차분 특성
(Differential Characteristic)

김상원

https://youtu.be/jmJkrzVlCME

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

DES

차분(Difference)

차분 특성(Differential Characteristic)

Q & A

DES

1972년에 미국 NBS (National Bureau of Standards, 오늘날의 NIST)는 암호 기술의 필요성을 절감하고 미국 정부 규모의 표준적인 암호 알고리즘을 개발하기로 했다. 이에 1974년 8월 27일, IBM에서 루시퍼 암호 알고리즘을 제안했고, 이를 수정하여 1975년 3월 17일에 **DES**를 발표했다.

DES(Data Encryption Standard)는 64비트의 평문을 46비트의 암호문으로 만드는 블록암호 시스템으로 64비트의 키를 사용한다. **데이터 암호화 표준**이라고 한다. 64비트의 키(외부 키)중에서 56비트는 실제의 키(내부 키)가 되고 나머지는 거사용 비트로 사용된다.

DES

- 비선형성(Nonlinearity)

정의 : 출력의 변화가 입력의 변화에 비례하지 않는 성질

블록 암호에서의 "비선형성"은 암호의 강도와 보안성을 높이는 데 중요한 역할을 함 비선형성이 없다면, 암호는 선형적인 방식으로만 동작하게 되어, 암호 해독이 훨씬 쉬워질 수 있음

블록암호 암호문 블록의 각 비트는 키 비트와 평문 블록 비트에 관한 고차 비선형식으로 표현됨

만약 블록 암호 DES의 모든 연산이 선형이라면?

⇒ 암호의 강도가 현저히 낮아짐

차분 (Difference)

정의 : 임의 두 점에서의 함수 값들의 차이

Δ는 모든 과학 분야에서 특정 변수의 앞에 쓰여 해당 변수의 변화량(difference)을 뜻하는 기호로 쓰인다.

$f(x_i + \Delta x) - f(x_i)$

두 값의 **XOR**

변수 $\mathbf{X}$에 대해

$\mathbf{X} = \mathbf{x}_1$ 인 경우와 $\mathbf{X} = \mathbf{x}_2$ 인 경우

$\mathbf{X}$의 차분은 $\Delta\mathbf{X} = \mathbf{x}_1 \oplus \mathbf{x}_2$

⊕	0	1
0	0	1
1	1	0

차분 (선형연산)

$\mathbf{Y} = \mathbf{g}(\mathbf{X})$: 선형 함수

$\mathbf{X} = \mathbf{x}_1$, $\mathbf{X} = \mathbf{x}_2$, $\Delta\mathbf{X} = \mathbf{x}_1 \oplus \mathbf{x}_2$

$\mathbf{y}_1 = \mathbf{g}(\mathbf{x}_1)$, $\mathbf{y}_2 = \mathbf{g}(\mathbf{x}_2)$, $\Delta\mathbf{Y} = \mathbf{y}_1 \oplus \mathbf{y}_2$

$$\Longrightarrow \quad \mathbf{g}(\Delta\mathbf{X}) = \mathbf{g}(\mathbf{x}_1 \oplus \mathbf{x}_2)$$

$$= \mathbf{g}(\mathbf{x}_1) \oplus \mathbf{g}(\mathbf{x}_2)$$

$$= \mathbf{y}_1 \oplus \mathbf{y}_2 = \Delta\mathbf{Y}$$

$$\left(x_1 = \begin{bmatrix} 1 \\ 2 \end{bmatrix} + x_2 = \begin{bmatrix} 3 \\ 4 \end{bmatrix} \right) \times A = \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix}$$

$$= \left(x_1 = \begin{bmatrix} 1 \\ 2 \end{bmatrix} \times A = \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} \right) +$$

$$\left(x_2 = \begin{bmatrix} 3 \\ 4 \end{bmatrix} \times A = \begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} \right)$$

S-box S1의 차분(비선형연산)

- $\mathbf{x_1 = 0x20 \Longrightarrow S1(x_1) = 0x4}$
  $\mathbf{x_2 = 0x10 \Longrightarrow S1(x_2) = 0x3}$
- $\mathbf{S1(x_1) \oplus S1(x_2) = 0x4 \oplus 0x3 = 0x7}$
- $\mathbf{S1(x_1 \oplus x_2) = S1(0x30) = 0x0F}$

S[0]

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2.	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

$S[0]: (x_0, \underbrace{x_1, x_2, x_3, x_4}_{\text{column}}, x_5) \rightarrow (y_0, y_1, y_2, y_3)$

(1, 1, 0, 0, 1, 1): row 3, column 9, S[0](1, 1, 0, 0, 1, 1) = 11 = (1, 0, 1, 1)

S-box S1의 차분(비선형연산)

입력 차분이 $\Delta X = 0x30$인 경우, S1의 모든 입력 쌍

No.	(x1, x2)	No.	(x1, x2)	No.	(x1, x2)	No.	(x1, x2)
0	(0x0, 0x30)	16	(0x10, 0x20)	32	(0x20, 0x10)	48	(0x30, 0x0)
1	(0x1, 0x31)	17	(0x11, 0x21)	33	(0x21, 0x11)	49	(0x31, 0x1)
2	(0x2, 0x32)	18	(0x12, 0x22)	34	(0x22, 0x12)	50	(0x32, 0x2)
3	(0x3, 0x33)	19	(0x13, 0x23)	35	(0x23, 0x13)	51	(0x33, 0x3)
4	(0x4, 0x34)	20	(0x14, 0x24)	36	(0x24, 0x14)	52	(0x34, 0x4)
5	(0x5, 0x35)	21	(0x15, 0x25)	37	(0x25, 0x15)	53	(0x35, 0x5)
6	(0x6, 0x36)	22	(0x16, 0x26)	38	(0x26, 0x16)	54	(0x36, 0x6)
7	(0x7, 0x37)	23	(0x17, 0x27)	39	(0x27, 0x17)	55	(0x37, 0x7)
8	(0x8, 0x38)	24	(0x18, 0x28)	40	(0x28, 0x18)	56	(0x38, 0x8)
9	(0x9, 0x39)	25	(0x19, 0x29)	41	(0x29, 0x19)	57	(0x39, 0x9)
10	(0xA, 0x3A)	26	(0x1A, 0x2A)	42	(0x2A, 0x1A)	58	(0x3A, 0xA)
11	(0xB, 0x3B)	27	(0x1B, 0x2B)	43	(0x2B, 0x1B)	59	(0x3B, 0xB)
12	(0xC, 0x3C)	28	(0x1C, 0x2C)	44	(0x2C, 0x1C)	60	(0x3C, 0xC)
13	(0xD, 0x3D)	29	(0x1D, 0x2D)	45	(0x2D, 0x1D)	61	(0x3D, 0xD)
14	(0xE, 0x3E)	30	(0x1E, 0x2E)	46	(0x2E, 0x1E)	62	(0x3E, 0xE)
15	(0xF, 0x3F)	31	(0x1F, 0x2F)	47	(0x2F, 0x1F)	63	(0x3F, 0xF)

S-box S1의 차분(비선형연산)

입력 차분이 $\Delta X = 0x30$인 경우, S1의 모든 입력 쌍 및 출력 차분 ΔY

No.	(x1, x2) -> ΔY	No.	(x1, x2) -> ΔY	No.	(x1, x2) -> ΔY	No.	(x1, x2) -> ΔY
0	(0x0, 0x30) -> 0x1	16	(0x10, 0x20) -> 0x7	32	(0x20, 0x10) -> 0x7	48	(0x30, 0x0) -> 0x1
1	(0x1, 0x31) -> 0x5	17	(0x11, 0x21) -> 0x5	33	(0x21, 0x11) -> 0x5	49	(0x31, 0x1) -> 0x5
2	(0x2, 0x32) -> 0x8	18	(0x12, 0x22) -> 0xB	34	(0x22, 0x12) -> 0xB	50	(0x32, 0x2) -> 0x8
3	(0x3, 0x33) -> 0x4	19	(0x13, 0x23) -> 0xA	35	(0x23, 0x13) -> 0xA	51	(0x33, 0x3) -> 0x4
4	(0x4, 0x34-> 0x4	20	(0x14, 0x24-> 0x8	36	(0x24, 0x14) -> -0x8	52	(0x34, 0x4) -> 0x4
5	(0x5, 0x35) -> 0x4	21	(0x15, 0x25) -> 0x4	37	(0x25, 0x15) -> 0x4	53	(0x35, 0x5) -> 0x4
6	(0x6, 0x36) -> 0x6	22	(0x16, 0x26) -> 0x4	38	(0x26, 0x16) -> 0x4	54	(0x36, 0x6) -> 0x6
7	(0x7, 0x37) -> 0xA	23	(0x17, 0x27) -> 0x9	39	(0x27, 0x17) -> 0x9	55	(0x37, 0x7) -> 0xA
8	(0x8, 0x38) -> 0x1	24	(0x18, 0x28) -> 0x8	40	(0x28, 0x18) -> 0x8	56	(0x38, 0x8) -> 0x1
9	(0x9, 0x39) -> 0x4	25	(0x19, 0x29) -> 0xD	41	(0x29, 0x19) -> 0xD	57	(0x39, 0x9) -> 0x4
10	(0xA, 0x3A) -> 0x5	26	(0x1A, 0x2A) -> 0xF	42	(0x2A, 0x1A) -> 0xF	58	(0x3A, 0xA) -> 0x5
11	(0xB, 0x3B) -> 0x2	27	(0x1B, 0x2B) -> 0xC	43	(0x2B, 0x1B) -> 0xC	59	(0x3B, 0xB) -> 0x2
12	(0xC, 0x3C) -> 0xE	28	(0x1C, 0x2C) -> 0x2	44	(0x2C, 0x1C) -> 0x2	60	(0x3C, 0xC) -> 0xE
13	(0xD, 0x3D) -> 0xB	29	(0x1D, 0x2D) -> 0x2	45	(0x2D, 0x1D) -> 0x2	61	(0x3D, 0xD) -> 0xB
14	(0xE, 0x3E) -> 0x8	30	(0x1E, 0x2E) -> 0xC	46	(0x2E, 0x1E) -> 0xC	62	(0x3E, 0xE) -> 0x8
15	(0xf, 0x3f) -> 0xC	31	(0x1f, 0x2f) -> 0xF	47	(0x2f, 0x1f) -> 0xF	63	(0x3f, 0xf) -> 0xC

S-box S1의 차분(비선형연산)

입력 차분이 $\Delta X = 0x30$인 경우, S1의 모든 입력 쌍 및 출력 차분 ΔY

No.	(x1, x2) -> ΔY	No.	(x1, x2) -> ΔY	No.	(x1, x2) -> ΔY	No.	(x1, x2) -> ΔY
0	(0x0, 0x30) -> 0x1	16	(0x10, 0x20) -> 0x7	32	(0x2, 0x32) -> 0x8	48	(0x3, 0x33) -> 0x4
1	(0x30, 0x0) -> 0x1	17	(0x20, 0x10) -> 0x7	33	(0x32, 0x2) -> 0x8	49	(0x33, 0x3) -> 0x4
2	(0x8, 0x38) -> 0x1	18	(0x6, 0x36) -> 0x6	34	(0xE, 0x3E) -> 0x8	50	(0x4, 0x34)-> 0x4
3	(0x38, 0x8) -> 0x1	19	(0x36, 0x6) -> 0x6	35	(0x3E, 0xE) -> 0x8	51	(0x34, 0x4) -> 0x4
4	(0xB, 0x3B) -> 0x2	20	(0xF, 0x3F) -> 0xC	36	(0x14, 0x24)-> 0x8	52	(0x5, 0x35) -> 0x4
5	(0x3B, 0xB) -> 0x2	21	(0x3F, 0xF) -> 0xC	37	(0x24, 0x14) -> 0x8	53	(0x35, 0x5) -> 0x4
6	(0x1C, 0x2C) -> 0x2	22	(0x1B, 0x2B) -> 0xC	38	(0x18, 0x28) -> 0x8	54	(0x9, 0x39) -> 0x4
7	(0x2C, 0x1C) -> 0x2	23	(0x2B, 0x1B) -> 0xC	39	(0x28, 0x18) -> 0x8	55	(0x39, 0x9) -> 0x4
8	(0x1D, 0x2D) -> 0x2	24	(0x1E, 0x2E) -> 0xC	40	(0x1, 0x31) -> 0x5	56	(0x15, 0x25) -> 0x4
9	(0x2D, 0x1D) -> 0x2	25	(0x2E, 0x1E) -> 0xC	41	(0x31, 0x1) -> 0x5	57	(0x25, 0x15) -> 0x4
10	(0xC, 0x3C) -> 0xE	26	(0x19, 0x29) -> 0xD	42	(0xA, 0x3A) -> 0x5	58	(0x16, 0x26) -> 0x4
11	(0x3C, 0xC) -> 0xE	27	(0x29, 0x19) -> 0xD	43	(0x3A, 0xA) -> 0x5	59	(0x26, 0x16) -> 0x4
12	(0xD, 0x3D) -> 0xB	28	(0x1A, 0x2A) -> 0xF	44	(0x11, 0x21) -> 0x5	60	(0x7, 0x37) -> 0xA
13	(0x3D, 0xD) -> 0xB	29	(0x2A, 0x1A) -> 0xF	45	(0x21, 0x11) -> 0x5	61	(0x37, 0x7) -> 0xA
14	(0x12, 0x22) -> 0xB	30	(0x1F, 0x2F) -> 0xF	46	(0x17, 0x27) -> 0x9	62	(0x13, 0x23) -> 0xA
15	(0x22, 0x12) -> 0xB	31	(0x2F, 0x1F) -> 0xF	47	(0x27, 0x17) -> 0x9	63	(0x23, 0x13) -> 0xA

Pr(S1 : ΔX -> ΔY)

입력 차분 ΔX에 대해 S1의 출력 차분이 ΔY가 될 확률

Pr(S1:0x30 -> 0x1) = 4/64
Pr(S1:0x30 -> 0x2) = 6/64
Pr(S1:0x30 -> 0x4) = 12/64
Pr(S1:0x30 -> 0x5) = 6/64
Pr(S1:0x30 -> 0x6) = 2/64
Pr(S1:0x30 -> 0x7) = 2/64
Pr(S1:0x30 -> 0x8) = 8/64
Pr(S1:0x30 -> 0x9) = 2/64
Pr(S1:0x30 -> 0xA) = 4/64
Pr(S1:0x30 -> 0xB) = 4/64
Pr(S1:0x30 -> 0xC) = 6/64
Pr(S1:0x30 -> 0xD) = 2/64
Pr(S1:0x30 -> 0xE) = 2/64
Pr(S1:0x30 -> 0xF) = 4/64

Q & A