تحلیل خطی الگوریتم IES80

قدمعلی باقری کرم (دانشجوی کارشناسی ارشد دانشگاه صنعتی اصفهان) gh_ali_bk@yahoo.com
محمد دخیل علیان (استادیار دانشگاه صنعتی اصفهان) mdalian@yahoo.com
مهدی برنجکوب (استادیار دانشگاه صنعتی اصفهان) brenjkoub@yahoo.com

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 ٦٦ بیت می‌گردد که با صرف اندکی حافظه بیشتر این الگوریتم ٦٤ بیتی می‌شود.

کلمات کلیدی : IES80 ،تحلیل خطی

۱- مقدمه

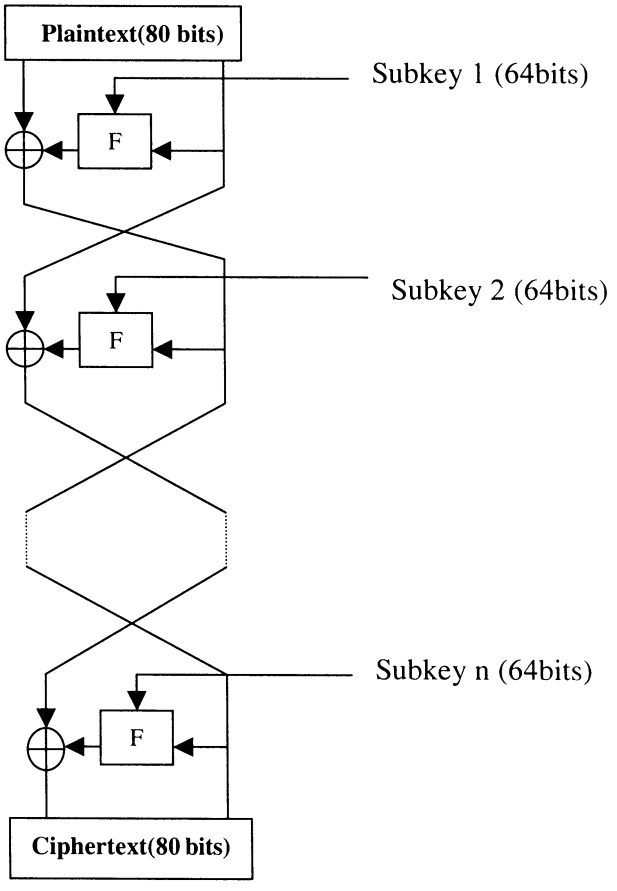
آقای ماتسوئی در سال ۱۹۹۳ ایده تحلیل خطی به الگوریتم DES را مطرح کرد[۱] و در سال بعد موفق به شکستن DES، ١٦ دوری در مدت ۵۰ روز گردید[۲]. حمله خطی یک حمله متن اصلی معلوم است و هدف آن بدست آوردن یک تقریب خطی از الگوریتم رمز مربوطه است. برای این منظور باید به دنبال یک مسیر آماری بین ورودی و خروجی هر S-box بود سپس این مسیر را به کل الگوریتم تعمیم داد تا در نهایت به یک تقریب خطی مناسب رسید.

در ایـن مقالـه روش تحلیل خطی به الگوریتم IES80 –یکی از کاندیداهای مسابقه ارزیابی انجمن رمز ایران- اعمال می‌شود . نتایج این حمله روی IES80 به صورت زیر می باشد:

- 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 ، ١٦ دوری با 2^{66} متن اصلی معلوم،سریعتر از جستجوی کامل کلید، قابل شکستن است.
- با صرف اندکی حافظه بیشتر IES80 ، ١٦ دوری با 2^{64} متن اصلی معلوم قابل شکستن است.

۲- ساختارکلی الگوریتم

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



شکل ۱ : ساختار کلی IES80 ، n دوری

۳- روش تحلیل خطی[۱و۴]

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 ازکل الگوریتم می‌گردد . مقدار $P_{i_1} \oplus P_{i_2} \oplus .... \oplus P_{i_a}$ با $P[\chi_p]$ نمایش داده می‌شود و به همین ترتیب از این نمایش برای Cها و K ها استفاده می‌شود.بنابراین یک تقریب خطی به صورت زیر نوشته می‌شود:

$$P[\chi_p] \oplus C[\chi_c] = K[\chi_k] \qquad (۱)$$

اگر معادله (۱) با احتمال $P = \frac{1}{2} + \varepsilon$ برای متنهای 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 متنهای اصلی و متنهای رمز شده ، می‌توان مقدار $K[\chi_k]$ را در صورتی که $\varepsilon \neq 0$ باشد ، حدس زد. در این صورت هرچه تعداد متنهای اصلی ، بیشتر باشد ، حدس کلید با احتمال بالاتری انجام می‌شود.

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

باید توجه شود که بین توزیع با میانگین $\frac{1}{2} + \varepsilon$ و واریانس $\frac{1}{4} - \varepsilon^2$ و توزیع با میانگین $\frac{1}{2} - \varepsilon$ و واریانس $\frac{1}{4} - \varepsilon^2$ 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 قایل شود . هرچه ε کوچکتر باشد ، برای رسیدن به یک درجه اطمینان مشخص، تعداد زوج متنهای 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 $\frac{1}{2}+\varepsilon$ صحیح باشد .

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

گام ۲ : اگر $T > N/2$ در این صورت

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

در غیر اینصورت

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

الگوریتمی که از نظر عملی مهمتر است ، الگوریتم ۲ می‌باشد که به شخص تحلیلگر اجازه می‌دهد 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 ام 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 می‌تواند به صورت زیر نوشته شود :

$$P[\chi_p]\oplus C[\chi_c]\oplus F_1(P_l,K_1)[\chi_{F_1}]\oplus F_r(C_l,K_r)[\chi_{F_r}]=K[\chi_k] \qquad (۲)$$

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

الگوریتم ۲ : گام ۱ : اگر $K_1^{(g)}(g=1,2,...)$ و $K_r^{(h)}(h=1,2,...)$ 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 ایی که سمت چپ معادله (۲) را صفر می‌کنند ، تعریف می‌شود. N نیز تعداد کل متنها در نظر گرفته می‌شود .

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 قبول‌اند و

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

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

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

الگوریتم ۲ یک حدسی برای زیر کلیدهای K_1 و K_r به دست می‌دهد و همچنین اطلاعاتی در مورد یک بیت سمت راست می‌دهد . ماتسوئی نشان داده است که با $8\varepsilon^{-2}$ زوج متن اصلی و رمز شده می‌توان با استفاده از الگوریتم ۲ با احتمال صحت بالایی به بیتهایی از کلید رسید[۱] . برای بدست آوردن بیتهای بیشتر ، می‌توان یک تقریب خطی دیگر که با جابجا کردن نقش P ها و C ها بدست می‌آید ، دوباره الگوریتم ۲ را اعمال کرد . با استفاده از روش فوق می‌توان به ۳۴ بیت از کلیدIES80 ، 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 می‌توان از روش جستجوی کامل بدست آورد .

٤- 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 ، $1 \le \alpha \le 255$و $1 \le \beta \le 31$ عبارت $NS_a(\alpha,\beta)$ عبارت است ازتعداد دفعاتی از۲۵٦ ورودی ممکن S_aکه یک مقدار XOR شده ورودی که با α ماسک شده است ،با یک مقدار XOR شده خروجی که با βماسک شده است،مطابقت کندیعنی :

$$NS_a(\alpha,\beta)=\#.\left\{x \mid 0 \le x \le 255, (\bigoplus_{s=0}^{8}(x[s]\bullet\alpha[s])) = (\bigoplus_{t=0}^{5}(S_a(x)[t]\bullet\beta[t]))\right\} \quad (٣)$$

که علامت $\bullet$مشخص کننده AND بیت با بیت است[١].مثلا

$$\forall a \qquad NS_a(4,16)=199 \quad (٤)$$

هنگامیکه $NS_a(\alpha,\beta)$برابر با ۱۲۸ نیست در این صورت یک همبستگی بین ورودی و خروجی S_aوجود دارد. مثلا معادله(٤) بیان می کند که بیت دوم S_aبا بیت چهارم S_aبا احتمال $\frac{199}{256}=0.78$ مطابقت دارد.در نتیجه با توجه به ساختار تابع F و با توجه به جداول E وP داریم:

$$X[3]\oplus F(X,K)[9]=K[6] \qquad P=0.78 \quad (٥)$$

جدول ۱ قسمتی از توزیع جدول S_aرا نشان می دهدکه محورهای عمودی وافقی به ترتیب مشخص کننده αوβهستند و هر عدد در جدول $NS_a(\alpha,\beta)-128$را نشان می دهد.جدول کامل این S-box ها نشان می دهدکه معادله (٤) بهترین تقریب خطی در تمام S-box هاست.(یعنی $|NS_a(\alpha,\beta)-128|$ماکزیمم است)بنابراین معادله (٥) بهترین تقریب از تابع F است.

٥-تقریب خطی الگوریتم IES80

در این قسمت تقریب خطی تابع F به کل الگوریتم تعمیم داده می‌شود. اولین مثال IES80 ، ۳ دوری است . بااعمال معادله (٥) به دور اول رابطه زیر با احتمال $P=\frac{199}{256}$ برقرار است:

$$X_2[9]\oplus P_H[9]\oplus P_L[3]=K_1[6] \quad (٦)$$

به همین ترتیب:

$$X_2[9]\oplus C_H[9]\oplus C_L[3]=K_3[6] \quad (٧)$$

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

$$P_H[9]\oplus C_H[9]\oplus P_L[3]\oplus C_L[3]=K_1[6]\oplus K_3[6] \quad (٨)$$

احتمال اینکه معادله (٨) برای متنهای تصادفی P و متنهای رمز شده نظیرC برقرار باشد برابر است با $(\frac{199}{256})^2+(1-\frac{199}{256})^2=0.65$.چونکه معادله (٥) بهترین تقریب خطی از تابع F است بنابراین معادله (٨) نیز بهترین عبارت برای IES80 ،۳دوری است.حال می توان معادله (٨) را با استفاده از الگوریتم۱ 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_a

-۷	۳	۱۳	-۱	-۵	۱	۷	۵	-۳	۳	۱	-۵۷	-۹	۱	۳
۱	۱	۱	۹	-۵	۳	۱۱	۱۱	۱۳	-۳	۱	-۲۳	-۱	-۱	- ۵
-۸	-۲	۱۲	-۶	-۱۲	-۲	۱۶	۲	۱۶	-۶	۱۶	-۲۲	-٤	-٦	۱۲
۷	-۳	-۱۱	-۵	-۱	-۷	۱	۱۱	-۳	-۵	-۱۳	-۷	۹	-۵	۳
٦	۲	٤	-۱٦	۰	-٤	۱۰	٦	-۲۰	-٤	-٦	-٦	-۱٤	-٦	۱۲
۱۰	-٤	-۸	۱۸	-۸	-۱۰	-٦	۱٦	-۱۲	٦	-۱۸	-۱٦	٦	-٤	۱۲
-۱	۳	۵	-۷	-۱۷	-۵	۱	-۳	-۷	۱	-۲۱	-۱۳	۵	-۱۱	۱۱
-۵	-۱	۱	-۷	۵	۱	-۱	-۹	-۵	۳	۹	-۲۷	۵	-۳	-۹
-٦	۰	٤	-۱۰	٦	۰	-٤	-٦	٦	٤	۱٦	-۱٤	۱۰	-٤	۰
-۲	۲	-۱۲	-٤	٦	۱۰	-۱٦	-۱٦	-۱٦	۲	-۱۲	۰	۲	-٦	-۸
-۱	۱	۹	-۱	۹	۷	-۱	-۷	۷	۹	-۱۱	-۱۳	-۷	-۱	-۵
-۸	۲	-۸	-۱۰	۲	۰	-۱٤	۱۲	-۲	-٤	٦	-۱٦	٤	-۲	۱۲
-۷	۱	۹	-۱۱	۵	-۳	-۳	۱۷	-۱	-۱	-۹	-۵	-۱	-۱	-۱
-۳	-۵	-۳	-۱	-۷	-۱۳	۹	-۱	-۹	۱	-۵	-۱۵	۷	-۳	۳
۰	۸	-۸	-٤	-۲	-۲	-۲	۲	-۱٤	۲	-۱۰	-۱٤	-٤	-٤	۰
-۱	۱	۱۱	-۷	-۷	-۱	۱۳	-۹	۵	۳	-۳	۷۱	۳	-۳	-۵

لم۱ [۱]: اگر N تعداد متنهای اصلی تصادفی وP احتمال برقراری رابطه (۱) باشد،فرض کنید $|P-1/2|$ به اندازه کافی کوچک است،در این صورت نرخ موفقیت الگوریتم۱ عبارت است از:

$$\int_{2\sqrt{N}|p-\frac{1}{2}|}^{\infty} \frac{1}{\sqrt{2\pi}} \quad e^{-\frac{x^2}{2}}\, dx \qquad (۹)$$

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	٪۸٤،۱	٪۹۲،۱	٪۹۷،۷	٪۹۹،۸

حال به یک IES80 ، ۵ دوری پرداخته می‌شود . در این مورد معادله (۵) به دورهای دوم وچهارم اعمال می‌شود ومعادله خطی زیر به دورهای اول وآخر اعمال می‌شود.

$$NS_a(4,16)=199 \Rightarrow X[8]\oplus F(X,K)[3]=K[14] \qquad (۱۰)$$

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

$$P_H[3]\oplus P_L[9,8]\oplus C_H[3]\oplus C_L[9,8]=K_1[14]\oplus K_2[6]\oplus K_4[6]\oplus K_5[14] \qquad (۱۱)$$

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

لم۲[۱]۱ :اگر $(1\le i\le n)$ X_i ها متغییر های تصادفی مستقل باشند که مقادیر آنها با احتمال P_i برابر صفر وبا احتمال $1-P_i$ برابر یک باشد،در این صورت احتمال اینکه $X_1\oplus X_2\oplus\ldots\oplus X_n=0$ باشد عبارت است از:

$$\frac{1}{2}+2^{n-1}\prod_{i=1}^{n}(P_i-\frac{1}{2}) \qquad (۱۲)$$

۱. piling-up lemma

این لم بیان می کند که معادله (۱۱) با احتمال $\frac{1}{2}+2^3(\frac{71}{256})^2(\frac{71}{256})^2=0.547$ 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 .

درجدول۳ بهترین عبارتها واحتمالات نظیر آنها برای IES80، n دوری $(3\le n\le 20)$ 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 تابعF 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 $|1.44\times 2^{-33}|^{-2}\approx 2^{66}$ متن اصلی معلوم ، حدس زده می شود.در قسمت بعد روشی ارائه می‌شود که می توان نهایتا 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

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

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

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

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

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

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

٦- 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، ۷دوری با احتمال $0.5 + 1.23 \times 2^{-13}$ داریم:

$$P_H[10] \oplus P_L[1] \oplus C_H[3] \oplus C_L[9] \oplus F_8(C_L, K_8)[3] = K_1[4] \oplus K_3[6] \oplus K_4[15,16] \oplus K_5[6] \oplus K_7[6] \qquad (۱۳)$$

هر چند که این معادله شامل ٦٤ 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. بنابر این به ۲۵٦ 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

لـم ۳ [۱]: اگـر 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 $l_1,l_2,...l_d$ و $|P-1/2|$ $\sqrt{N}$ بستگی دارد.

در شرایط خاص لم (٤) را داریم:

لم ٤[۱]:با همان شرایط لم (۳) اگر $q^{(i)}$ احتمال صحت رابطه زیر برای یک کاندید $K_n^{(i)}$ باشد وX یک متغیر تصادفی باشد

$$F_n(X,K_n)[l_1,l_2,...l_d]=F_n(X,K_n^{(i)})[l_1,l_2,...l_d] \qquad (١٤)$$

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

$$\int_{x=-2\sqrt{N}|P-1/2|}^{\infty}\Big(\prod_{K_n^{(i)}\neq K_n}\int_{-x-4\sqrt{N}(P-1/2)q^{(i)}}^{x+4\sqrt{N}(P-1/2)(1-q^{(i)})}\frac{1}{\sqrt{2\pi}}e^{-y^2/2}dy\Big)\frac{1}{\sqrt{2\pi}}e^{-x^2/2}dx \qquad (١٥)$$

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

هرچند که $q^{(i)}$ ها درهمه شرایط مستقل نیستند،ولی نتایج عملی نشان داده است که لم ٤ یک تقریب خوبی برای نرخ موفقیت بدست می دهد،همان طور که درجدول ٤ مشاهده می شود:

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

جدول ٤ : 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	٪٤٨،٦	٪٧٨،٥	٪٩٦،٧	٪٩٩،٩

اگر الگوریتم ۲ روی دوگان معادله (۱۳) نیز به کارگرفته شود در نهایت با استفاده از حافظه کوچکی ١٦ بیت کلید فرعی بدست می‌آید.در این صورت باید سایر بیتهای کلید را با جستجو بدست آورد.نتایج عملی با کامپیوتر به نتایج بهتر از جدول(٤) ختم شده است. با استفاده از $4|1.23\times2^{-13}|^{-2}\cong2^{27}$ متن اصلی معلوم ،کل سیستم شکسته می‌شود . نرخ موفقیت ٪۸۸ است.

روش شکستن IES80 ،۱۲ دوری هم مشابه ۸ دوری است. ، با استفاده از $8|1.3\times2^{-24}|^{-2}\cong2^{50}$ متن اصلی معلوم می‌توان آنرا شکست

به طور مشابه مطابق لم ٤ ، می توانIES80 ،١٦ دوری را با استفاده از $8|1.44\times2^{-33}|^{-2}\cong2^{66}$ متن اصلی معلوم ،با حل عبارت زیر شکست:

$$\begin{aligned}&P_H[10]\oplus P_L[1]\oplus C_H[3]\oplus C_L[9]\oplus F_{16}(C_L,K_{16})[3]\\&=K_1[4]\oplus K_3[6]\oplus K_4[15,16]\oplus K_5[6]\oplus K_7[6]\oplus K_8[15,16]\oplus K_9[6]\oplus\\&K_{11}[6]\oplus K_{12}[15,16]\oplus K_{13}[6]\oplus K_{15}[6]\end{aligned} \qquad (١٦)$$

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،١٦ دوری را با حافظه کمی خیلی سریعتر از جستجوی کامل شکست.حال یک روش دیگر برای شکستن IES80، ١٦ 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 ، می‌شود.در نتیجه IES80 ،١٦ دوری با نرخ موفقیت بزرگی با مشخص بودن 2^{64} متن اصلی معلوم ومتنهای رمز شده نظیر ، شکسته میشود.

در روش قبل از دو معادله تقریبی خطی برایIES80 ، ١٦ 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 درنتیجه ۹ بیت کلید را بدست می دهد.در روش جدید از دو تقریب خطی جدید که از بهترین عبارت برای IES80 ،١٤ دوری بدست می آیند،استفاده می شود که هر معادله دو S-box فعال را شامل می شود،درنتیجه ۱۷ بیت کلید را بدست می دهد.در نتیجه این معادلات ۳۴ بیت کلید را مشخص می کنند وبقیه ٣٦=٣٤-٧٠ بیت کلید باید توسط جستجوی کامل مشخص شوند.

در روش جدید از دو معادله زیر که برای IES80 ،۱٤ دوری با احتمال $1/2+1.71\times2^{-32}$ برقرار است ،استفاده می شود:

$$P_L[10]\oplus C_H[9]\oplus C_L[3]=K_2[6]\oplus K_3[15,16]\oplus K_4[6]\oplus K_6[6]\oplus K_7[15,16]\oplus K_8[6]\oplus K_{10}[6]\oplus K_{11}[15,16]\oplus K_{12}[6]\oplus K_{14}[6] \quad (۱۷)$$

$$C_L[10]\oplus P_H[9]\oplus P_L[3]=K_{13}[6]\oplus K_{12}[15,16]\oplus K_{11}[6]\oplus K_9[6]\oplus K_8[15,16]\oplus K_7[6]\oplus K_5[6]\oplus K_4[15,16]\oplus K_3[6]\oplus K_1[6] \quad (۱۸)$$

حال معادلات (۱۷) و (۱۸) را به دورهای دوم تا پانزدهم یکIES80 ،۱٦ دوری اعمال می شود. در نتیجه معادلات زیر را برای IES80 ،۱٦ دوری متناظر با متنهای تصادفی P وC با احتمال $1/2-1.71\times2^{-32}$ داریم:

$$P_H[10]\oplus F_1(P_L,K_1)[10]\oplus C_H[3]\oplus C_L[9]\oplus F_{16}(C_L,K_{16})[3]= K_3[6]\oplus K_4[15,16]\oplus K_5[6]\oplus K_7[6]\oplus K_8[15,16]\oplus K_9[6]\oplus K_{11}[6]\oplus K_{12}[15,16]\oplus K_{13}[6]\oplus K_{15}[6] \quad (۱۹)$$

$$C_H[10]\oplus F_{16}(C_L,K_{16})[10]\oplus P_H[3]\oplus P_L[9]\oplus F_1(P_L,K_1)[3]= K_{14}[6]\oplus K_{13}[15,16]\oplus K_{12}[6]\oplus K_{10}[6]\oplus K_9[15,16]\oplus K_8[6]\oplus K_6[6]\oplus K_5[15,16]\oplus K_4[6]\oplus K_2[6] \quad (۲۰)$$

اولین مرحله از حمله،حل معادلات فوق است تا اینکه تعدادی از ۷۰بیت کلید مشخص شوند.

حال اگر با استفاده از الگوریتم ۲ اقدام به حل معادلات (۱۹) و (۲۰) شود در نهایت ۳٤ بیت از کلید اصلی بدست می‌آید . بقیه ۳٦ بیت از کلید را باید با استفاده از جستجوی کامل بدست آورد.

۷- جمع بندی و نتیجه‌گیری

در این مقاله ما به بررسی حمله خطی بر روی الگوریتم IES80 پرداختیم و مشاهده کردیم که جدول $|NS_a(\alpha,\beta)-128|$مربوط به S_box ها دارای توزیع یکسان نمی‌باشد . 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.