

تحلیل خطی الگوریتم IES80

gh_ali_bk@yahoo.com

mdalian@yahoo.com

brenjkoub@yahoo.com

قدمعلی باقری کرم (دانشجوی کارشناسی ارشد دانشگاه صنعتی اصفهان)

محمد دخیل علیان (استادیار دانشگاه صنعتی اصفهان)

مهدی برنجکوب (استادیار دانشگاه صنعتی اصفهان)

چکیده: الگوریتم IES80، یک الگوریتم شبه DES می‌باشد و در این مقاله نتایج حمله خطی بر روی آن بررسی می‌شود. طول کلید این الگوریتم ۷۰ بیت می‌باشد اما خواهیم دید که اعمال تحلیل خطی به آن موجب کاهش فضای کلید به ۶۶ بیت می‌گردد که با صرف اندکی حافظه بیشتر این الگوریتم ۶۴ بیتی می‌شود.

کلمات کلیدی: IES80، تحلیل خطی

۱- مقدمه

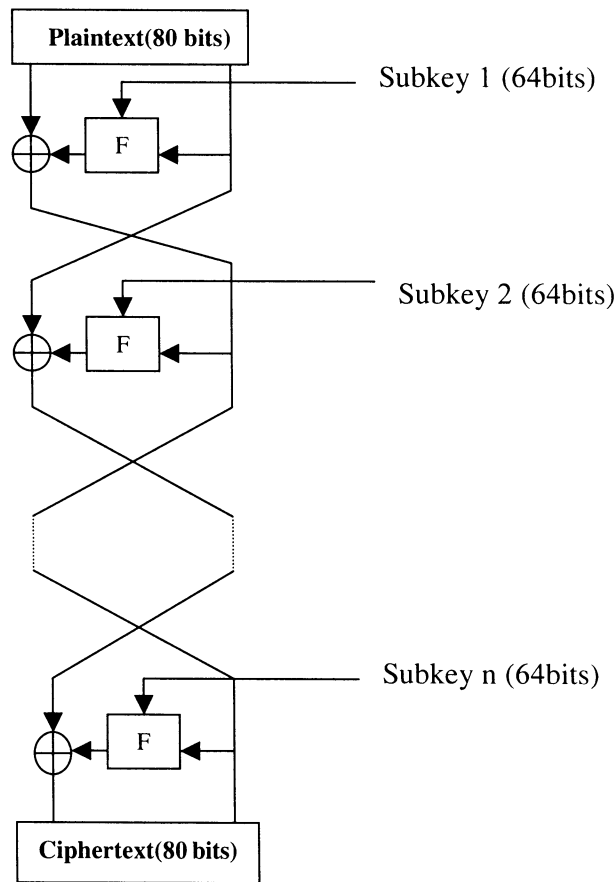
آقای ماتسونی در سال ۱۹۹۳ ایده تحلیل خطی به الگوریتم DES را مطرح کرد [۱] و در سال بعد موفق به شکستن DES ۱۶ دوری در مدت ۵۰ روز گردید [۲]. حمله خطی یک حمله متن اصلی معلوم است و هدف آن بدست آوردن یک تقریب خطی از الگوریتم رمز مربوطه است. برای این منظور باید به دنبال یک مسیر آماری بین ورودی و خروجی هر S-box بود سپس این مسیر را به کل الگوریتم تعمیم داد تا در نهایت به یک تقریب خطی مناسب رسید.

در این مقاله روش تحلیل خطی به الگوریتم IES80 - یکی از کاندیداهای مسابقه ارزیابی انجمن رمز ایران - اعمال می‌شود. نتایج این حمله روی IES80 به صورت زیر می‌باشد:

- ◆ IES80، ۸ دوری با 2^{28} متن اصلی معلوم قابل شکستن است.
- ◆ IES80، ۱۲ دوری با 2^{50} متن اصلی معلوم قابل شکستن است.
- ◆ IES80، ۱۶ دوری با 2^{66} متن اصلی معلوم، سریعتر از جستجوی کامل کلید، قابل شکستن است.
- ◆ با صرف اندکی حافظه بیشتر IES80، ۱۶ دوری با 2^{64} متن اصلی معلوم قابل شکستن است.

۲- ساختار کلی الگوریتم

شکل ۱ ساختار کلی الگوریتم IES80 را نشان می‌دهد. در این شکل جایگشت‌های اولیه IP و نهایی FP حذف شده‌اند زیرا ارزش امنیتی ندارند.



شکل ۱: ساختار کلی IES80 ، n دوری

۳- روش تحلیل خطی [۴۹]

ایده اصلی در تحلیل خطی ، پیدا کردن تقریبهایی خطی است که برای یک دور تابع بدست می‌آید و در نهایت منجر به پیدا شدن یک تقریب خطی از کل الگوریتم می‌گردد . مقدار $P_i \oplus P_{i_2} \oplus \dots \oplus P_{i_n}$ با $P[\chi_p]$ نمایش داده می‌شود و به همین ترتیب از این نمایش برای C ها و K ها استفاده می‌شود. بنابراین یک تقریب خطی به صورت زیر نوشته می‌شود:

$$P[\chi_p] \oplus C[\chi_c] = K[\chi_k] \quad (1)$$

اگر معادله (۱) با احتمال $P = \frac{1}{2} + \epsilon$ برای منتهای تصادفی ، صحیح باشد و کلید هم ثابت فرض شود ، در این صورت گفته می‌شود که این معادله دارای بایاس ϵ است. با جمع آوری زوج منتهای اصلی و منتهای رمز شده ، می‌توان مقدار $K[\chi_k]$ را در صورتی که $\epsilon \neq 0$ باشد ، حدس زد. در این صورت هرچه تعداد منتهای اصلی ، بیشتر باشد ، حدس کلید با احتمال بالاتری انجام می‌شود.

اگر $K[\chi_k] = 1$ باشد مقدار متوسط مورد انتظار برای سمت چپ معادله $\frac{1}{2} + \epsilon$ است و اگر $K[\chi_k] = 0$ باشد ، برابر $\frac{1}{2} - \epsilon$ است .

باید توجه شود که بین توزیع با میانگین $\frac{1}{2} + \epsilon$ و واریانس $\frac{1}{4} - \epsilon^2$ و توزیع با میانگین $\frac{1}{2} - \epsilon$ و واریانس $\frac{1}{4} - \epsilon^2$ تفاوت گذاشت . یک تحلیلگر باید به تعداد کافی زوج متن اصلی و متن رمز شده در اختیار داشته باشد تا بین این دو توزیع تفاوت قابل شود . هرچه ϵ کوچکتر باشد ، برای رسیدن به یک درجه اطمینان مشخص ، تعداد زوج منتهای اصلی و رمز شده بیشتری نیاز است . الگوریتم اساسی که موجب مشخص شدن یک بیت از کلید از روی یک تقریب خطی می‌شود ، با الگوریتم ۱ مشخص می‌شود .

الگوریتم ۱: فرض کنید معادله (۱) با احتمال $\frac{1}{2} + \epsilon$ صحیح باشد.

گام ۱: T به صورت تعداد زوجهای متنهای اصلی و رمز شده ای که سمت چپ معادله (۱) را صفر می کنند، تعریف می شود. N تعداد کل زوج متنهای است.

گام ۲: اگر $T > N/2$ در این صورت

$$K[\chi_k] = \begin{cases} 0 & \epsilon > 0 \\ 1 & \epsilon < 0 \end{cases}$$

در غیر اینصورت

$$K[\chi_k] = \begin{cases} 1 & \epsilon > 0 \\ 0 & \epsilon < 0 \end{cases}$$

الگوریتمی که از نظر عملی مهمتر است، الگوریتم ۲ می باشد که به شخص تحلیلگر اجازه می دهد که در IES80، ۱۶ دوری ۱۷ بیت از کلید را مشخص کند. به طور کلی برای یک الگوریتم فیستلی r دوری باید $r-2$ دور آنرا، از دور ۲ تا $r-1$ ام تقریب زد و سپس تعدادی از بیتهای زیر کلیدهای اول و آخر را حدس زد. برای آنکه تعداد کاندیداهای زیر کلیدها زیاد نشود بهتر است زیر کلیدهای مربوط به یک S-box حدس زده شود.

تقریب خطی مربوطه می تواند به صورت زیر نوشته شود:

$$P[\chi_p] \oplus C[\chi_c] \oplus F_1(P_1, K_1)[\chi_{F_1}] \oplus F_r(C_r, K_r)[\chi_{F_r}] = K[\chi_k] \quad (2)$$

فرض می شود که معادله (۲) با احتمال $P = \frac{1}{2} + \epsilon$ صحیح باشد.

الگوریتم ۲: گام ۱: اگر $K_1^{(g)}$ ($g = 1, 2, \dots$) و $K_r^{(h)}$ ($h = 1, 2, \dots$) به ترتیب کاندیداهای ممکن باشند در این صورت برای هر زوج $(K_1^{(g)}, K_r^{(h)})$ ، $T_{g,h}$ به صورت تعداد متنهای اصلی ای که سمت چپ معادله (۲) را صفر می کنند، تعریف می شود. N نیز تعداد کل متنها در نظر گرفته می شود.

گام ۲: اگر T_{\max} ماکزیمم مقدار $T_{g,h}$ ها و T_{\min} مینیمم مقدار آن باشد:

اگر $\left| T_{\max} - \frac{N}{2} \right| > \left| T_{\min} - \frac{N}{2} \right|$ باشد زیر کلیدهای مربوط به T_{\max} قابل قبول اند و

$$K[\chi_k] = \begin{cases} 0 & \epsilon > 0 \\ 1 & \epsilon < 0 \end{cases}$$

اگر $\left| T_{\max} - \frac{N}{2} \right| < \left| T_{\min} - \frac{N}{2} \right|$ باشد زیر کلیدهای مربوط به T_{\min} قابل قبول اند و

$$K[\chi_k] = \begin{cases} 1 & \epsilon > 0 \\ 0 & \epsilon < 0 \end{cases}$$

الگوریتم ۲ یک حدسی برای زیر کلیدهای K_1 و K_r به دست می دهد و همچنین اطلاعاتی در مورد یک بیت سمت راست می دهد. ماتسوئی

نشان داده است که با $8\epsilon^{-2}$ زوج متن اصلی و رمز شده می توان با استفاده از الگوریتم ۲ با احتمال صحت بالایی به بیتهایی از کلید رسید [۱]. برای بدست آوردن بیتهای بیشتر، می توان یک تقریب خطی دیگر که با جابجا کردن نقش P ها و C ها بدست می آید، دوباره الگوریتم ۲ را اعمال کرد. با استفاده از روش فوق می توان به ۳۴ بیت از کلید IES80، ۱۶ دوری رسید. اگر تولید زیر کلیدها طوری باشد که این ۳۴ بیت از زیرکلید معادل ۳۴ بیت کلید اصلی باشد در اینصورت بقیه ۳۶ بیت دیگر را می توان از روش جستجوی کامل بدست آورد.

۴- تقریب خطی از S-box ها

در این قسمت به مطالعه تقریب خطی برای S-box ها پرداخته می شود. اولین هدف، بدست آوردن احتمالی است که یک مقدار از بیت ورودی با مقداری از بیت خروجی مطابقت کند. به طور کلی تر بهتر است نه تنها بر روی یک بیت بحث شود بلکه روی XOR شده چند بیت بحث شود.

تعریف: برای یک S-box مشخص S_a ، $1 \leq \alpha \leq 255$ و $1 \leq \beta \leq 31$ عبارت $NS_a(\alpha, \beta)$ عبارت است از تعداد دفعاتی از ۲۵۶ ورودی ممکن S_a که یک مقدار XOR شده ورودی که با α ماسک شده است، با یک مقدار XOR شده خروجی که با β ماسک شده است، مطابقت کند یعنی:

$$NS_a(\alpha, \beta) = \# \left\{ x \mid 0 \leq x \leq 255, \left(\bigoplus_{s=0}^8 (x[s] \cdot \alpha[s]) \right) = \left(\bigoplus_{t=0}^5 (S_a(x)[t] \cdot \beta[t]) \right) \right\} \quad (3)$$

که علامت • مشخص کننده AND بیت با بیت است [۱]، مثلاً

$$\forall a \quad NS_a(4,16) = 199 \quad (4)$$

هنگامیکه $NS_a(\alpha, \beta)$ برابر با ۱۲۸ نیست در این صورت یک همبستگی بین ورودی و خروجی S_a وجود دارد. مثلاً معادله (۴) بیان می کند که

بیت دوم S_a با بیت چهارم S_a با احتمال $\frac{199}{256} = 0.78$ مطابقت دارد. در نتیجه با توجه به ساختار تابع F و با توجه به جداول E و P داریم:

$$X[3] \oplus F(X, K)[9] = K[6] \quad P = 0.78 \quad (5)$$

جدول ۱ قسمتی از توزیع جدول S_a را نشان می دهد که محورهای عمودی و افقی به ترتیب مشخص کننده α و β هستند و هر عدد در جدول $NS_a(\alpha, \beta) - 128$ را نشان می دهد. جدول کامل این S-box ها نشان می دهد که معادله (۴) بهترین تقریب خطی در تمام S-box ها است. (یعنی $|NS_a(\alpha, \beta) - 128|$ ماکزیمم است) بنابراین معادله (۵) بهترین تقریب از تابع F است.

۵- تقریب خطی الگوریتم IES80

در این قسمت تقریب خطی تابع F به کل الگوریتم تعمیم داده می شود. اولین مثال IES80، ۳ دوری است. با اعمال معادله (۵) به دور اول

رابطه زیر با احتمال $P = \frac{199}{256}$ برقرار است:

$$X_2[9] \oplus P_H[9] \oplus P_L[3] = K_1[6] \quad (6)$$

به همین ترتیب:

$$X_2[9] \oplus C_H[9] \oplus C_L[3] = K_3[6] \quad (7)$$

در نتیجه به تقریب خطی زیر برای IES80، ۳ دوری می رسمیم:

$$P_H[9] \oplus C_H[9] \oplus P_L[3] \oplus C_L[3] = K_1[6] \oplus K_3[6] \quad (8)$$

احتمال اینکه معادله (۸) برای متنهای تصادفی P و متنهای رمز شده نظیر C برقرار باشد برابر است با $0.65 = \left(\frac{199}{256}\right)^2 + \left(1 - \frac{199}{256}\right)^2$. چونکه

معادله (۵) بهترین تقریب خطی از تابع F است بنابراین معادله (۸) نیز بهترین عبارت برای IES80، ۳ دوری است. حال می توان معادله (۸) را با استفاده از الگوریتم ۱ حل کرد تا به $K_1[6] \oplus K_3[6]$ رسید. لم زیر نرخ موفقیت این روش را بیان میکند.

جدول ۱: قسمتی از جدول توزیع S_n

۳	۱	-۹	-۵۷	۱	۳	-۳	۵	۷	۱	-۵	-۱	۱۳	۳	-۷
-۵	-۱	-۱	-۲۳	۱	-۳	۱۳	۱۱	۱۱	۳	-۵	۹	۱	۱	۱
۱۲	-۶	-۴	-۲۲	۱۶	-۶	۱۶	۲	۱۶	-۲	-۱۲	-۶	۱۲	-۲	-۸
۳	-۵	۹	-۷	-۱۳	-۵	-۳	۱۱	۱	-۷	-۱	-۵	-۱۱	-۳	۷
۱۲	-۶	-۱۴	-۶	-۶	-۴	-۲۰	۶	۱۰	-۴	۰	-۱۶	۴	۲	۶
۱۲	-۴	۶	-۱۶	-۱۸	۶	-۱۲	۱۶	-۶	-۱۰	-۸	۱۸	-۸	-۴	۱۰
۱۱	-۱۱	۵	-۱۳	-۲۱	۱	-۷	-۳	۱	-۵	-۱۷	-۷	۵	۳	-۱
-۹	-۳	۵	-۲۷	۹	۳	-۵	-۹	-۱	۱	۵	-۷	۱	-۱	-۵
۰	-۴	۱۰	-۱۴	۱۶	۴	۶	-۶	-۴	۰	۶	-۱۰	۴	۰	-۶
-۸	-۶	۲	۰	-۱۲	۲	۱۰	-۱۶	-۱۶	۱۰	۶	-۴	-۱۲	۲	-۲
-۵	-۱	-۷	-۱۳	-۱۱	۹	۷	-۷	-۱	۷	۹	-۱	۹	۱	-۱
۱۲	-۲	۴	-۱۶	۶	-۴	-۲	۱۲	-۱۴	۰	۲	-۱۰	-۸	۲	-۸
-۱	-۱	-۱	-۵	-۹	-۱	-۱	۱۷	-۳	-۳	۵	-۱۱	۹	۱	-۷
۳	-۳	۷	-۱۵	-۵	۱	-۹	-۱	۹	-۱۳	-۷	-۱	-۳	-۵	-۳
۰	-۴	-۴	-۱۴	-۱۰	۲	-۱۴	۲	-۲	-۲	-۲	-۴	-۸	۸	۰
-۵	-۳	۳	۷۱	-۳	۳	۵	-۹	۱۳	-۱	-۷	-۷	۱۱	۱	-۱

لم ۱ [۱]: اگر N تعداد منتهای اصلی تصادفی و P احتمال برقراری رابطه (۱) باشد، فرض کنید $|P - 1/2|$ به اندازه کافی کوچک است، در این صورت نرخ موفقیت الگوریتم ۱ عبارت است از:

$$\int_{-2\sqrt{N}|P-1/2|}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} dx \quad (9)$$

جدول (۲) حل عددی معادله (۹) را نشان می دهد:

جدول ۲: نرخ موفقیت الگوریتم ۱

N	$1/4 P-1/2 ^{-2}$	$1/2 P-1/2 ^{-2}$	$ P-1/2 ^{-2}$	$2 P-1/2 ^{-2}$
Success Rate	%۸۴.۱	%۹۲.۱	%۹۷.۷	%۹۹.۸

حال به یک IES80، ۵ دوری پرداخته می شود. در این مورد معادله (۵) به دورهای دوم و چهارم اعمال می شود و معادله خطی زیر به دورهای اول و آخر اعمال می شود.

$$NS_n(4,16) = 199 \Rightarrow X[8] \oplus F(X, K)[3] = K[14] \quad (10)$$

با محاسبات خطی ساده ای به عبارت تقریبی خطی زیر برای IES80، ۵ دوری می رسم:

$$P_H[3] \oplus P_L[9,8] \oplus C_H[3] \oplus C_L[9,8] = K_1[14] \oplus K_2[6] \oplus K_4[6] \oplus K_5[14] \quad (11)$$

لم بعدی روش ساده ای برای محاسبه احتمال اینکه اینگونه معادلات صادق باشند را بیان می کند.

لم ۲ [۱]: اگر X_i ها متغیرهای تصادفی مستقل باشند که مقادیر آنها با احتمال P_i برابر صفر و با احتمال $1 - P_i$ برابر یک

باشد، در این صورت احتمال اینکه $X_1 \oplus X_2 \oplus \dots \oplus X_n = 0$ باشد عبارت است از:

$$\frac{1}{2} + 2^{n-1} \prod_{i=1}^n (P_i - \frac{1}{2}) \quad (12)$$

۱. piling-up lemma

این لم بیان می کند که معادله (۱۱) با احتمال $\frac{1}{2} + 2^3 \left(\frac{71}{256}\right)^2 \left(\frac{71}{256}\right)^2 = 0.547$ صادق است. بنابراین مطابق لم ۱ اگر

$$|0.547 - 1/2|^{-2} = 446$$

متن اصلی معلوم داده شود، می توان سمت راست معادله (۱۱) را با نرخ موفقیت ۹۷.۷٪ حدس زد.

در جدول ۳ بهترین عبارتها و احتمالات نظیر آنها برای IES80 n دوری ($3 \leq n \leq 20$) آمده است. این جدول با استفاده از الگوریتم مرجع [۳] بدست آمده است. در این جدول از چپ به راست تعداد دورها، بهترین عبارت، بهترین احتمال و تقریب خطی تابع F در هر دور آمده است. علامت - نشان می دهد که هیچ تقریبی نیاز نیست. دقت کنید که در برخی موارد دو تقریب خطی داریم که با علامت * مشخص شده

است. از این جدول مشاهده می شود که دو بیت IES80، ۱۶ دوری با نرخ صحت بالایی با $2^{66} \approx |1.44 \times 2^{-33}|^{-2}$ متن اصلی معلوم. حدس زده می شود. در قسمت بعد روشی ارائه می شود که می توان نهایتاً به ۱۸ بیت کلید با استفاده از حافظه کمی رسید.

جدول ۳: بهترین عبارتها و بهترین احتمالات نظیر IES80

3	$P_H[9] \oplus P_L[3] \oplus C_H[9] \oplus C_L[3]$ $= K_1[6] \oplus K_3[6]$	$1/2 - 1.23 \times 2^{-3}$	A-A
*4	$P_H[9] \oplus P_L[3] \oplus C_H[9] \oplus C_L[3,8]$ $= K_1[6] \oplus K_3[6] \oplus K_4[14]$	$1/2 - 1.36 \times 2^{-4}$	A-AB
5	$P_H[3] \oplus P_L[8,9] \oplus C_H[3] \oplus C_L[8,9]$ $= K_1[14] \oplus K_2[6] \oplus K_4[6] \oplus K_5[14]$	$1/2 - 1.51 \times 2^{-5}$	BA-AB
*6	$P_L[10] \oplus C_H[9] \oplus C_L[3]$ $= L_2 \oplus K_6[6]$	$1/2 - 1.62 \times 2^{-13}$	-DCA-A
*7	$P_H[10] \oplus P_L[1] \oplus C_H[9] \oplus C_L[3]$ $= K_1[4] \oplus L_3 \oplus K_7[6]$	$1/2 - 1.23 \times 2^{-13}$	E-DCA-A
*8	$P_H[10] \oplus P_L[1] \oplus C_H[3] \oplus C_L[8,9]$ $= K_1[4] \oplus L_3 \oplus K_7[6] \oplus K_8[14]$	$1/2 - 1.51 \times 2^{-16}$	E-DCA-AB
*9	$P_H[3] \oplus P_L[8,9] \oplus C_H[3] \oplus C_L[8,9]$ $= K_1[14] \oplus K_2[6] \oplus L_4 \oplus K_8[6] \oplus K_9[10]$	$1/2 - 1.74 \times 2^{-19}$	BD-DCA-AB
*10	$P_L[9] \oplus C_H[9] \oplus C_L[3]$ $= L_2 \oplus L_5 \oplus K_{10}[6]$	$1/2 - 1.17 \times 2^{-23}$	-ACD-DCA-A
11	$P_H[9] \oplus P_L[3] \oplus C_H[9] \oplus C_L[3]$ $= K_1[6] \oplus L_3 \oplus L_7 \oplus K_{11}[6]$	$1/2 - 1.3 \times 2^{-24}$	A-ACD-DCA-A
*12	$P_H[9] \oplus P_L[3] \oplus C_H[3] \oplus C_L[8,9]$ $= K_1[6] \oplus L_3 \oplus L_7 \oplus K_{11}[6] \oplus K_{12}[14]$	$1/2 - 1.44 \times 2^{-25}$	A-ACD-DCA-AB

13	$P_H[3] \oplus P_L[8,9] \oplus C_H[3] \oplus C_L[8,9]$ $= K_1[14] \oplus K_2[6] \oplus L_4 \oplus L_8 \oplus K_{12}[6] \oplus K_{13}[14]$	$1/2 - 1.6 \times 2^{-26}$	BA-ACD- DCA-AB
*14	$P_L[10] \oplus C_H[9] \oplus C_L[3]$ $= L_2 \oplus L_6 \oplus L_{10} \oplus K_{14}[6]$	$1/2 - 1.71 \times 2^{-32}$	-DCA- ACD- DCA-A
*15	$P_H[10] \oplus P_L[1] \oplus C_H[9] \oplus C_L[3]$ $= K_1[4] \oplus L_3 \oplus L_7 \oplus L_{11} \oplus K_{15}[6]$	$1/2 - 1.44 \times 2^{-33}$	E-DCA- ACD- DCA-A
*16	$P_H[10] \oplus P_L[1] \oplus C_H[3] \oplus C_L[8,9]$ $= K_1[4] \oplus L_3 \oplus L_7 \oplus L_{11} \oplus K_{15}[6] \oplus K_{16}[14]$	$1/2 - 1.59 \times 2^{-37}$	A-ACD- DCA- ACD- DCA-AB
*17	$[3] \oplus P_L[8,10] \oplus C_H[3] \oplus C_L[8,9]$ $K_1[14] \oplus K_2[6] \oplus L_4 \oplus L_8 \oplus L_{12} \oplus K_{16}[6] \oplus K_{17}[14]$	$1/2 - 1.84 \times 2^{-39}$	BD-DCA- ACD- DCA-AB
*18	$P_L[9] \oplus C_H[9] \oplus C_L[3]$ $= L_2 \oplus L_6 \oplus L_{10} \oplus L_{14} \oplus K_{18}[6]$	$1/2 - 1.24 \times 2^{-43}$	-ACD- DCA- ACD- DCA-A
19	$P_H[9] \oplus P_L[3] \oplus C_H[9] \oplus C_L[3]$ $= K_1[6] \oplus L_3 \oplus L_7 \oplus L_{11} \oplus L_{15} \oplus K_{19}[6]$	$1/2 - 1.38 \times 2^{-44}$	A-ACD- DCA- ACD- DCA-A
*20	$P_H[9] \oplus P_L[3] \oplus C_H[3] \oplus C_L[8,9]$ $= K_1[6] \oplus L_3 \oplus L_7 \oplus L_{11} \oplus L_{15} \oplus K_{19}[6] \oplus K_{20}[14]$	$1/2 - 1.53 \times 2^{-45}$	A-ACD- DCA- ACD- DCA-AB

$$A: X[3] \oplus F(X, K)[9] = K[6] \quad p = 1/2 + 71/256$$

$$B: X[8] \oplus F(X, K)[3] = K[14] \quad p = 1/2 + 71/256$$

$$C: X[9,10] \oplus F(X, K)[3] = K[15,16] \quad p = 1/2 + 3/256$$

$$D: X[3] \oplus F(X, K)[10] = K[6] \quad p = 1/2 + 7/256$$

$$E: X[1] \oplus F(X, K)[10] = K[4] \quad p = 1/2 + 27/256$$

$$L_i: K_i[6] \oplus K_{i+1}[15,16] \oplus K_{i+2}[6]$$

۶- حمله متن اصلی معلوم روی IES80

اکنون می‌توان حمله متن اصلی معلوم را به IES80 اعمال کرد. اولین مثال در مورد IES80، ۸ دوری است. همانطور که در قسمت ۳ بیان

شد، عبارت زیر را برای IES80، ۸ دوری با استفاده از IES80، ۷ دوری با احتمال $0.5 + 1.23 \times 2^{-13}$ داریم:

$$P_H[10] \oplus P_L[1] \oplus C_H[3] \oplus C_L[9] \oplus F_8(C_L, K_8)[3]$$

$$= K_1[4] \oplus K_3[6] \oplus K_4[15,16] \oplus K_5[6] \oplus K_7[6]$$

(۱۳)

هر چند که این معادله شامل ۶۴ زیر کلید K_8 است ولی تعداد بیت‌های کلیدی که در به دست آوردن $F_8(C_L, K_8)[3]$ موثرند، ۸ بیت اند. بنابراین به ۲۵۶ شمارنده نیاز است تا اینکه الگوریتم ۲ را انجام داد. لم زیر که در واقع حالت کلی تر لم ۲ است در مورد نرخ موفقیت بحث می کند لم ۳ [۱]: اگر N تعداد متنهای اصلی تصادفی باشد و P احتمال این باشد که معادله (۲) برقرار باشد و فرض کنیم $|P - 1/2|$ به اندازه کافی کوچک است در این صورت نرخ موفقیت الگوریتم ۲ به l_1, l_2, \dots, l_d و $\sqrt{N}|P - 1/2|$ بستگی دارد.

در شرایط خاص لم (۴) را داریم:

لم ۴ [۱]: با همان شرایط لم (۳) اگر $q^{(i)}$ احتمال صحت رابطه زیر برای یک کاندید $K_n^{(i)}$ باشد و X یک متغیر تصادفی باشد

$$F_n(X, K_n)[l_1, l_2, \dots, l_d] = F_n(X, K_n^{(i)})[l_1, l_2, \dots, l_d] \quad (14)$$

در این صورت اگر $q^{(i)}$ ها مستقل باشند، نرخ موفقیت الگوریتم ۲ عبارت است از:

$$\int_{x=-2\sqrt{N}|P-1/2|}^{\infty} \left(\prod_{K_n^{(i)} \neq K_n} \int_{x-4\sqrt{N}(P-1/2)q^{(i)}}^{x+4\sqrt{N}(P-1/2)(1-q^{(i)})} \frac{1}{\sqrt{2\pi}} e^{-y^2/2} dy \right) \frac{1}{\sqrt{2\pi}} e^{-x^2/2} dx \quad (15)$$

که حاصلضرب روی تمام کاندیدهای کلید فرعی $K_n^{(i)}$ به جز خود K_n انجام می شود.

هرچند که $q^{(i)}$ ها در همه شرایط مستقل نیستند، ولی نتایج عملی نشان داده است که لم ۴ یک تقریب خوبی برای نرخ موفقیت بدست می

دهد. همان طور که در جدول ۴ مشاهده می شود:

اگر در معادله (۱۴) $l_1 = 3, d = 1$ محاسبات عددی عبارت (۱۵) به صورت زیر است:

جدول ۴: نرخ موفقیت الگوریتم ۲

N	$2 P-1/2 ^{-2}$	$4 P-1/2 ^{-2}$	$8 P-1/2 ^{-2}$	$16 P-1/2 ^{-2}$
Success Rate	%۴۸.۶	%۷۸.۵	%۹۶.۷	%۹۹.۹

اگر الگوریتم ۲ روی دوگان معادله (۱۳) نیز به کار گرفته شود در نهایت با استفاده از حافظه کوچکی ۱۶ بیت کلید فرعی بدست می آید. در این صورت باید سایر بیت‌های کلید را با جستجو بدست آورد. نتایج عملی با کامپیوتر به نتایج بهتر از جدول (۴) ختم شده است. با استفاده از

$$4|1.23 \times 2^{-13}|^{-2} \cong 2^{27}$$

متن اصلی معلوم، کل سیستم شکسته می شود. نرخ موفقیت %۸۸ است.

روش شکستن IES80، ۱۲ دوری هم مشابه ۸ دوری است. با استفاده از $8|1.3 \times 2^{-24}|^{-2} \cong 2^{50}$ متن اصلی معلوم می توان آنرا شکست

به طور مشابه مطابق لم ۴، می توان IES80، ۱۶ دوری را با استفاده از $8|1.44 \times 2^{-33}|^{-2} \cong 2^{66}$ متن اصلی معلوم، با حل عبارت زیر شکست:

$$P_H[10] \oplus P_L[1] \oplus C_H[3] \oplus C_L[9] \oplus F_{16}(C_L, K_{16})[3] \\ = K_1[4] \oplus K_3[6] \oplus K_4[15,16] \oplus K_5[6] \oplus K_7[6] \oplus K_8[15,16] \oplus K_9[6] \oplus \\ K_{11}[6] \oplus K_{12}[15,16] \oplus K_{13}[6] \oplus K_{15}[6] \quad (16)$$

البته توجه کنید که با حل عبارت فوق ۹ بیت از کلید بدست می آید و با حل دوگان معادله فوق ۹ بیت دیگر از کلید مشخص میشود. وقتی

۱۸ بیت از کلید مشخص شد، بقیه ۵۲ بیت از کلید باید با جستجوی کامل بدست آید. بنابراین می توان IES80، ۱۶ دوری را با حافظه کمی خیلی

سریعتر از جستجوی کامل شکست. حال یک روش دیگر برای شکستن IES80، ۱۶ دوری مطرح می شود.

در این قسمت یک مدل بهبود یافته از حمله خطی ارائه می شود. این حمله از نوع متن اصلی معلوم است که بر مبنای دو تقریب خطی

جدید، استوار است و هر معادله منجر به تعیین ۱۷ بیت کلید با استفاده از حافظه کمی، می شود. در نتیجه IES80، ۱۶ دوری با نرخ موفقیت

بزرگی با مشخص بودن 2^{11} متن اصلی معلوم و متنهای رمز شده نظیر، شکسته میشود.

در روش قبل از دو معادله تقریبی خطی برای IES80، ۱۶ دوری استفاده شد که این معادلات از بهترین عبارت خطی برای IES80، ۱۵ دوری

بدست می آیند. هر معادله شامل یک S-box فعال است و در نتیجه ۹ بیت کلید را بدست می دهد. در روش جدید از دو تقریب خطی جدید که از

بهترین عبارت برای IES80، ۱۴ دوری بدست می آیند، استفاده می شود که هر معادله دو S-box فعال را شامل می شود. در نتیجه ۱۷ بیت کلید را

بدست می دهد. در نتیجه این معادلات ۳۴ بیت کلید را مشخص می کنند و بقیه $36 - 34 = 2$ بیت کلید باید توسط جستجوی کامل مشخص شوند.

در روش جدید از دو معادله زیر که برای IES80، ۱۴ دوری با احتمال $1/2 + 1.71 \times 2^{-32}$ برقرار است، استفاده می شود:

$$P_L[10] \oplus C_H[9] \oplus C_L[3] = K_2[6] \oplus K_3[15,16] \oplus K_4[6] \oplus K_6[6] \oplus K_7[15,16] \oplus K_8[6] \oplus K_{10}[6] \oplus K_{11}[15,16] \oplus K_{12}[6] \oplus K_{14}[6] \quad (17)$$

$$C_L[10] \oplus P_H[9] \oplus P_L[3] = K_{13}[6] \oplus K_{12}[15,16] \oplus K_{11}[6] \oplus K_9[6] \oplus K_8[15,16] \oplus K_7[6] \oplus K_5[6] \oplus K_4[15,16] \oplus K_3[6] \oplus K_1[6] \quad (18)$$

حال معادلات (۱۷) و (۱۸) را به دورهای دوم تا پانزدهم یک IES80، ۱۶ دوری اعمال می شود. در نتیجه معادلات زیر را برای IES80، ۱۶ دوری متناظر با متناهی تصادفی P و C با احتمال $1/2 - 1.71 \times 2^{-32}$ داریم:

$$P_H[10] \oplus F_1(P_L, K_1)[10] \oplus C_H[3] \oplus C_L[9] \oplus F_{16}(C_L, K_{16})[3] = K_3[6] \oplus K_4[15,16] \oplus K_5[6] \oplus K_7[6] \oplus K_8[15,16] \oplus K_9[6] \oplus K_{11}[6] \oplus K_{12}[15,16] \oplus K_{13}[6] \oplus K_{15}[6] \quad (19)$$

$$C_H[10] \oplus F_{16}(C_L, K_{16})[10] \oplus P_H[3] \oplus P_L[9] \oplus F_1(P_L, K_1)[3] = K_{14}[6] \oplus K_{13}[15,16] \oplus K_{12}[6] \oplus K_{10}[6] \oplus K_9[15,16] \oplus K_8[6] \oplus K_6[6] \oplus K_5[15,16] \oplus K_4[6] \oplus K_2[6] \quad (20)$$

اولین مرحله از حمله. حل معادلات فوق است تا اینکه تعدادی از ۷۰ بیت کلید مشخص شوند. حال اگر با استفاده از الگوریتم ۲ اقدام به حل معادلات (۱۹) و (۲۰) شود در نهایت ۳۴ بیت از کلید اصلی بدست می آید. بقیه ۳۶ بیت از کلید را باید با استفاده از جستجوی کامل بدست آورد.

۷- جمع بندی و نتیجه گیری

در این مقاله ما به بررسی حمله خطی بر روی الگوریتم IES80 پرداختیم و مشاهده کردیم که جدول $|NS_n(\alpha, \beta) - 128|$ مربوط به S-box دارای توزیع یکسان نمی باشد. همین مطلب باعث کاهش فضای جستجوی کلید از 2^{70} به 2^{64} شد.

مراجع

- [1] Matsui, M. "Linear cryptanalysis method for DES cipher", *Advances in Cryptology-Eurocrypt 93, Lecture Notes in Computer Science*, Springer-Verlag 765, pp. 386-397, 1993.
- [2] Matsui, M. "The first experimental cryptanalysis of the Data Encryption Standard", *Advances in Cryptology-Eurocrypt 94, Lecture Notes in Computer Science*, Springer-Verlag, pp. 1-11, 1994.
- [3] Matsui, M. "On correlation between the order of S-boxes and the strength of DES", *Advances in Cryptology-Eurocrypt 94, Lecture Notes in Computer Science*, Springer-Verlag, pp. 366-375, 1994.