Cryptanalysis - FINAL

June 10, 2024

Ji, Yong-hyeon

1 2021

1. 치환함수 $S : \{0,1\}^3 \to \{0,1\}^3$가 다음과 같이 정의되었다고 하자.

x	0(000)	1(001)	2(010)	3(011)	4(100)	5(101)	6(110)	7(111)
$S[x]$	0	2	4	6	5	7	3	1

(a) 입력차분이 $\alpha = 4$일 때, 출력차분이 β가 될 확률 $P[\alpha \to \beta]$의 최댓값과 그 때의 β를 구하면?

(b) 입력 마스크가 $a = 6(110)$이고 출력 마스크가 $b = 2(010)$일 때

$$NS(a,b) = \{x \mid a \cdot x = b \cdot S[x]\}$$

의 원소의 개수는? 임이의 입력 x에 대하여 $a \cdot x = b \cdot S[x]$가 만족될 확률은?

Sol.

(a)

x	$x \oplus 100$	$S[x]$	$S[x \oplus 100]$	$\beta = S[x] \oplus S[x \oplus 100]$
000	100	000	101	101
001	101	010	111	101
010	110	100	011	111
011	111	110	001	111
100	000	101	000	101
101	001	111	010	101
110	010	011	100	111
111	011	001	110	111

따라서 $\beta \in \{(101)_2, (111)_2\} = \{5,7\}$ 일 때,

$$P[100 \to 101] = \frac{1}{2} = P[100 \to 111]$$

이다.

(b) Let $x = (x_2x_1x_0)_2$ and $S[x] = (y_2y_1y_0)_2$. Consider $a = (110)_2$ and $b = (010)_2$:

$[x_2]$	$[x_1]$	x_0	y_2	$[y_1]$	y_0	$a \cdot x = b \cdot y$	
0	0	0	0	0	0	$0 = 0$	✓
0	0	1	0	1	0	$0 = 1$	✗
0	1	0	1	0	0	$1 = 0$	✗
0	1	1	1	1	0	$1 = 1$	✓
1	0	0	1	0	1	$1 = 0$	✗
1	0	1	1	1	1	$1 = 1$	✓
1	1	0	0	1	1	$0 = 1$	✗
1	1	1	0	0	1	$0 = 0$	✓

따라서 집합 $NS(a, b)$의 원소의 개수는 4이고, 임이의 입력 x에 대하여 $a \cdot x = b \cdot S[x]$가 만족될 확률은 $\frac{4}{8} = \frac{1}{2}$이다.

□

2. 표본공간(sample space) $\{0, 1\}$인 독립확률변수(independent random variable) X_1, X_2, X_3가

$$P[X_1 = 0] = P[X_2 = 0] = P[X_3 = 0] = \frac{3}{4}$$

를 만족할 때, Piling-up lemma를 이용하여 확률 $P[X_1 \oplus X_2 \oplus X_3 = 0]$을 구하면?

Sol.

Theorem (Piling-Up Lemma). Let $X_i \in \{0, 1\}$ is independent binary random variables. Then

$$\Pr\left[\bigoplus_{i=1}^{n} X_i = 0\right] = \frac{1}{2} + 2^{n-1} \prod_{i=1}^{n} \left(p_i - \frac{1}{2}\right)$$

where $p_i = \Pr[X_i = 0]$ and $\bigoplus$ denotes the XOR operation.

Thus,

$$\begin{aligned} P[X_1 \oplus X_2 \oplus X_3 = 0] &= \frac{1}{2} + 2^{3-1} \left(\frac{3}{4} - \frac{1}{2}\right)\left(\frac{3}{4} - \frac{1}{2}\right)\left(\frac{3}{4} - \frac{1}{2}\right) \\ &= \frac{1}{2} + 4 \cdot \left(\frac{1}{4}\right)^3 \\ &= \frac{1}{2} + \frac{1}{16} = \frac{9}{16}. \end{aligned}$$

□

2 2023

1. [10점] 치환함수 $S : \{0,1\}^3 \to \{0,1\}^3$가 다음과 같이 정의되었다고 하자.

x	0(000)	1(001)	2(010)	3(011)	4(100)	5(101)	6(110)	7(111)
$S[x]$	2	1	0	5	3	7	6	4

(a) 이 함수의 차분특성은 다음표와 같다.

입력차분 Δx	출력차분 Δy							
	0	1	2	3	4	5	6	7
0	8	0	0	0	0	0	0	0
1	0	0	2	2	2	2	0	0
2	0	0	Ⓐ	*	*	*	0	0
3	0	Ⓑ	0	0	0	0	0	4
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

빈칸 Ⓐ와 Ⓑ에 들어갈 값을 계산하면?

(b) 입력 $x = x_2x_1x_0$에 대한 출력을 $S[x] = y_2y_1y_0$라 할 때,

$$x_1 \oplus x_2 = y_0 \oplus y_2$$

를 만족할 확률은? 즉, 입력 마스크 $a = 6(110)$, 출력 마스크 $b = 5(101)$에 대하여 $a \cdot x = b \cdot S[x]$를 만족할 확률은?

Sol. (a) $A = 2$ and $B = 4$:

x	$x \oplus 010$	$S[x]$	$S[x \oplus 010]$	Δy
000	010	010	000	010
001	011	001	101	100
010	000	000	010	010
011	001	101	001	100
100	110	011	110	101
101	111	111	100	011
110	100	110	011	101
111	101	100	111	011

$\Longrightarrow P[\Delta x = 2 \to \Delta y = 2] = 2/8 = 1/4.$

(b)

$[x_2]$	$[x_1]$	x_0	$[y_2]$	y_1	$[y_0]$	$a \cdot x = b \cdot y$	
0	0	0	0	1	0	0 = 0	✓
0	0	1	0	0	1	0 = 1	✗
0	1	0	0	0	0	1 = 0	✗
0	1	1	1	0	1	1 = 0	✗
1	0	0	0	1	1	1 = 1	✓
1	0	1	1	1	1	1 = 0	✗
1	1	0	1	1	0	0 = 1	✗
1	1	1	1	0	0	0 = 1	✗

$\Longrightarrow$ the probability is 2/8 = 1/4.

□

2. [20점] 다음 그림과 같이 8비트 평문 메시지 m을 암호문 c로 변환하는 암호 알고리즘을 생각하자.

사용된 Sbox 함수 $S : \{0,1\}^8 \to \{0,1\}^8$는 다음과 같은 선형특성을 갖는다.

S의 선형근사 확률

입력 마스크(a)	출력 마스크(b)	선형근사 확률 $P[a \cdot x = b \cdot S(x)]$
0000 0001	0000 0011	$0.5 + 0.4$
0000 0001	0000 0010	$0.5 + 0.3$
0000 0010	0001 0001	$0.5 - 0.3$
0000 0001	0000 1001	$0.5 + 0.2$
0001 0001	0000 0001	$0.5 - 0.1$
0000 0011	0000 0010	$0.5 - 0.1$
0000 1001	0001 0001	$0.5 - 0.1$
⋮	⋮	⋮

(a) 다음과 같은 단계로 선형 공격을 시도할 수 있다.

1. 다수의 (평문, 암호문) 쌍 $\{(m_i, c_i) \mid i = 1, 2, \ldots, N\}$를 수집한다.
2. 암호키 k_3를 예측하여 다음 식을 계산한다.

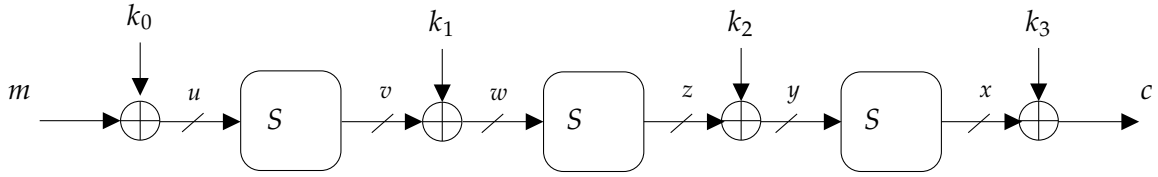
$$L_i := \alpha \cdot m_i \oplus \gamma \cdot S^{-1}[c_i \oplus k_3]$$

3. $L_1, L_2, \ldots, L_N$의 값을 보고 가장 가능성이 높은 라운드 키 k_3를 찾는다.

표에 주어진 선형특성을 고려할 때, α, γ를 어떻게 선택하는 것이 바람직한가? 그 이유는?

(b) 위의 공격을 통해 올바른 라운드 키 k_3를 찾았다고 가정하자. 선형공격으로 나머지 키를 찾는 방법을 설명하라. 이 과정에서 사용하는 선형관계식은 무엇인가?

Sol.



Let

$$u = m \oplus k_0 \qquad v = S[u] \qquad w = v \oplus k_1$$
$$x = c \oplus k_3 \qquad y = S^{-1}[x] \qquad z = y \oplus k_2$$

(a) Consider

$$\alpha \cdot u \oplus \beta \cdot v = 0 \qquad \cdots\cdots \; p_1 = \frac{1}{2} + \epsilon_1,$$
$$\beta \cdot w \oplus \gamma \cdot z = 0 \qquad \cdots\cdots \; p_2 = \frac{1}{2} + \epsilon_2.$$

By Piling-up Lemma, we have

$$\alpha \cdot u \oplus \beta \cdot (v \oplus w) \oplus \gamma \cdot z = 0 \qquad \cdots\cdots \; p = \frac{1}{2} + 2\epsilon_1\epsilon_2$$
$$\alpha \cdot (m \oplus k_0) \oplus \beta \cdot k_1 \oplus \gamma \cdot (S^{-1}[c \oplus k_3] \oplus k_2) = 0$$
$$\alpha \cdot m \oplus \gamma \cdot S^{-1}[c \oplus k_3] = \alpha \cdot k_0 \oplus \beta \cdot k_1 \oplus \gamma \cdot k_2.$$

여기서 확률 p가 최대가 되도록 α와 β를 선택한다. 따라서

$$\alpha = 0000\ 0001, \quad \beta = 0000\ 0010, \quad \gamma = 0001\ 0001.$$

(b) k_3를 찾은 경우 $y = S^{-1}[c \oplus k_3]$가 주어진다. 따라서

$$a \cdot u = b \cdot v \qquad \cdots\cdots \; p$$
$$a \cdot (m \oplus k_0) = b \cdot (S^{-1}[y \oplus k_2] \oplus k_1)$$
$$a \cdot m \oplus b \cdot S^{-1}[y \oplus k_2] = a \cdot k_0 \oplus b \cdot k_1.$$

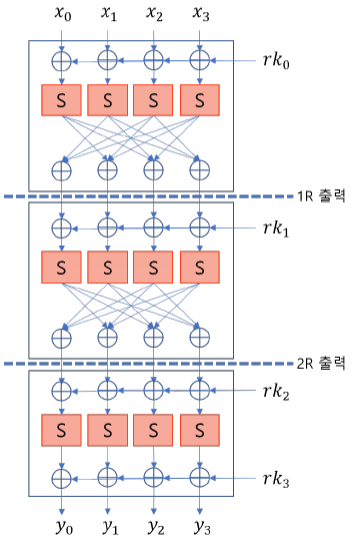
여기서 확률 p가 최대가 되도록 a와 b를 선택한다. 따라서

$$\begin{cases} a = 0000\ 0001 \\ b = 0000\ 0011 \end{cases} \qquad \cdots\cdots p = P[a \cdot x = b \cdot S[x]] = 0.5 + 0.4 = 0.9$$

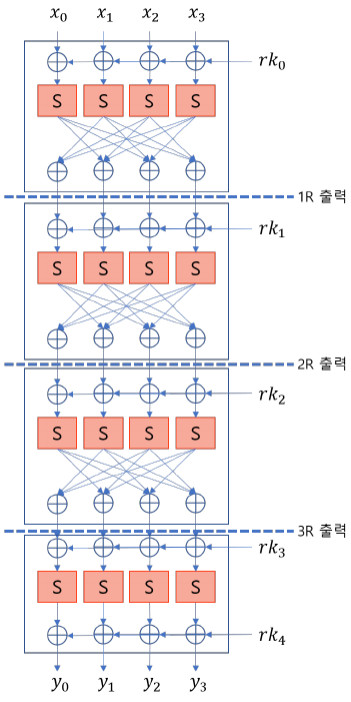
□

3. [20점] 아래는 TC20R과 동일한 라운드함수를 사용하는 블록암호 알고리즘이다. Sbox[]는 AES의 $S : \{0,1\}^8 \rightarrow \{0,1\}^8$를 사용한다고 가정하자. 왼쪽 그림은 3라운드, 오른쪽 그림은 4라운드 암호화를 나타내며 마지막 라운드에는 선형함수 LM이 사용되지 않는다. 블록암호의 입출력 크기와 암호키는 32비트이며, 각 라운드에서 사용한 라운드 키는 적절한 키 스케줄에 따라 생성된다고 하자.

```
#== AR: Add Roundkey
def AR(in_state, rkey):
    out_state = [0] * len(in_state)
    for i in range(len(in_state)):
        out_state[i] = in_state[i] ^ rkey[i]
    return out_state

#== SB: Sbox layer
def SB(in_state):
    out_state = [0] * len(in_state)
    for i in range(len(in_state)):
        out_state[i] = Sbox[in_state[i]]
    return out_state

#== LM: Linear Map
def LM(in_state):
    out_state = [0] * len(in_state)
    All_Xor = in_state[0] ^ in_state[1] ^ in_state[2] ^ in_state[3]
    for i in range(len(in_state)):
        out_state[i] = All_Xor ^ in_state[i]
    return out_state

#== Enc_Round
def Enc_Round(in_state, rkey):
    out_state = [0] * len(in_state)
    out_state = AR(in_state, rkey)
    in_state = SB(out_state)
    out_state = LM(in_state)
    return out_state
```



3라운드 암호화



4라운드 암호화

(a) 다음과 같이 (Active, const, const, const) 성질을 갖는 256개의 평문을 입력할 때, 1라운드 출력의 각 바이트는 Active, const, Balanced 중 어떤 성질을 가지는가?

$$\Lambda = \{(x_0, x_1, x_2, x_3) \,|\, x_0 = 0, 1, 2, \ldots, 255, x_1 = 1, x_2 = 2, x_3 = 2\}.$$

(b) (a)와 동일한 입력 Λ를 사용할 때, 2라운드 출력의 각 바이트는 Active, const, Balanced 중 어떤 성질을 가지는가?

(c) 3라운드 암호화(왼쪽 그림)에 대하여 Integral cryptanalysis를 사용하면, 3라운드 키 rk_3(4바이트)를 구할 수 있음을 보여라. 이 때, 공격에 필요한 선택평문, 암호문 쌍의 개수와 계산량을 설명하라.

(d) 4라운드 암호화(오른쪽 그림)에 대하여 Integral cryptanalysis를 사용하면, 4라운드 키 rk_4(4바이트)를 구할 수 있는가? 이 공격은 32비트 키에 대한 전주조사 공격보다 효율적인가?

(a) (1R) $(A, C, C, C) \xrightarrow{S} (A, C, C, C) \xrightarrow{LM} (C, A, A, A)$. Thus,

(Const, Active, Active, Active)

(b) (2R) $(C, A, A, A) \xrightarrow{S} (C, A, A, A) \xrightarrow{LM} (B, B, B, B)$. Thus,

(Balanced, Balanced, Balanced, Balanced)

(c) Blanced를 만족할 확률은 $1/2^8$이며, $2^8 \times 1/2^8 = 1$이다. 따라서 $2^8 = 256$개만 하면 wrong key가 나올 수 있으니, (P, C) 쌍 $2^8 \times 2$ 개 정도 필요하다. Sbox 하나 당

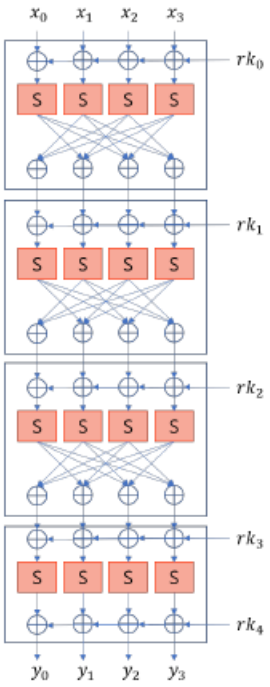
$$2^8 \times 2^8(\text{키후보}) \times 2.$$

(d) 2라운드 0번째 바이트가 Balanced 인 것을 확인한다.

$$rk_3'[0], rk_4[1], rk_4[2], rk_4[3]$$

를 예측한다. 이는 2^{32} 계산량으로 round key를 예측하는 것이므로 32 비트 (2^{32}) 키에 대한 전수보다 비효율적이다.

4. [20점] 아래는 TC20R과 유사한 라운드함수를 사용하는 블록암호 알고리즘이다.



3번 문제와 같은 구조의 라운드 함수로 구성된 알고리즘이지만 다른 Sbox[]를 사용한다. 사용된 Sbox[]의 주요 차분특성은 다음 표와 같다.

S의 차분 확률 $P[\Delta x \to \Delta y]$

$P[\texttt{0x01} \to \texttt{0x01}] = 0.0$	$P[\texttt{0x03} \to \texttt{0x01}] = 0.0$	$P[\texttt{0x0F} \to \texttt{0x01}] = 0.063$
$P[\texttt{0x01} \to \texttt{0x02}] = 0.016$	$P[\texttt{0x03} \to \texttt{0x02}] = 0.016$	$P[\texttt{0x0F} \to \texttt{0x02}] = 0.016$
$P[\texttt{0x01} \to \texttt{0x03}] = 0.25$	$P[\texttt{0x03} \to \texttt{0x03}] = 0.0$	$P[\texttt{0x0F} \to \texttt{0x03}] = 0.0$
$P[\texttt{0x01} \to \texttt{0x0F}] = 0.25$	$P[\texttt{0x03} \to \texttt{0x0F}] = 0.25$	$P[\texttt{0x0F} \to \texttt{0x0F}] = 0.016$
$P[\texttt{0x01} \to \texttt{0x10}] = 0.0$	$P[\texttt{0x03} \to \texttt{0x10}] = 0.0$	$P[\texttt{0x0F} \to \texttt{0x10}] = 0.125$
$\vdots$	$\vdots$	$\vdots$

(a) 1라운드 출력차분을 $(\Delta w_0, \Delta w_1, \Delta w_2, \Delta w_3)$라고 할 때 $\Delta w_2 = 0$이 되는 입력 평문 쌍 P_1, P_2 $(P_1 \neq P_2)$를 제시하라.

(b) 3라운드 차분특성을 이용하여 4라운드 키 rk_4를 찾는 공격을 구성하고자 한다. 차분공격에 적합한 입력차분 ΔX와 대응되는 3라운드 출력차분 ΔY를 찾고 중간단계의 차분경로와 차분확률을 계산하라.

$$\Delta X = (\Delta x_0, \Delta x_1, \Delta x_2, \Delta x_3) \longrightarrow \Delta Y = (\Delta y_0, \Delta y_1, \Delta y_2, \Delta y_3)$$

$$\Delta X \xrightarrow{1R} \Delta V \xrightarrow{2R} \Delta W \xrightarrow{3R} \Delta Y$$

Sol.

(a) $P_1 = \texttt{0x00 00 00 00}, P_2 = \texttt{0x00 00 01 00}$

(b) Consider

$$(\alpha,0,0,0) \xrightarrow{S \text{ with } p_1} (\beta,0,0,0) \qquad \cdots\cdots \text{ Round 1}$$
$$\xrightarrow{LM} (0,\beta,\beta,\beta)$$

$$(0,\beta,\beta,\beta) \xrightarrow{S \text{ with } p_2^3} (0,\gamma,\gamma,\gamma) \qquad \cdots\cdots \text{ Round 2}$$
$$\xrightarrow{LM} (\gamma,0,0,0)$$

$$(\gamma,0,0,0) \xrightarrow{S \text{ with } p_3^1} (\delta,0,0,0) \qquad \cdots\cdots \text{ Round 3}$$
$$\xrightarrow{LM} (0,\delta,\delta,\delta)$$

Consider

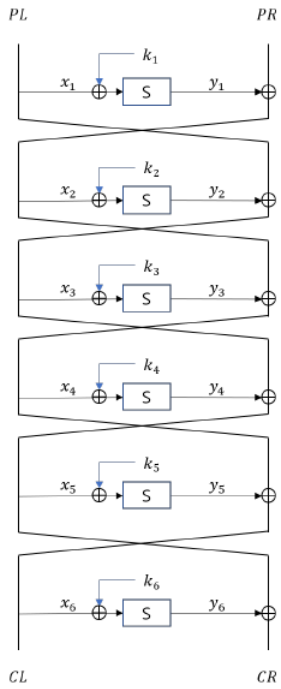
$$p_1 = P[\texttt{0x01} \rightarrow \texttt{0x03}] = 0.25,$$
$$p_2 = P[\texttt{0x03} \rightarrow \texttt{0x0F}] = 0.25,$$
$$p_3 = P[\texttt{0x0F} \rightarrow \texttt{0x10}] = 0.125.$$

Then $p = \left(\frac{1}{4}\right)\left(\frac{1}{4}\right)^3\left(\frac{1}{8}\right) = \frac{1}{2^{11}} > \frac{1}{2^{32}}$ and

$$(\texttt{0x01},\texttt{0x00},\texttt{0x00},\texttt{0x00}) \xrightarrow{1R} (\texttt{0x00},\texttt{0x03},\texttt{0x03},\texttt{0x03}) \qquad \cdots\cdots\ p_1 = 1/4$$
$$\xrightarrow{2R} (\texttt{0x0F},\texttt{0x00},\texttt{0x00},\texttt{0x00}) \qquad \cdots\cdots\ p_2^3 = 1/4^3$$
$$\xrightarrow{3R} (\texttt{0x00},\texttt{0x10},\texttt{0x10},\texttt{0x10}) \qquad \cdots\cdots\ p_3 = 1/8.$$

□

5. [20점] 다음과 같은 6라운드 Feistel 암호를 생각하자. 입력 평문 $P = (PL, PR)$, 출력 암호문 $C = (CL, CR)$은 8비트이며, 4비트 라운드키 6개 $k_1, k_2, \ldots, k_6$가 사용된다.



라운드 함수 $F : \{0,1\}^4 \to \{0,1\}^4$는 $F(x,k) = S(x \oplus k)$로 정의되고, S는 아래와 같은 일대일 Sbox 함수이다.

$$S = [0, 4, 11, 2, 1, 5, 14, 15, 10, 3, 6, 7, 9, 13, 12, 8]$$

S의 차분특성은 다음 표와 같다.

입력차분 Δx	출력차분 Δy															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	4	0	0	8	0	0	0	0	4	0	0	0	0	0	0
2	0	0	0	0	2	4	2	0	0	0	2	2	2	0	0	2
3	0	4	2	0	0	2	0	0	0	0	0	2	0	2	2	2
4	0	4	0	2	0	2	0	0	0	0	2	0	0	2	2	2
5	0	0	0	0	2	4	0	2	0	0	2	2	2	0	2	0
6	0	0	0	0	0	0	2	2	0	0	4	4	0	0	2	2
7	0	0	2	2	0	0	0	0	0	0	2	2	0	0	4	4
8	0	0	2	0	0	2	0	4	4	0	2	0	0	2	0	0
9	0	0	0	4	2	0	2	0	0	0	0	0	6	0	2	0
10	0	4	2	2	0	0	2	2	0	0	0	0	0	4	0	0
11	0	0	2	2	0	0	2	2	4	4	0	0	0	0	0	0
12	0	0	0	0	0	0	2	2	4	4	2	2	0	0	0	0
13	0	0	2	2	0	0	0	0	0	4	0	0	0	4	2	2
14	0	0	4	0	2	0	0	2	0	0	0	0	6	0	0	2
15	0	0	0	2	0	2	4	0	4	0	0	2	0	2	0	0

(a) 두 평문 $P_1 = (PL_1, PR_1)$, $P_2 = (PL_2, PR_2)$가 다음 조건을 만족한다고 하자.

$$PL_1 \oplus PL_2 = 0, \quad PR_1 \oplus PR_2 = \alpha \ (\alpha \neq 0).$$

대응되는 암호문을 $C_1 = (CL_1, CR_1)$, $C_2 = (CL_2, CR_2)$라 할 때, 두 조건

$$CL_1 \oplus CL_2 = \alpha, \quad CR_1 \oplus CR_2 = F(CL_1, k_6) \oplus F(CL_2, k_6)$$

이 모두 성립할 수는 없음을 설명하라.

(b) 입력 평문 $P_1 = (6, 14)$, $P_2 = (6, 13)$에 대응되는 암호문이 $C_1 = (7, 15)$, $C_2 = (4, 13)$이라고 하자. 이 정보로부터 6라운드 키 k_6가 될 수 없는 값을 찾으면?

Sol.

(a) 입력 차분 $(0, \alpha)$, 5라운드 차분 $(\alpha, 0)$. 5R 불능차분특성:

$$\alpha \oplus \alpha = 0 = \gamma \neq 0.$$

(b) Consider $\Delta P = P_1 \oplus P_2 = (0, 14 \oplus 13) = (0, 3)$. Then

- $CL_1 \oplus CL_2 = 7 \oplus 4 = 3 = \alpha$;
- $CR_1 \oplus CR_2 = F(CL_1, k_6) \oplus F(CL_2, k_6)$을 만족하는 k_6는 키 후보에서 삭제.
  - $CR_1 \oplus CR_2 = 15 \oplus 3 = 2$
  -

k_6	$0111 \oplus k_6$	$0100 \oplus k_6$	$S[0111 \oplus k_6]$	$S[0100 \oplus k_6]$	$\Delta = S[CL_1 \oplus k_6] \oplus S[CL_2 \oplus k_6]$
⋮	⋮	⋮	⋮	⋮	⋮
0100	0011	0000	0010	0000	0010

Thus, $k \neq 0100$

□

6. [10점] 64비트 입출력과 64비트 키를 사용하는 블록암호 E에 대한 TMTO 공격을 생각하자.

   (1) 랜덤한 m개 시작점을 선택한다.

   (2) 각 시작점에 대하여 길이 t인 체인을 만든다.

   (3) 과정 (1)과 (2)를 반복하여 ℓ개의 Hellman 테이블을 만든다.

$$X_{i,j+1} = f(X_{i,j}) = E(PT, X_{i,j}), \quad (i = 1, 2, \ldots, m, \ j = 0, 1, \ldots, t).$$

공격에 필요한 파라미터를 $m = 2^{20}$, $t = 2^{20}$, $\ell = 2^{24}$ 로 설정한다고 하자.

$$\begin{array}{|l|l|l|}
\hline
SP_1 & = X_{1,0} \to X_{1,1} \to X_{1,2} \to \cdots \to X_{1,t-1} \to X_{1,t} = & EP_1 \\
SP_2 & = X_{2,0} \to X_{2,1} \to X_{2,2} \to \cdots \to X_{2,t-1} \to X_{2,t} = & EP_2 \\
SP_i & = X_{i,0} \to X_{i,1} \to X_{i,2} \to \cdots \to X_{i,t-1} \to X_{i,t} = & EP_i \\
SP_m & = X_{m,0} \to X_{m,1} \to X_{m,2} \to \cdots \to X_{m,t-1} \to X_{m,t} = & EP_m \\
\hline
\end{array}$$

하나의 TMTO 테이블에 포함된 $m \times t$개 암호키 중 서로 다른 암호키의 비율을 ECR(Expected Coverage Rate)라고 한다.

ECR $= 0.8$일 때, 이 TMTO 공격이 성공할 확률을 추정하라.

Sol. Note that

$$1 - \left(1 - \frac{ECR \cdot mt}{2^{64}}\right)^{\ell}.$$

Since $(1-a)^b = \exp(-ab)$ ($\lim_{h\to 0}(1+h)^{1/h} = e$, $\lim_{a\to 0}(1-a)^b = \lim_{a\to 0}[(1-a)^{-1/a}]^{-ab} = \exp(-ab)$), we have

$$1 - \exp(-\frac{ECR \cdot mt\ell}{2^{64}}) = 1 - \exp(-0.8).$$

□

Department of Information Security, Cryptology and Mathematics
College of Science and Technology
Kookmin University