باسمه تعالی

پوریا ولدخواه - ۴۰۱۲۰۱۳۸۹

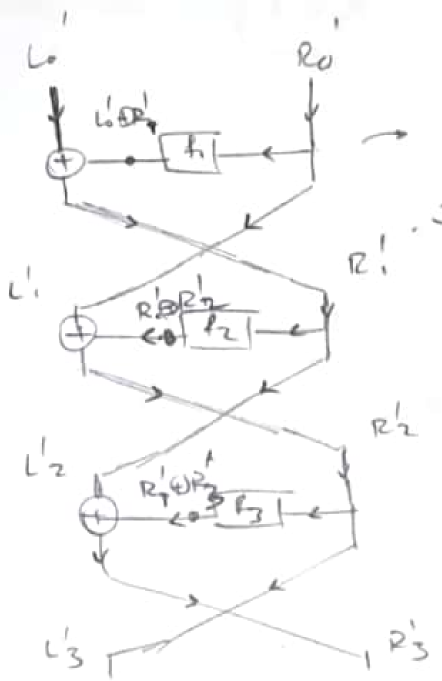
تمرین سری سوم

رمزنگاری پیشرفته

۱- * جدول P^{-1} به این صورت است:

۹	۱۷	۲۳	۳۱
۱۳	۲۸	۲	۱۸
۲۴	۱۶	۳۰	۶
۲۶	۲۰	۱۰	۱
۸	۱۴	۲۵	۳
۴	۲۹	۱۱	۱۹
۳۲	۱۲	۲۲	۷
۵	۲۷	۱۵	۲۱

P^{-1}



ورودی f_1 برابر R_0' و خروجی $L_0' \oplus R_1'$ است.

R_0' پس از ورود به f، از E عبور می‌کند تا مقدار تفاضلی در ورودی S-Box ها مشخص شود. بر $L_0' + R_1'$ هم P^{-1} اعمال می‌شود تا خروجی S-Box مشخص شود؛

$R_0' = 0x00000400$

پس از عبور از E → ورودی: $\overbrace{000000}^{S_1}\ \overbrace{000000}^{S_2}\ \overbrace{000000}^{S_3}\ \overbrace{000000}^{S_4}\ \overbrace{000000}^{S_5}\ \overbrace{001000}^{S_6}\ \overbrace{000000}^{S_7}\ \overbrace{000000}^{S_8}$

$R_1' \oplus L_0' = L_0' = 0000\ 0000\ 0010\ 0000\ 0000\ 0000\ 0000\ 1000$

$P^{-1}(L_0) = \underbrace{0000}_{S_1}\ \underbrace{0000}_{S_2}\ \underbrace{0000}_{S_3}\ \underbrace{0000}_{S_4}\ \underbrace{0000}_{S_5}\ \underbrace{0110}_{S_6}\ \underbrace{0000}_{S_7}\ \underbrace{0000}_{S_8}$

خروجی

پس تمام ورودی‌های تمام صفر به خروجی تمام صفر رفته‌اند که انتظار داشتیم با احتمال ۱ اتفاق بیفتد!

$$R = P(\overbrace{000000 \to 0000}^{S_1}) \times P(\overbrace{000000 \to 0000}^{S_2}) \times \dots \times P(\overbrace{001000 \to 0110}^{S_6}) \times \dots$$

$P_1 = 1 \times 1 \times \dots \times \frac{16}{64} \times \dots 1 \Rightarrow \boxed{P_1 = \frac{1}{4}}$

از جدول S-Box ۶ داریم $\Delta = \frac{16}{64} = P(8x \to 6x)$

* به طور مشابه برای f_2 عمل می‌کنیم:

ورودی: $R_1' = 0x\,00\ldots0 \xrightarrow{E\text{ عبور از}} \overbrace{00000}^{S_1} \cdots \overbrace{000000}^{S_8}$

خروجی: $R_0' \oplus R_2' = 0 \Rightarrow P^{-1}(R_0' + R_2') = 0$

اینجا نیز همه‌ی تمام صفر به خروجی تمام صفر رفته طبق انتظار $\Rightarrow$ $P_2 = 1$

* برای f_3 داریم:

ورودی: $R_2' = 0x\,0000040 = R_0'$

خروجی: $R_1' \oplus R_3' \underset{=}{\overset{R_3' = L_0'}{}} R_1' \oplus L_0' = L_0' \Rightarrow P_3 = P_1 = \frac{1}{4}$

احتمال کل: $P = P_1 \times P_2 \times P_3 = \frac{1}{16}$

۲ـ در این سؤال نیز مشابه سؤال قبل جلو می‌رویم:

* (f_1):

ورودی $= R_0' = \overbrace{000000}^{S_1} \cdots \overbrace{000000}^{S_8} = 0$

خروجی $= R_1' \oplus L_0' \underset{=}{\overset{L_0' = R_1'}{}} 0$

$\Leftarrow$ ورودی تمام صفر به خروجی تمام صفر نظیر شده است

$\Rightarrow P_1 = 1$

* (f_2) ورودی: $R_1' = 0x19600000 = 0001\;1001\;0110\;0000 \cdots 0000$

$E(R_1') = \underbrace{000011}_{S_1}\;\underbrace{110010}_{S_2}\;\underbrace{101100}_{S_3}\;\underbrace{000000}_{S_4} \cdots \underbrace{000000}_{S_8}$:ورودی

خروجی: $R_0' \oplus R_2' = 0 \oplus 0 = 0$ خروجی تمام صفر

$\Leftarrow$ احتمال اینکه خروجی S-Box تمام صفر باشد را باید حساب کنیم. ورودی S4 تا S8 و خروجی تمام صفر دارند ✓

احتمال ①

$$\left.\begin{array}{l} P_{S_1}(000011 \to 0000) = P(3x \to 0x) = \frac{16}{64} \\ P_{S_2}(110010 \to 0000) = P(32x \to 0x) = \frac{8}{64} \\ P_{S_3}(101100 \to 0000) = P(2Cx \to 0x) = 10/64 \end{array}\right\}$$

احتمال S_1 تا S_3 $\Leftarrow$ $\Rightarrow P = P_1 \times P_2 \times P_3 \approx 0/00$

۳- طبق مشخصه‌های تفاضلی داده شده در سوال قبل احتمال $p_1=1$ است که بیشترین احتمال است.

با داشتن R'_1 ، L'_1 باید حالتی را بیابیم که با بیشترین احتمال ما R'_2 ، L'_2 رخ دهد.

$R'_1 = 0x\,196\,00000 = 0001\ 1001\ 0110\ 0000\ \dots\ 0000$

$E(R'_1) = \underbrace{000011}_{S_1}\ \underbrace{110010}_{S_2}\ \underbrace{101100}_{S_3}\ \underbrace{000000}_{S_4}\ \dots\ \underbrace{000000}_{S_8}$

$\max P_{S_1}(000011 \to x) \Rightarrow x = 0000 \Rightarrow P = \frac{14}{64}$

$\max P_{S_2}(110010 \to x) \Rightarrow x = 0000, 0111, 1011 \Rightarrow P = \frac{8}{64}$

$\max P_{S_3}(101100 \to x) \Rightarrow x = 0000, 1001 \Rightarrow P = \frac{10}{64}$

$\max P_{S_{4\to 8}} = 1$

⇐ مولد انتهایی در سوال ۲ بیشترین احتمال را دارند (در سایر حالت‌های دیگر) بنابراین همان احتمال پیش می‌رویم.

⇐ اگر مشخصه تفاضلی سوال ۲ را ۶ بار تکرار کنیم باز هم به $L'_{12}=L'_0$ ، $R'_{12}=R'_0$ می‌رسیم و احتمال اینکه

$R'_{12}=0x00\dots0$

$L'_{12}=0x1960\dots0$

باشد که بیشترین احتمال ممکن برای یک حالت در راند ۱۲ ام است، برابر $(4\times10^{-3})^6$ خواهد شد.

اکنون با داشتن R'_{12} ، L'_{12} حالتی با بیشترین احتمال برای R_{13} ، L_{13} می‌خواهیم: L'_{13} به صورت تنها از R'_{12} به دست می‌آید و R'_{13} حاصل XOR L'_{12} با خروجی تابع f از R'_{12} می‌باشد. چون $R'_{12}=0$ ، خروجی f نیز 0 بوده و داریم

$R'_{13} = L'_{12} = 0x19600000 \Rightarrow P = 1$

پس بیشترین احتمال یک مشخصه تفاضلی زمانی رخ می‌دهد که مشخصه سوال قبل را ۶ بار تکرار کنیم و در دور ۱۳ نیز با $P=1$ رخ می‌دهد

$L'_i = 0x19600000 \ , \ R'_i = 0x00000000 \qquad i = 2k < 13$

$L'_i = 0x00000000 \ , \ R'_i = 0x19600000 \qquad i = 2k+1 \le 13$

$\max P = (4\times10^{-3})^6 \simeq \boxed{2^{-47.2}}$

٤- a) مقدار R'_2 را بر داده شده در نظر بگیریم و با f ای که در سؤال قبل بدست آمده آن را اثبات کنیم

$$\xrightarrow{R'_1} \boxed{f} \longrightarrow R'_0 \oplus R'_2$$

$$R'_1 = 0x20000000 = 0010\ 0000 \dots 0000$$

$$E(R'_1) = \underbrace{000100}_{S_1}\ \underbrace{000000}_{S_2}\ \dots\ \underbrace{000000}_{S_8}$$

ورودی

$$R'_0 \oplus R'_2 \overset{R'_0 = 0}{=\!=} \underset{\text{فرض سؤال}}{R'_2} = P(0x\overset{\text{مجهول}}{\delta}0000000)$$ خروجی S-Box ها به صورت $0x\delta0000000$ باشد

همان طور که از ورودی مشخص است، بجز اولی، سایر S-Box ها ورودی صفر دارند و نتیجتاً خروجی صفر نیز خواهند داشت

خروجی S-Box اول نیز مقدار δ خواهد بود. احتمال δ را از جدول بدست می‌آوریم:

$$P(000100 \to \delta) = P(4x \to \delta) \Rightarrow \begin{cases} P(\delta = 2x, 7x, Ax, Ex) = \frac{6}{64} \\ P(\delta = 5x, 6x) = \frac{10}{64} \\ P(\delta = 9x, Bx) = \frac{4}{64} \\ P(\delta = Dx) = \frac{8}{64} \\ \text{o.w.} = 0 \end{cases}$$

---

b)

$$R_1 = L_0 \oplus f(R_0, K_1) \quad (\mathrm{I}) \qquad R_2 = L_1 \oplus f(R_1, K_2) \quad (\mathrm{II})$$

$$R_3 = L_2 \oplus f(R_2, K_3) \quad (\mathrm{III})$$

$$R_4 = L_3 \oplus f(R_3, K_4) \overset{L_3 = R_2}{=\!=} R_2 \oplus f(R_3, K_4) \overset{(\mathrm{II})}{=\!=} L_1 \oplus f(R_1, K_2) \oplus f(R_3, K_4)$$

$$\overset{L_1 = R_0}{=\!=} R_0 \oplus f(R_1, K_2) \oplus f(R_3, K_4) \Rightarrow R_4 = R_0 \oplus f(R_1, K_2) \oplus f(R_3, K_4)$$

طبق جدول: $R''_4 = R''_0 \oplus f(R''_1, K_2) \oplus f(R''_3, K_4)$

$$\Rightarrow R'_4 = R_4 \oplus R''_4 = \underbrace{(R_0 \oplus R''_0)}_{R'_0} \oplus f(R_1, K_2) \oplus f(R''_1, K_2) \oplus f(R_3, K_4) \oplus f(R''_3, K_4)$$

$\xrightarrow[R'_4=0]{\text{از فرض سوال}}$ $R'_4 = \underbrace{f(R_1, K_2)}_{*} \oplus \underbrace{f(R'_1, K_2)}_{**} \oplus f(R_3, K_4) \oplus f(R''_3, K_4)$ ...

$(*)$: $f(R_1, K_2) \oplus L_1 = R_2 \xrightarrow{L_1 = R_0 = 0} f(R_1, K_2) = R_2$

مشابه $\Rightarrow f(R''_1, K_2) = R''_2$

$\Rightarrow R'_4 = \underset{R'_2}{\cancel{R_2 \oplus R''_2}} \oplus \underbrace{\underbrace{f(R_3, K_4)}_{:= P(C)} \oplus \underbrace{f(R''_3, K_4)}_{:= P(C'')}}_{= P(C')}$

$\Rightarrow P(C') = R'_4 \oplus R'_2 \Rightarrow \boxed{C' = P^{-1}(R'_4 \oplus R'_2)}$