[x2]
        dy = y1 ^ y2
        DTable[dx][dy] += 1

# 차분분포표 출력
print('    ', end='')
for i in range(len(S)):
    print('%3d ' %(i), end='')
print('\n')
for dx in range(len(S)):
    print('%3d ' %(dx), end='')
    for dy in range(len(S)):
        print('%3d ' %(DTable[dx][dy]), end='')
    print('\n')
```

```python
#== 부울 함수(Boolean function) 정의 ===
S = [ 0, 1, 7, 2, 3, 4, 5, 6]

# 함수값 확인
for i  in range(len(S)):
    print('S[%d] = %d' %(i, S[i]))
```

AES의 Sbox

- AES에 사용된 8비트 Sbox

```
S = [   0x63, 0x7C, 0x77, 0x7B, 0xF2, 0x6B, 0x6F, 0xC5, 0x30, 0x01, 0x67, 0x2B, 0xFE, 0xD7, 0xAB, 0x76,
        0xCA, 0x82, 0xC9, 0x7D, 0xFA, 0x59, 0x47, 0xF0, 0xAD, 0xD4, 0xA2, 0xAF, 0x9C, 0xA4, 0x72, 0xC0,
        0xB7, 0xFD, 0x93, 0x26, 0x36, 0x3F, 0xF7, 0xCC, 0x34, 0xA5, 0xE5, 0xF1, 0x71, 0xD8, 0x31, 0x15,
        0x04, 0xC7, 0x23, 0xC3, 0x18, 0x96, 0x05, 0x9A, 0x07, 0x12, 0x80, 0xE2, 0xEB, 0x27, 0xB2, 0x75,
        0x09, 0x83, 0x2C, 0x1A, 0x1B, 0x6E, 0x5A, 0xA0, 0x52, 0x3B, 0xD6, 0xB3, 0x29, 0xE3, 0x2F, 0x84,
        0x53, 0xD1, 0x00, 0xED, 0x20, 0xFC, 0xB1, 0x5B, 0x6A, 0xCB, 0xBE, 0x39, 0x4A, 0x4C, 0x58, 0xCF,
        0xD0, 0xEF, 0xAA, 0xFB, 0x43, 0x4D, 0x33, 0x85, 0x45, 0xF9, 0x02, 0x7F, 0x50, 0x3C, 0x9F, 0xA8,
        0x51, 0xA3, 0x40, 0x8F, 0x92, 0x9D, 0x38, 0xF5, 0xBC, 0xB6, 0xDA, 0x21, 0x10, 0xFF, 0xF3, 0xD2,
        0xCD, 0x0C, 0x13, 0xEC, 0x5F, 0x97, 0x44, 0x17, 0xC4, 0xA7, 0x7E, 0x3D, 0x64, 0x5D, 0x19, 0x73,
        0x60, 0x81, 0x4F, 0xDC, 0x22, 0x2A, 0x90, 0x88, 0x46, 0xEE, 0xB8, 0x14, 0xDE, 0x5E, 0x0B, 0xDB,
        0xE0, 0x32, 0x3A, 0x0A, 0x49, 0x06, 0x24, 0x5C, 0xC2, 0xD3, 0xAC, 0x62, 0x91, 0x95, 0xE4, 0x79,
        0xE7, 0xC8, 0x37, 0x6D, 0x8D, 0xD5, 0x4E, 0xA9, 0x6C, 0x56, 0xF4, 0xEA, 0x65, 0x7A, 0xAE, 0x08,
        0xBA, 0x78, 0x25, 0x2E, 0x1C, 0xA6, 0xB4, 0xC6, 0xE8, 0xDD, 0x74, 0x1F, 0x4B, 0xBD, 0x8B, 0x8A,
        0x70, 0x3E, 0xB5, 0x66, 0x48, 0x03, 0xF6, 0x0E, 0x61, 0x35, 0x57, 0xB9, 0x86, 0xC1, 0x1D, 0x9E,
        0xE1, 0xF8, 0x98, 0x11, 0x69, 0xD9, 0x8E, 0x94, 0x9B, 0x1E, 0x87, 0xE9, 0xCE, 0x55, 0x28, 0xDF,
        0x8C, 0xA1, 0x89, 0x0D, 0xBF, 0xE6, 0x42, 0x68, 0x41, 0x99, 0x2D, 0x0F, 0xB0, 0x54, 0xBB, 0x16
        ]
```

AES Sbox의 차분분포표

	0	1	2	3	4	5	6	7	8 ⋯
0	256	0	0	0	0	0	0	0	0
1	0	2	0	0	2	0	2	0	2
2	0	0	0	2	2	2	2	2	0
3	0	0	2	0	2	2	0	0	2
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	2	0	0	0	4
6	0	2	0	0	2	2	0	0	0
255	0	2	2	2	0	0	0	2	0

$\delta(\alpha, \beta)$ 의 최댓값 =4

차분분포표 일부 생략

최대차분확률은?

$$\mathrm{P}[\alpha \to \beta] = DP(\alpha, \beta) = \frac{\delta(\alpha, \beta)}{2^n} = \frac{4}{256} = 2^{-6}$$

Bad Sbox

- 안전하지 않은 8비트 Bad Sbox 예제

```
BSbox = [ 0x06,0x97,0x13,0xa1,0xa5,0xb1,0x92,0xb6,0x25,0x27,0xb3,0x00,0x15,0x05,0xb4,0x82,
          0x84,0x32,0xa6,0x87,0x26,0x22,0x86,0xb5,0x33,0x23,0x20,0x03,0x02,0x36,0x24,0x30,
          0x90,0x11,0x01,0x34,0x80,0x96,0x17,0x91,0xa2,0x35,0xa4,0xa0,0x31,0xa3,0xb0,0x95,
          0x21,0x07,0x81,0xb7,0x83,0x12,0x14,0x85,0xb2,0xa7,0x10,0x04,0x94,0x37,0x93,0x16,
          0x4e,0xdf,0x5b,0xe9,0xed,0xf9,0xda,0xfe,0x6d,0x6f,0xfb,0x48,0x5d,0x4d,0xfc,0xca,
          0xcc,0x7a,0xee,0xcf,0x6e,0x6a,0xce,0xfd,0x7b,0x6b,0x68,0x4b,0x4a,0x7e,0x6c,0x78,
          0xd8,0x59,0x49,0x7c,0xc8,0xde,0x5f,0xd9,0xea,0x7d,0xec,0xe8,0x79,0xeb,0xf8,0xdd,
          0x69,0x4f,0xc9,0xff,0xcb,0x5a,0x5c,0xcd,0xfa,0xef,0x58,0x4c,0xdc,0x7f,0xdb,0x5e,
          0x0e,0x9f,0x1b,0xa9,0xad,0xb9,0x9a,0xbe,0x2d,0x2f,0xbb,0x08,0x1d,0x0d,0xbc,0x8a,
          0x8c,0x3a,0xae,0x8f,0x2e,0x2a,0x8e,0xbd,0x3b,0x2b,0x28,0x0b,0x0a,0x3e,0x2c,0x38,
          0x98,0x19,0x09,0x3c,0x88,0x9e,0x1f,0x99,0xaa,0x3d,0xac,0xa8,0x39,0xab,0xb8,0x9d,
          0x29,0x0f,0x89,0xbf,0x8b,0x1a,0x1c,0x8d,0xba,0xaf,0x18,0x0c,0x9c,0x3f,0x9b,0x1e,
          0x46,0xd7,0x53,0xe1,0xe5,0xf1,0xd2,0xf6,0x65,0x67,0xf3,0x40,0x55,0x45,0xf4,0xc2,
          0xc4,0x72,0xe6,0xc7,0x66,0x62,0xc6,0xf5,0x73,0x63,0x60,0x43,0x42,0x76,0x64,0x70,
          0xd0,0x51,0x41,0x74,0xc0,0xd6,0x57,0xd1,0xe2,0x75,0xe4,0xe0,0x71,0xe3,0xf0,0xd5,
          0x61,0x47,0xc1,0xf7,0xc3,0x52,0x54,0xc5,0xf2,0xe7,0x50,0x44,0xd4,0x77,0xd3,0x56 ]
```

Bad Sbox의 차분분포표

	0	1	2	3	4	5	6	7	8	9
0	256	0	0	0	0	0	0	0	0	0
1	0	0	8	0	16	0	0	0	0	0
2	0	0	0	0	0	0	16	24	0	0
3	0	0	8	16	0	0	16	0	0	0
4	0	0	0	0	8	0	0	8	0	0
5	0	16	0	0	16	8	16	0	0	0
128	0	0	0	0	0	0	0	0	256	0
255	0	0	8	0	0	0	0	0	0	0

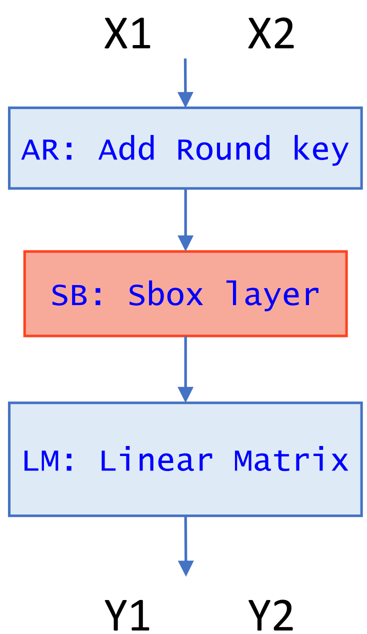
$\delta(\alpha,\beta)$ 의
최댓값 = 256

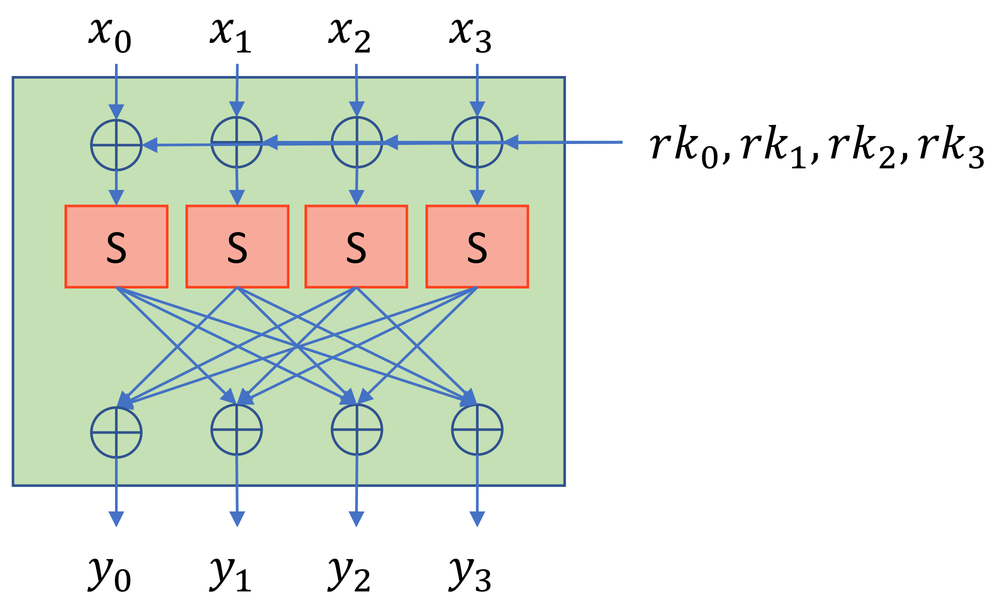
최대차분확률은?

$$\mathrm{P}[\alpha \rightarrow \beta] = DP(\alpha,\beta) = \frac{\delta(\alpha,\beta)}{2^n} = \frac{256}{256} = 1$$

TC20 라운드 함수의 차분

- 라운드 함수의 입력 X1, X2의 차분이 X1 xor X2 = dx일 때
  - AR(Add Round Key) 단계에서는 차분의 변화가 없다.
  - Sbox를 통과하면서 입력차분에 대한 출력차분 확률이 적용된다.
  - 선형함수 LM에서는 확률 1로 결과의 차분을 알 수 있다.

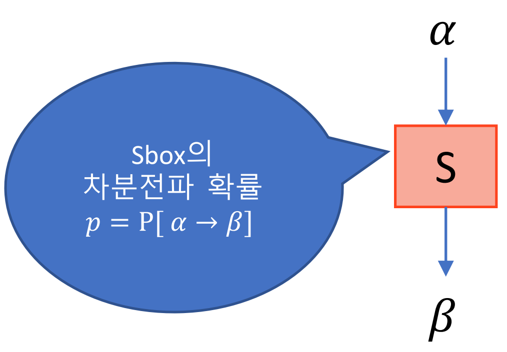


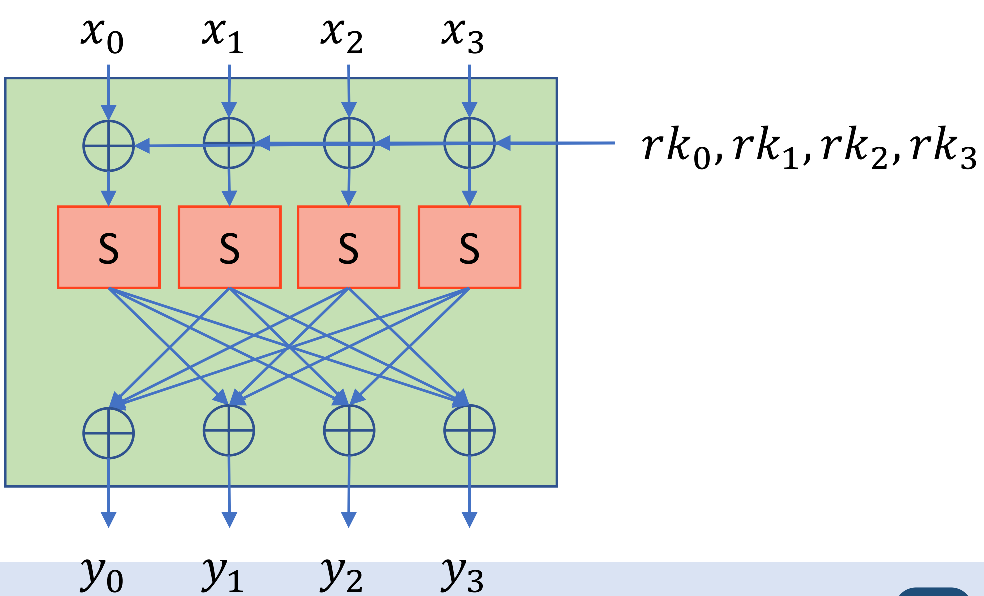


예: TC20 라운드 함수의 차분

- 라운드 함수의 입력: $X1 \oplus X2 = [\alpha, 0, 0, 0]$
  - AR(Add Round Key) 직후 차분: $[\alpha, 0, 0, 0]$
  - Sbox를 통과 후 차분: $[\beta, 0, 0, 0]$
  - 선형함수 LM 후: $[0, \beta, \beta, \beta]$

라운드 차분특성 $[\boldsymbol{\alpha}, \mathbf{0}, \mathbf{0}, \mathbf{0}]$ → $[\mathbf{0}, \boldsymbol{\beta}, \boldsymbol{\beta}, \boldsymbol{\beta}]$ (확률 $\boldsymbol{p}$)

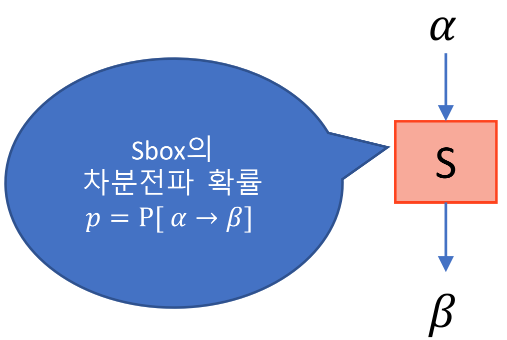


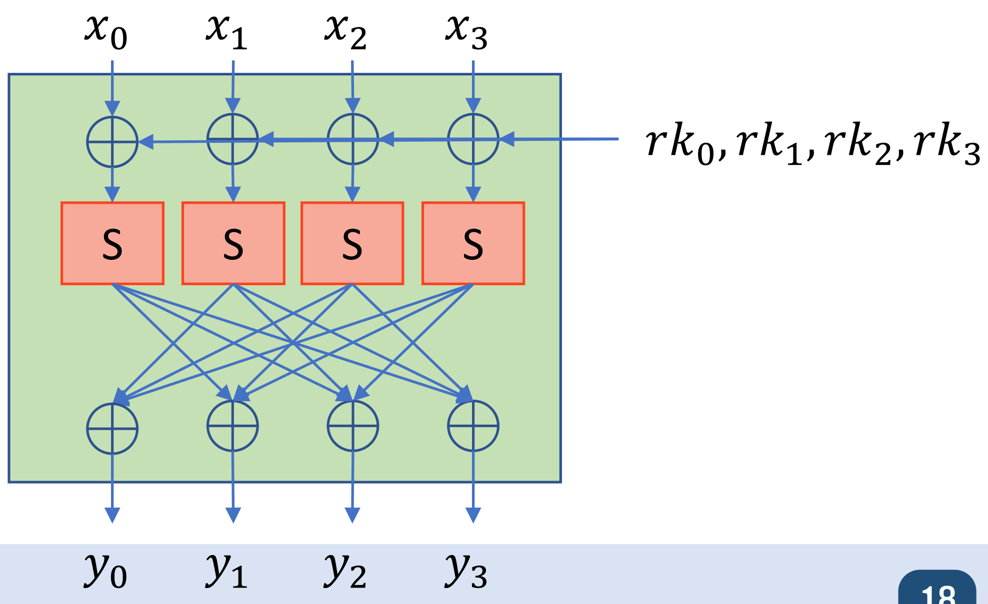


예: TC20 라운드 함수의 차분

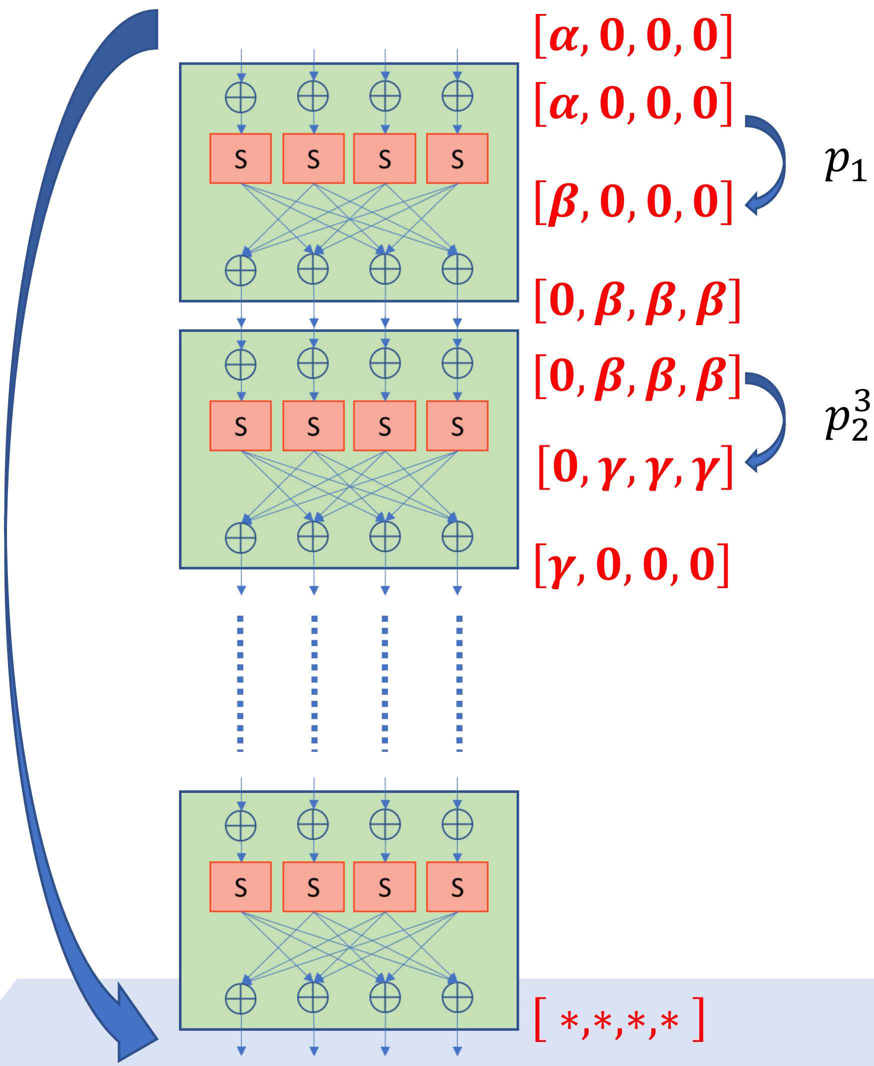
- 라운드 함수의 입력: $X1 \oplus X2 = [\alpha, \alpha, \alpha, 0]$
  - AR(Add Round Key) 직후 차분: $[\alpha, \alpha, \alpha, 0]$
  - Sbox를 통과 후 차분: $[\beta, \beta, \beta, 0]$
  - 선형함수 LM 후: $[0, 0, 0, \beta]$

  라운드 차분특성 $[\alpha, \alpha, \alpha, 0]$ → $[0, 0, 0, \beta]$ (확률 p^3)





예: TC20 다중 라운드의 차분



Sbox의 차분확률

$p_1 = \mathrm{P}[\alpha \to \beta]$

$p_2 = \mathrm{P}[\beta \to \gamma]$

$[\alpha, 0, 0, 0] \to [*, *, *, *]$

다중 라운드 차분확률은
각 라운드 차분확률의 곱
이 확률이 충분히 크면
랜덤함수와 암호를 구별할 수 있다.

차분공격 개요

- 차분 공격(DC, Differential Cryptanalysis)
  - n개 라운드에 대한 높은 확률의 차분특성을 찾는다.
    $[\alpha_1, \alpha_2, \alpha_3, \alpha_4] \rightarrow [\beta_1, \beta_2, \beta_3, \beta_4]$ (확률 p)
  - 입력 평문쌍 P1, P2에 대한 (n+1)라운드 암호화 결과를 C1, C2라 한다.
    $$C1 = E_{n+1}(P1), C2 = E_{n+1}(P2)$$
  - (n+1)번째 라운드 키를 예측(guessing)하여 마지막 라운드를 복화화 한다.
    $$D1 = R^{-1}(C1), D2 = R^{-1}(C2)$$
  - D1, D2의 차분이 차분특성과 일치하면 예측한 키를 올바른 키 후보로 등록한다.
  - 이 과정을 반복하여 가장 많이 추천된 키 후보를 암호키로 판정한다.