ارزیابی تحلیلی الگوریتم رمز طارق۲

قدمعلی باقری کرم
دانشجوی کارشناسی ارشد دانشگاه صنعتی اصفهان
gh_ali_bk@yahoo.com

محمد دخیل علیان
استادیار دانشگاه صنعتی اصفهان
mdalian@cc.iut.ac.ir

چکیده : در این مقاله ابتدا برخی مبانی تئوری امنیت قابل اثبات در برابر حملات تفاضلی و خطی،بررسی می‌گردد وسپس قوانین طراحی الگوریتم رمز طارق ۲ ،خصوصا مقاومت آن در برابر حملات تفاضلی و خطی مرور می گردد و ثابت می‌گردد که این الگوریتم دارای امنیت قابل اثبات در برابر مدلهای اولیه حملات تفاضلی و خطی می‌باشد.

کلمات کلیدی: طارق ۲ ، حمله تفاضلی ، حمله خطی ، امنیت قابل اثبات ، همبستگی

۱- مقدمه

پس از ابداع حملات تفاضلی و خطی،تلاشهای زیادی برای طراحی الگوریتمهای رمز قالبی مقاوم در برابر این حملات انجام شده است. یکی از این تلاشها معطوف به امنیت قابل اثبات در برابر حملات تفاضلی و خطی شده است.اولین الگوریتم رمز قالبی با امنیت قابل اثبات در برابر حملات تفاضلی و خطی تحت شرط استقلال کلیدهای دور توسط نایبرگ[۱] و نادسن[۲] طراحی شد[۱و۲] سپس ماتسوئی[۳] یک روش جهت طراحی الگوریتمهای رمز قالبی با امنیت قابل اثبات در برابر حملات تفاضلی و خطی مطرح کرد. این روش بر مبنای همان قوانین مطروحه توسط نایبرگ و نادسن بود اما در آن از برخی ساختارهای جدید استفاده شده بود که می تواند جهت کاهش اندازه جعبه های S-box به کار گرفته شود. این روش در طراحی برخی الگوریتمهای رمز قالبی از جمله MISTY[4] , KASUMI[5,6] و طارق ۲ استفاده شده است. در این مقاله برخی مبانی تئوری امنیت قابل اثبات در برابر حملات تفاضلی و خطی تحت شرط استقلال کلیدهای دور بررسی می گردد. در اینجا تاکید بیشتر بر روی تئوریهایی است که ارتباط بیشتری با مبنای طراحی طارق ۲ دارند . نکته قابل توجه این است که تئوریهای مطرح شده در این مقاله صرفا برای بررسی امنیت قابل اثبات در برابر حملات مرسوم تفاضلی و خطی قابل استفاده اند.

۲- تحلیلهای تفاضلی و خطی

در این قسمت یک مرور سریع بر روی حملات تفاضلی و خطی انجام می گیرد تا اینکه نمادهای به کار رفته در سایر قسمتها تعریف گردد.

1.Nyberg
2.Knudsen

۲-۱- تحلیل تفاضلی

تحلیل تفاضلی[۷] یک حمله متن اصلی برگزیده است که به مطالعه انتشار تفاضلهای ورودی به تفاضلهای خروجی در تبدیلات دوری می‌پردازد. این انتشار تفاضل درتعریف بعد به طور رسمی بیان می‌گردد.

تعریف۱: فرض کنید $a, a^* \in GF(2)^n, f: GF(2)^n \to GF(2)^m$ باشد.در این صورت گفته می شود که تفاضل $a' = a \oplus a^*$ به تفاضل $b' = f(a) \oplus f(a^*)$ انتشار می یابد. این انتشار با نماد $a' \xrightarrow{f} b'$ یا $a' \longrightarrow b'$ نمایش داده می شود. یک عبارت به صورت $\alpha \xrightarrow{f} \beta$ یک مشخصه تفاضلی نامیده می‌شود.

اگر تفاضل یک زوج ورودی α باشد،مشخصه تفاضلی $\alpha \longrightarrow \beta$ می‌تواند جهت پیش‌بینی تفاضل خروجی به کار رود. طبیعی است که راندمان یک مشخصه تفاضلی توسط تعداد ورودی هایی با تفاضل α که منجر به خروجی هایی با تفاضل β می‌شوند،اندازه گرفته شود. این نسبت تعداد،نسبت انتشار مشخصه تفاضلی نامیده می‌شود.

تعریف ۲ : نسبت انتشار[۱] R_P برای مشخصه تفاضلی $\alpha \xrightarrow{f} \beta$ توسط رابطه زیر تعریف می گردد:

$$R_P(\alpha \xrightarrow{f} \beta) = 2^{-n}\left|\left\{X \in GF(2)^n \middle| f(x) \oplus f(x \oplus \alpha) = \beta\right\}\right|$$

روند حمله تفاضلی بر روی یک الگوریتم دوری r دوری به صورت زیر می‌باشد :

۱- یک مشخصه r-1 دوری $\alpha \longrightarrow \beta$ با نسبت انتشار به اندازه کافی بزرگ پیدا کنید .

۲- برای هر زیر کلید K_r در دورr ام یک شمارنده با مقدار اولیه صفر در نظر بگیرید .

۳- یک متن اصلی x به صورت تصادفی با توزیع یکنواخت انتخاب کنید و $x^* = x \oplus \alpha$ را بدست آورید. سپس متنهای x و x^* را تحت کلید نا معلوم K رمز کنید تا متنهای رمز شده y و y^* بدست آیند. برای هر مقدار ممکن زیر کلید دور K_r که تفاضل ورودی β در دورr ام منجر به تفاضل y و y^* می شود یکی به شمارنده نظیر زیرکلید اضافه نمائید .

۴-گام سوم را برای متنهای تصادفی دیگر تکرار کنید تا یکی از شمارنده ها به اندازه کافی بزرگتر از دیگران شود.این شمارنده متناظر زیر کلید صحیح با معیار حداکثر درستنمائی خواهد بود.

بهبودهای مختلفی برای این حمله ارائه شده اند که باعث کاهش تعداد متنهای اصلی مورد نیاز می شود. همچنین حملاتی مطرح شده اند که از مشخصه تفاضلی r-2 دوری استفاده می کنند و زیر کلیدهای دورهای اول و آخر را تعیین می نمایند. برای جزئیات بیشتر به [۷] مراجعه شود.

با استفاده از آنالیز آماری می توان نشان داد که کلید دور صحیح از یک کلید تصادفی قابل تمایز است. ثابت می شود که تعداد متنهای اصلی مورد نیاز برای این تمایز با نسبت انتشار مشخصه به کار رفته نسبت عکس دارد. بنابراین یک شرط لازم برای مقاومت در برابر حمله تفاضلی این است که مشخصه ایی تفاضلی با نسبت انتشار بزرگتر از 2^{-n} برای تعدادی دور (معمولا ۳ دور) وجود نداشته باشد که n طول قالب ورودی است. برای توابع وابسته به کلید،متوسط مقاومت در برابر حمله تفاضلی مطرح است و بنابراین متوسط نسبتهای انتشار دوری همه کلیدها مطرح می شود .

تعریف ۳ [۱]: فرض کنید $F: GF(2)^n \times K \longrightarrow GF(2)^m$ یک تابع وابسته به کلید باشد. برای هر کلید ثابت $k \in K$ ، داریم $f_k(x) = F(x,k)$.وهمچنین فرض کنید $\alpha \in GF(2)^n$ و $\beta \in GF(2)^m$ مقادیر ثابتی هستند. پتانسیل مشخصه های تفاضلی $\alpha \xrightarrow{f_k} \beta$ و $\alpha \xrightarrow{F} \beta$ به صورت زیر تعریف می شوند :

$$DP(\alpha \xrightarrow{f_K} \beta) = R_p(\alpha \xrightarrow{f_K} \beta)$$[۲]

$$DP(\alpha \xrightarrow{F} \beta) = \frac{1}{|K|}\sum_{k \in K} DP(\alpha \xrightarrow{f_K} \beta)$$

پتانسیل ماکزیمم F به صورت زیر تعریف می شود :

$$DP^F_{\max} = \max Dp(\alpha \xrightarrow{F} \beta) \qquad \alpha \neq 0, \beta$$

1.Propagation ratio
2.Differential Potential

نتیجه ۱[۱و۳] : یک الگوریتم رمز قالبی با طول قالب n در برابر حمله تفاضلی تحت فرض استقلال زیرکلیدها مصون است،اگر هیچ مشخصه تفاضلی $\alpha \longrightarrow \beta$ و $\alpha \neq 0$ برای تمام دورها وجود نداشته باشد به طوری که $Dp(\alpha \longrightarrow \beta) >> 2^{-n}$ باشد.

توجه کنید که مصونیت در برابر حمله تفاضلی الزاما به معنای مصونیت در برابر سایر حملات از نوع تفاضلی مانند حمله غیر ممکن[۱] [۸و۹] ، حمله تفاضلی مرتبه بالاتر [۲][۱۰] ، حمله تفاضلی بریده[۳][۱۰] و حمله بومرنگ[۴] [۱۲] نیست .

۲-۲- تحلیل خطی

تحلیل خطی[۱۴و۱۵] یک حمله متن اصلی معلوم است که بر مبنای رابطه تقریبا خطی موثر بین متن اصلی، متن رمز شده و کلید،استوار است. یک بردار باینری انتخاب کننده $w \in GF(2)^n$، بیت i ام را انتخاب می کند وقتی که $w_i = 1$. ترکیب خطی بیتهای یک بردار $x \in GF(2)^n$ که توسط w انتخاب شده اند، به صورت حاصلضرب داخلی $w \bullet x = w_1 x_1 \oplus w_2 x_2 \oplus ... \oplus w_n x_n$ قابل بیان است. برای راحتی فرض کنید $l_w : GF(2)^n \longrightarrow GF(2)$ مشخص کننده نگاشت $l_w(x) = w \bullet x$ باشد. یک رابطه خطی تقریبی بین بردارهای باینری $x \in GF(2)^n$ و $y \in GF(2)^m$ عبارت است از یک عبارت از نوع $w \bullet x = u \bullet y$. راندمان این تقریب توسط همبستگی قابل ارزیابی است.

تعریف ۴ : فرض کنید $f, g : GF(2)^n \longrightarrow GF(2)$ توابع بولی باشند. ضریب همبستگی C(f,g) برای دو تابع g,f به صورت زیر تعریف می گردد.

$$C(f,g) = 2^{-n}\left(\left|\{x \in GF(2)^n \middle| f(x) = g(x)\}\right| - \left|\{x \in GF(2)^n \middle| f(x) \neq g(x)\}\right|\right)$$

به عبارت دیگر ضریب همبستگی برابر است با تعداد جاهایی که دو تابع f و g برابرند منهای تعداد جاهایی که برابر نیستند ، تقسیم بر کل حالتها .

در روش حمله خطی به یک الگوریتم رمز دوری r دوری، تحلیلگر سعی در پیدا کردن تقریب خطی r-2 دور آن از دور دوم تا r-1 ام می نماید تا به عبارت تقریبی زیر برسد :

$$a.X \oplus b.Y \oplus c.K = 0 \qquad (۱)$$

که برای متن اصلی معلوم x، $X = f_1(x, k_1)$ و $y = f_r(Y, k_r)$ متن رمز شده و $k = (k_2, ...k_{r-1})$ یک بردار روی تمام کلیدهای دور نامعلوم از دور دوم تا r-1 ام می‌باشد. با فرض در اختیار داشتن N متن اصلی معلوم می توان قسمتهائی از کلیدهای K_1, K_r را پیدا کرد. به این ترتیب که تمام زیر کلیدهای دور ممکن در دور اول و r ام تست می‌شوند و برای هر یک N_0 تعداد متنهائی که در رابطه زیر صدق می کنند پیدا می گردند.

$$a.f_1(x, k_1) \oplus b.f_r^{-1}(y, k_r) = 0 \qquad (۲)$$

زیر کلیدی که مقدار $\left|N_0 / N - 1/2\right|$ را ماکزیمم می‌کند، با معیار حد اکثر درستنمائی زیر کلید صحیح می‌باشد .

در [۱] نشان داده شده است که تعداد متنهای اصلی مورد نیاز به صورت معکوس متناسب است با متوسط روی K از مربع همبستگی بین a.x وb.y . در [۱] نشان داده شده است که این متوسط برابر با جمع روی C از مجذورات همبستگیهای معادله (۱) میباشد. بنابراین طبیعی است که تمام تقریبهای خطی به فرم معادله (۱) روی تمام مقادیر ممکن C در نظر گرفته شوند. این خانواده از تقریبها، هالهای خطی[۱] نامیده می شوند[۱] و با نماد $b \leftarrow a$ نمایش داده می‌شوند. پتانسیل آن به صورت متوسط ذکر شده در بالا تعریف می گردد. بنابراین یک الگوریتم رمز قالبی در برابر حمله خطی در صورتی مصون است که هیچ هال خطی برای کل الگوریتم وجود نداشته باشد که پتانسیل آن بزرگتر از 2^{-n} باشد که n طول قالب الگوریتم است .

---

1. Impossible differential
2. Higher order Differential attack
3. Truncated differential attack
4.Boomerange attack
1.Linear Hulls

تعریف ۵ : فرض کنید $F = GF(2)^n \times K \to GF(2)^m$ یک تابع وابسته به کلید باشد و برای هر کلید ثابت $k \in K$ ، $f_k(x) = F(x,k)$ باشد و همچنین فرض کنید $w \in GF(2)^n, u \in GF(2)^m$ مقادیر ثابتی هستند. پتانسیل تقریب خطی $u \xleftarrow{F} w, u \xleftarrow{f_K} w$ به صورت زیر تعریف می گردد :

$$Lp(u \xleftarrow{f_K} w) = \left|C(l_u of_K, l_w)\right|^2$$

$$Lp(u \xleftarrow{F} w) = \frac{1}{|K|}\sum_{k\in K} Lp(u \xleftarrow{f_K} w)$$

پتانسیل بهترین تقریب خطی F به صورت زیر تعریف می گردد:

$$Lp^F_{\max} = \max Lp(u \xleftarrow{F} W) \qquad u \neq 0, w$$

نتیجه ۲ [۱] : یک الگوریتم رمز قالبی با طول قالب n ، تحت فرض استقلال زیر کلیدها در صورتی در برابر حمله خطی مصون است که هیچ تقریب خطی $u \longleftarrow w$ و $u \neq 0$ روی کل الگوریتم وجود نداشته باشد که $Lp(u \leftarrow w) >> 2^{-n}$ باشد .

۳-الگوریتمهای رمز قالبی با امنیت قابل اثبات در برابر حملات تفاضلی و خطی

پس از ابداع حملات تفاضلی و خطی متخصصین بسیاری ساختارهای گوناگونی برای الگوریتمهای رمز قالبی که در برابر این حملات دارای امنیت باشد، ارائه کرده اند. در [۲] یک الگوریتم قالبی شبه DES ارائه شده است که دارای پتانسیل تفاضلی کوچکی می‌باشد و بنابراین تحت فرض استقلال کلیدهای دور دارای امنیت قابل اثبات در برابر حمله تفاضلی است. در [۱] نشان داده شده است که این الگوریتم دارای پتانسیل خطی کمی است و بنابراین در برابر حمله خطی نیز دارای امنیت قابل اثبات می باشد.

در [۳] برخی ساختارهای دیگری برای الگوریتمهای رمز قالبی ارائه شده است که دارای امنیت قابل اثبات در برابر حملات تفاضلی و خطی می باشد. یکی از مزایای ساختارهای مطروحه در مرجع [۳] این است که در این ساختارها از توابع دوری استفاده شده است و بنابراین ابعاد S-box ها کوچک شده اند و برای پیاده سازی نرم افزاری و سخت افزاری مناسب گردیده اند .

قضیه ۱ [۱] : فرض کنید $F : GF(2)^n \times GF(2)^n \times K_1$ و $G : GF(2)^n \times GF(2)^n \times K_2$ توابع وابسته به کلید از نوع $G(x,k,k') = g(x \oplus k, k'), F(x,k,k') = f(x \oplus k, k')$ باشند که $f : GF(2)^n \times K_1 \to GF(2)^n$ و $g : GF(2)^n \times K_2 \to GF(2)^n$ برای هر $k_1 \in K_1$ و $k_2 \in K_2$ دوسویه می باشند . در این صورت

$$Lp(u \xleftarrow{G\circ F} w) = \sum_{v\in GF(2)^n} Lp(u \xleftarrow{g} v) Lp(v \xleftarrow{f} w)$$

نتیجه ۱ [۱۵] : اگر G,F مطابق قضیه ۱ باشند در اینصورت

$$D_p(\alpha \xrightarrow{G\circ F} \beta) = \sum_{\xi\in GF(2)^m} Dp(\alpha \xrightarrow{f} \xi) Dp(\xi \xrightarrow{g} \beta)$$

نتیجه زیر بیان می کندکه افزایش تعداد دورها ، الگوریتم را ضعیف نمی‌کند .

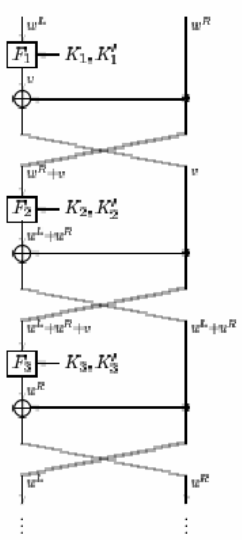
نتیجه ۲ : اگر G,F مطابق قضیه ۱ باشند در این صورت

$$Lp^{G\circ F}_{\max} \le \min(Lp^f_{\max}, Lp^g_{\max})$$
$$Dp^{G\circ F}_{\max} \le \min(Dp^f_{\max}, Dp^g_{\max})$$

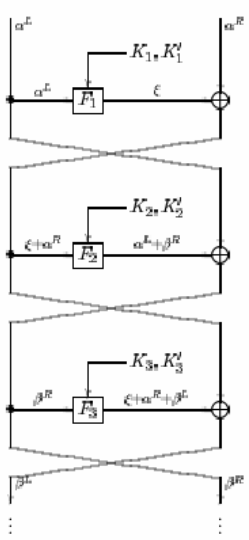
حال به تابع رسم شده در شکل ۱ توجه کنید .

---

2. Linear Potential



شکل ۱: تابع مطرح در قضیه ۲



شکل ۲ : تابع مطرح در قضیه ۳

قضیه۲ [۳] : فرض کنید F یک تابع r دوری مطابق شکل ۱ باشد که $r \geq 3$ است و هر $F_i : GF(2)^n \times GF(2)^n \times K_i \to GF(2)^n$ به صورت $F_i(x, k_i, k_i') = f_i(x \oplus k_i, k_i')$ می باشد که $F_i : GF(2)^n \times K_i \to GF(2)^n$ برای هر $k_i' \in K_i$ ثابت ، یک تابع دو سویه است . اگر $Lp_{\max}^{f_i} \leq p$ (یا به طریق مشابه $Dp_{\max}^{f_i} \leq p$) برای هر i باشد در اینصورت $Lp_{\max}^{F} \leq p^2$ (یا به طریق مشابه $Dp_{\max}^{F} \leq p^2$) می‌باشد .
حال الگوریتم فیستلی شکل ۲ را در نظر بگیرید.

قضیه ۳ [۱و۲] : فرض کنید F یک الگوریتم فیستلی r دوری $(r \geq 3)$ مطابق شکل ۲ باشد که هر $F_i : GF(2)^n \times GF(2)^n \times K_i \to GF(2)^n$ به صورت $F_i(x, k_i, k_i') = f_i(x \oplus k_i, k_i')$ می باشد و هر $f_i : GF(2)^n \times K_i \to GF(2)^n$ برای هر $k_i' \in K_i$ ثابت ، یک تابع دو سویه است . اگر $Lp_{\max}^{F} \leq P^2$ (یا به طریق مشابه $Dp_{\max}^{F} \leq P^2$) می‌باشد .

باید به این نکته توجه کرد که ساختارهای مطرح شده در این قسمت می توانند به صورت دوری به کار روند. به عنوان مثال اگر تابع دور نشان داده شده در شکل ۲ به صورت شکل ۱ باشد در اینصورت اگر پتانسیلهای خطی و تفاضلی زیر تابعها محدود به p باشند طبق قضیه ۳و۲ پتانسیلهای خطی و تفاضلی کل تابع محدود به P^4 می شوند. این ساختارها می توانند تکرار شوند تا اینکه زیر تابع هائی حاصل شوند که دارای ابعاد کوچکی باشند و توسط S-box ها قابل تحقق شوند. کران بالائی برای پتانسیلهای خطی و تفاضلی کل الگوریتم به سادگی با به کار بردن قضایای فوق امکان پذیر است. چنین ساختار هائی در الگوریتمهای KASUMI,MISTY و طارق ۲ به کار رفته اند.

قضیه۴[۳]: برای تابع F نشان داده شده در شکل ۳ داریم:

$$Lp_{\max}^{F} \leq Lp_{\max}^{F_1} + Lp_{\max}^{F_2}$$

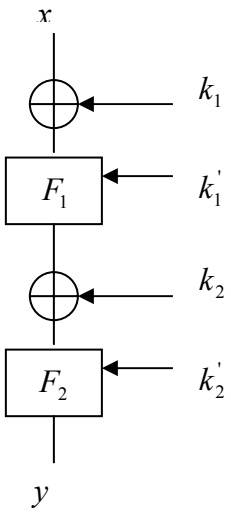
$$Dp_{\max}^{F} \leq Dp_{\max}^{F_1} + Dp_{\max}^{F_2}$$

علاوه بر این ، اگر تابع F برای همه مقادیر کلید،دوسویه باشد در اینصورت:

$$Lp_{\max}^{F} \leq \min\{Lp_{\max}^{F_1}, Lp_{\max}^{F_2}\}$$

$$Dp_{\max}^{F} \leq \min\{Dp_{\max}^{F_1}, Dp_{\max}^{F_2}\}$$

اثبات در [۳] موجود است.



شکل ۳ : تابع F مطرح در قضیه ۴

۴- ارزیابی تحلیلی الگوریتم طارق ۲

الگوریتم طارق۲ جهت رمزگذاری و رمزگشایی قالب‌های داده ۶۴ بیتی تحت کلید مخفی ۱۹۲ الی ۵۱۲ بیتی طراحی گردیده است. هسته اصلی فرآیند رمزگذاری الگوریتم یک ساختار فیستل ۱۶ دوری می‌باشد که توسط دو تبدیل غیرفیستل ابتدایی و انتهایی وابسته به کلید احاطه شده است. بنابراین ساختار الگوریتم ناهمگن می‌باشد.

همانند دیگر رمزنگارهای قالبی، این الگوریتم از دو بخش مجزای فرآیند رمزگذاری و الگوریتم تولید کلید تشکیل شده است. وظیفهٔ فرآیند رمزگذاری، تبدیل متن اصلی ورودی به متن رمز شده خروجی با استفاده از زیر کلیدهای تولید شده توسط الگوریتم تولید کلید می‌باشد.

۴-۱- فرآیند رمز گذاری

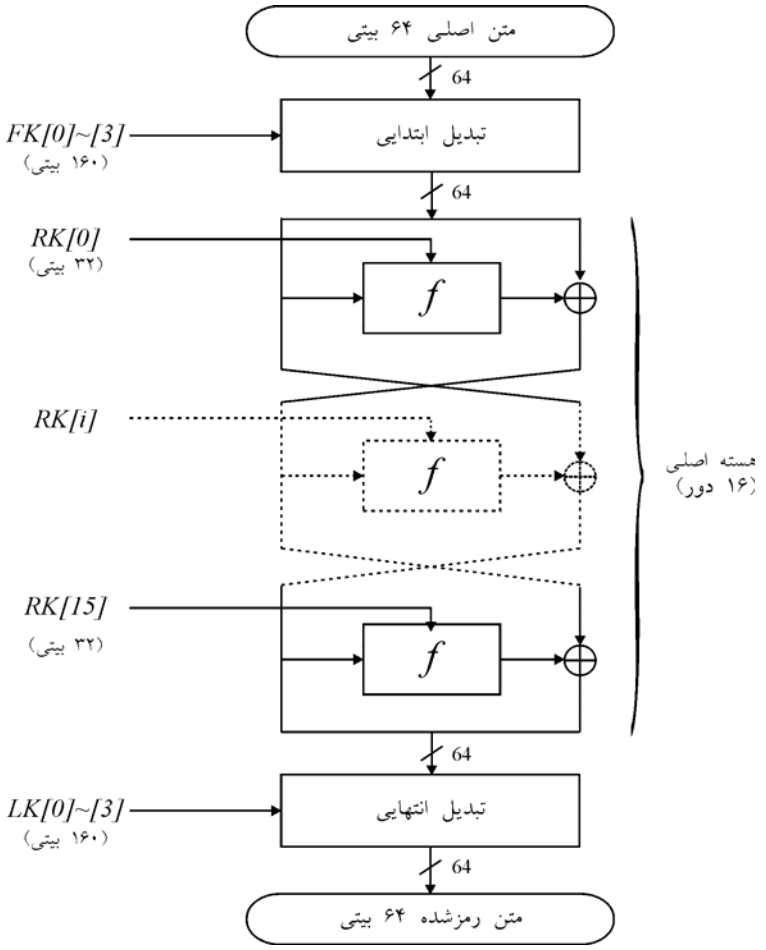
شکل(۴) شمای کلی تابع رمزنگار f در فرآیند رمزگذاری الگوریتم طارق را نشان می‌دهد. این فرآیند از سه بخش وابسته به کلید تشکیل شده است : تبدیل ابتدایی، هسته اصلی فرآیند و تبدیل انتهایی.

هسته اصلی فرآیند رمزگذاری یک ساختار فیستل ۱۶ دوری می‌باشد. تبدیلات ابتدایی و انتهایی، دو تبدیل غیرفیستلی معکوس هم می‌باشند که از دو طرف هسته اصلی را احاطه کرده‌اند. امنیت الگوریتم طارق۲ مبتنی بر امنیت هسته اصلی است و تبدیلات ابتدایی و انتهایی جهت جلوگیری از سهولت دسترسی به ورودی و خروجی هسته بکار رفته‌اند. بنابراین تبدیلات ابتدایی و انتهایی بر پیچیدگی حملات به الگوریتم می‌افزایند و از این طریق به بهبود امنیت الگوریتم کمک می‌نمایند.

فرآیند رمزگذاری نشان داده شده در شکل (۴) از ۱۷۹۲ بیت زیرکلید برای انجام عملیات رمزگذاری (رمزگشایی) استفاده می‌کند. این زیرکلیدها که توسط الگورتیم تولید کلید از روی کلید اصلی سیستم ساخته می‌شوند به نحو زیر استفاده می‌گردند:

- چهار زیرکلید ۱۶۰ بیتی FK[0]~FK[3] برای چهار دور تبدیل ابتدایی
- شانزده زیرکلید ۳۲ بیتی RK[0]~RK[15] برای شانزده دور هسته اصلی الگوریتم
- چهار زیرکلید ۱۶۰ بیتی LK[0]~LK[3] برای چهار دور تبدیل انتهایی.

در بخشهای بعدی به تشریح جزئیات الگوریتم طارق۲ می‌پردازیم.



شکل۴ :فرآیند رمزگذاری الگوریتم طارق ۲

۴-۲- تابع دور رمزنگار f

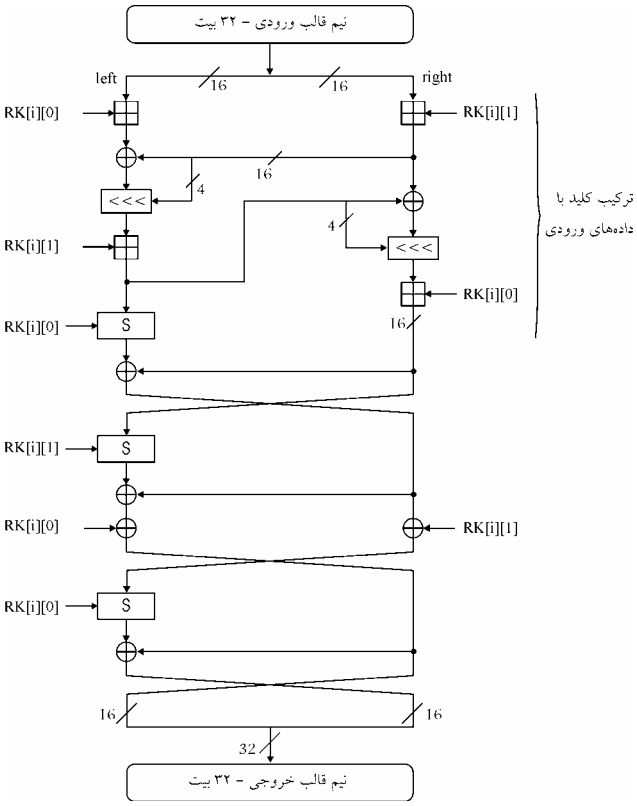
شکل (۵) شمای کلی تابع رمزنگار f در فرآیند رمزگذاری الگوریتم طارق را نشان می‌دهد. در تابع f ابتدا نیم‌قالب ورودی ۳۲ بیتی به دو زیرقالب ۱۶ بیتی left و rigth تقسیم می‌شود. زیرکلید ورودی به تابع f در دور i ام، RK[i] ، نیز به دو نیمه مساوی RK [i][0] و RK [i][1] تقسیم می‌شود.

در این تابع عملیات روی زیرقالبهای ۱۶ بیتی انجام می‌گیرد. در ابتدا زیرکلید ورودی به تابع با دو زیر قالب ورودی طی یک فرآیند غیرخطی ترکیب می‌شود. سپس این دو زیرقالب ۱۶ بیتی طی عملیات سه‌دوری و با استفاده از تابع S ، نیم قالب ۳۲ بیتی خروجی تابع f را به وجود می‌آورند.

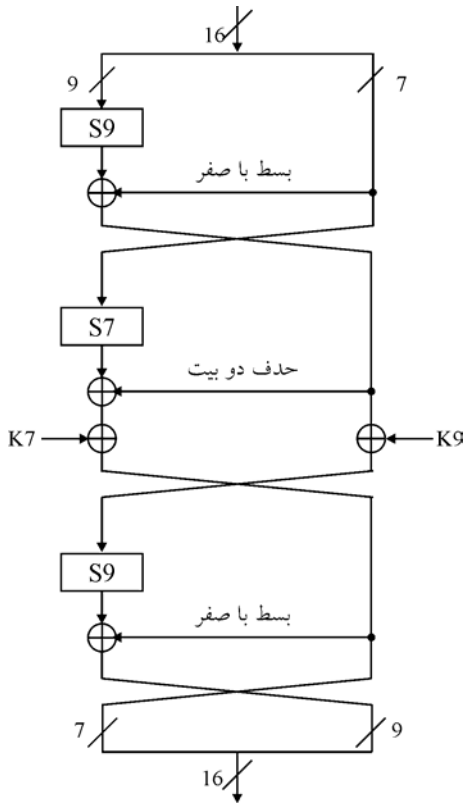
۴-۳- تابع S

در تابع f ، تابع S حکم یک S-box ۱۶×۱۶ بیتی وابسته به کلید را دارد. بنابراین ابعاد این S-box برای پیاده‌سازی به صورت یک جدول فراخوانی بزرگ است. بدین‌منظور ساختار شکل (۶) برای استفاده به عنوان S برگزیده شده است.

همانگونه که از شکل (۶) پیداست رشتهٔ ۱۶ بیتی ورودی به تابع S به دو قسمت ۹ بیتی و ۷ بیتی (و نه ۸ بیتی و ۸ بیتی) تقسیم شده است. این تقسیم غیرمساوی به این خاطر است که توابع دوسویی با بعد فرد عموماً از نقطه نظر امنیت قابل اثبات در مقابل حملات تفاضلی و خطی بهتر از توابع با بعد زوج می‌باشند. بنابراین با تقسیم ۱۶ بیت به ۷ بیت و ۹ بیت، رمزنگار مقاومت بیشتری در مقابل حملات تفاضلی و خطی خواهد داشت.



شکل۵ :تابع دور f



شکل ۶: تابع S

در ساختار نشان داده شده در شکل ۶ از دو S-box با نامهای S9 و S7 به ترتیب با ۹ بیت و ۷ بیت ورودی استفاده شده است. این S-box ها دوسویی هستند و توسط توابع تقریباً غیرخطی کامل ساخته می‌شوند. زمانی که خروجی S9 با داده‌های ۷ بیتی XOR می‌شود، با اضافه نمودن دو بیت صفر به منتهی‌الیه سمت چپ این داده‌ها طول آن به ۹ بیت بسط داده می‌شود. به عکس زمانی که خروجی S7 با داده‌های ۹ بیتی XOR می‌شود، با حذف دو بیت منتهی‌الیه سمت چپ، طول آن به ۷ بیت کاهش می‌یابد.

برای ساخت S-box های S9 و S7 به ترتیب از توابع غیرخطی کامل در $GF(2^9)$ و $GF(2^7)$ استفاده شده است. به این ترتیب این S-box ها حداکثر مقاومت را در مقابل حملات تفاضلی و خطی بوجود می‌آورند. توابع مورد استفاده عبارتند از :

$$S7(X)=(47X+123)^{111} \bmod 131$$
$$S9(X)=(47X+213)^{383} \bmod 529$$

البته در اینجا از یک تبدیل مستوی نیز علاوه بر توابع تقریباً غیرخطی کامل استفاده شده است. این تبدیل مستوی پیچیدگی به سیستم اضافه نمی‌کند و فقط باعث می‌شود که تبدیلات ثابت ۰→۰ و ۱→۱ که همواره در توابع نمایی $f(x)=x^P$ وجود دارد از بین برود. در ضمن اعداد مشخص شده در روابط فوق به جز توانها بیانگر ضرایب چندجمله ای بکار رفته است بدین معنی که اگر مثلا اعداد ۱۳۱و۵۲۹ به باینری تبدیل شوند این رقمها همان ضرایب چند جمله ای در نظر گرفته شده برای میدانهای $GF(2^7), GF(2^9)$ می باشند.

S7 و S9 وابسته به کلید نمی‌باشند و به صورت جداول ثابت استفاده می‌گردند. برای وابسته کردن تابع S به کلید در ساختار شکل(۶) از عمل XOR استفاده شده است. بدین ترتیب که کلید ۱۶ بیتی k ورودی به تابع S به دو قسمت ۷ بیتی k7 و ۹ بیتی k9 تقسیم می‌گردد. k7 هفت بیت سمت راست k و k9 نه بیت سمت چپ k را تشکیل می‌دهند. دخالت کلید k در ساختار S پیچیدگی سیستم را افزایش می‌دهد.

۴-۴- ارزیابی الگوریتم

به طور کلی برای توابع تقریبا غیر خطی کامل f روی $GF(2^n)$ اگر n زوج باشد $Dp^f_{\max} = Lp^f_{\max} = 2^{-n+2}$ و اگر n فرد باشد $Dp^f_{\max} = Lp^f_{\max} = 2^{-n+1}$ می‌باشد[۱۷].لذا برای S-box های S7 و S9 داریم :

$$Dp^{s7}_{\max} = Lp^{s7}_{\max} = 2^{-6}$$

$$Dp^{s9}_{\max} = Lp^{s9}_{\max} = 2^{-8}$$

با توجه به ساختار ساده تابع s می‌توان کرانهای بالایی برای $Dp^S_{\max}, Lp^S_{\max}$ را به روش مطروحه در قضیه۲ بدست آورد. لذا با استفاده از قضیه ۲ می توان نتیجه زیر را بیان کرد.

نتیجه ۳[۱۶]: فرض کنید تابع F_2 مطابق شکل(۷) یک تابع r دوری باشد که $r \geq 3$ است و ZE به مفهوم اضافه کردن دو بیت به منتهی الیه سمت چپ و TR به مفهوم حذف دو بیت سمت چپ می باشد، در اینصورت

$$Lp^F_{\max} \leq Lp^{S9}_{\max} Lp^{S7}_{\max}$$

$$Dp^F_{\max} \leq Dp^{S9}_{\max} Dp^{S7}_{\max}$$

اثبات مشابه اثبات قضیه ۲ می باشد و در [۱۶] آمده است.

بنابراین برای تابع S استفاده شده در الگوریتم طارق۲ که در شکل ۸ نشان داده شده است ، طبق نتیجه فوق داریم:

$$Lp^S_{\max} \leq 2^{-8} \times 2^{-6} = 2^{-14} \quad \text{و} \quad Dp^S_{\max} \leq 2^{-8} \times 2^{-6} = 2^{-14}$$

حال تابع دور رمزنگار الگوریتم طارق ۲ ، f را در نظر بگیرید . این تابع همانگونه که در شکل۵-۷ نیز مشخص است،از اتصال سری دو تابع تشکیل شده است که تابع اول یک تابع ترکیب کننده ورودی با کلید می باشد و آنرا F_1 می نامیم و تابع دوم نیز دارای ساختاری مشابه شکل ۹ می باشد و آنرا F_2 می نامیم . لذا طبق قضیه ۴ و با $k_1 = k_2 = 0$ داریم:

$$Lp^{f}_{\max} \le \min\{Lp^{F_1}_{\max}, Lp^{F_2}_{\max}\} \le Lp^{F_2}_{\max}$$

$$Dp^{f}_{\max} \le \min\{Dp^{F_1}_{\max}, Dp^{F_2}_{\max}\} \le Dp^{F_2}_{\max}$$

از طرف دیگر برای تابع F_2 طبق نتیجه ۳ داریم :

$$Dp^{F_2}_{\max} \le Dp^{S}_{\max} Dp^{S}_{\max} = 2^{-14} \times 2^{-14} = 2^{-28}$$

$$Lp^{F_2}_{\max} \le Lp^{S}_{\max} Lp^{S}_{\max} = 2^{-14} \times 2^{-14} = 2^{-28}$$

بنابراین برای تابع دور f الگوریتم طارق ۲ داریم :

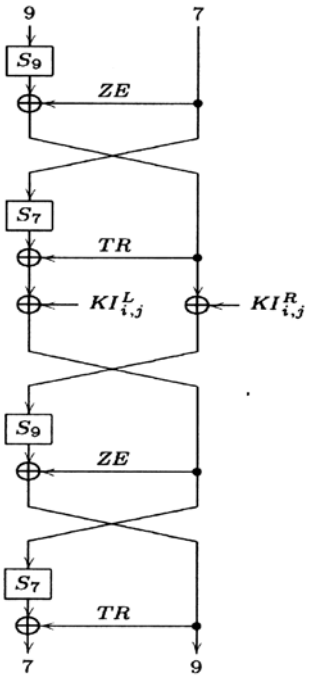
$$Lp^{f}_{\max} \le 2^{-28}$$

$$Dp^{f}_{\max} \le 2^{-28}$$

با توجه به اینکه ساختار کلی الگوریتم طارق ۲ فیستلی است لذا طبق قضیه ۳ برای سه دور از این الگوریتم داریم :

$$Lp^{3-round}_{\max} \le (2^{-28})^2 = 2^{-56}$$

$$Dp^{3-round}_{\max} \le (2^{-28})^2 = 2^{-56}$$



شکل۷ : تابع مطرح در نتیجه ۳

توجه به این نکته نیز مفید است که برای استفاده از قضیه ۳ در الگوریتم طارق ۲ در واقع $K = 0$ است و K' ها نقش کلید را ایفا می کنند یعنی در تابع دور الگوریتم طارق ۲ کلیدی با داده های ورودی XOR نمیشود که معادل با این است که کلید XOR شده صفر است.

حال الگوریتم طارق ۲ شش دوری را در نظر بگیرید. واضح است که شش دور الگوریتم را می توان بصورت اتصال سری یکی از سه حالت زیر در نظر گرفت.

۱- اتصال سری سه دور الگوریتم با سه دور دیگر: در این حالت در بدترین شرایط که خروجی مشخصه ماکزیمم مربوط به سه دور اول با ورودی مشخصه ماکزیمم مربوط به سه دور دوم یکی شود حداکثر احتمال مشخصه ۶ دوری الگوریتم حاصل می‌گردد که عبارت است از $Dp_{\max} = Lp_{\max} = 2^{-56} \times 2^{-56} = 2^{-112}$

۲- اتصال سری چهار دور الگوریتم با دو دور دیگر: در این حالت در بدترین شرایط که خروجی مشخصه ماکزیمم مربوط به چهار دور اول با ورودی مشخصه ماکزیمم مربوط به دو دور دوم یکی شود حداکثر احتمال مشخصه ۶ دوری الگوریتم حاصل می‌گردد که چون طبق نتیجه ۲ از قضیه۱ به ترتیب الگوریتمهای ۴ دوری و ۲ دوری از الگوریتمهای ۳ دوری و ۱ دوری ضعیفتر نیستند پس این حداکثر احتمال عبارت است از $Dp_{\max}^{6-round} = Lp_{\max}^{6-round} = 2^{-56} \times 2^{-28} = 2^{-84}$

۳- اتصال سری پنج دور الگوریتم با یک دور دیگر: در این حالت در بدترین شرایط که خروجی مشخصه ماکزیمم مربوط به پنج دور اول با ورودی مشخصه ماکزیمم مربوط به یک دور دوم یکی شود حداکثر احتمال مشخصه ۶ دوری الگوریتم حاصل می‌گردد که چون طبق نتیجه ۲ از قضیه۱ الگوریتم ۵ دوری از الگوریتم ۳ دوری ضعیفتر نیست پس این حداکثر احتمال عبارت است از $Dp_{\max}^{6-round} = Lp_{\max}^{6-round} = 2^{-56} \times 2^{-28} = 2^{-84}$

لذا در بدترین شرایط $Dp_{\max}^{6-round} = Lp_{\max}^{6-round} = 2^{-84} \prec\prec 2^{-64}$ پس می‌توان گفت که الگوریتم طارق۲ شش دوری کاملا در برابر حملات خطی و تفاضلی مصون است و چون افزایش دور الگوریتم را ضعیف نمی‌کند بنابراین الگوریتم طارق۲ شانزده دوری هم در برابر حملات فوق مصون است.

۵- خلاصه و نتیجه‌گیری

در این مقاله تئوری امنیت قابل اثبات الگوریتمهای رمز قالبی در برابر حملات تفاضلی و خطی مورد بررسی قرار گرفت تا ابزار مفیدی جهت طراحی اینگونه الگوریتمها بدست دهد. نکات قابل توجه این است که اولا فرض استقلال زیر کلیدها همواره صحیح نیست ولی عملا یک فرض تقریبی خوبی تلقی می‌شود. دوم اینکه در اینجا صرفا متوسط پتانسیلهای تفاضلی و خطی مطرح شدند و لذا این امکان وجود دارد که کلیدهای ضعیف‌تری وجود داشته باشند که منجر به نسبتهای انتشار و همبستگی بزرگتری شوند. نهایتا اینکه در این مقاله صرفا مدلهای اولیه حملات تفاضلی و خطی در نظر گرفته شدند و امنیت در برابر این مدلها به معنی امنیت در برابر سایر مدلهای این حملات نیست. با در نظر گرفتن نکات فوق مشاهده شد که الگوریتم طارق ۲ دارای امنیت قابل اثبات در برابر حملات تفاضلی و خطی می‌باشد

مراجع :

[۱] Nyberg,K. , " Linear approximation of block ciphers" , *Advanced in Cryptology-EUROCRYPT'94* ,LNCS 950, Springer-Verlag , pp.439-444 , 1995.

[۲] Nyberg, K., and Knudsen,L. ," Provable security against a differential attack",*Journal of Cryptology*,pp.27-37,1995.

[۳] Matsui,M. ,"New structure of block ciphers with provable security against differential and linear cryptanalysis, *in Fast Software Encryption ' 96*,Vol.1039 , pp. 205-218, Springer-Verlag ,1996.

[۴] Matsui,M. ,"New block encryption algorithm MISTY", *in Fast Software Encryption ' 97*, Vol.1267,pp 54-68, Springer-Verlag 1997.

[۵] ETSI/SAGE.KUSUMI specifications, http://www.etsi.org/dvbandca/3GPP/3gppspecs.html.

[۶] ETSI/SAGE. f_8 and f_9 specifications, http://www.etsi.org/dvbandca/3GPP/3gppspecs.html

[۷] Biham,E., and Shamir,A. , "Differential cryptanalysis of DES-like cryptosystems" *Journal of Cryptology* , Vol.4 , No.1 ,pp.3-72,1991.

[۸] Biham,E. , Biryoukov,A. ,and Shamir,A. , "Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials", *Advanced in cryptology-EUROCRYPT'99*,Vol.1592 of LNCS pp 12-23,Springer-Verlag 1999.

[۹] Biham,E. , Biryoukov,A. ,and Shamir,A. , "Meet in the middle attacks on IDEA and Khufu", *Fast Software Encryption'99*,Vol.1636,pp 124-138, Springer-Verlag 1999.

[۱۰] Knudsen, L.,"Truncated and higher order differentails" *, in Fast Software Encryption ' 95*, Vol 1008 of LNCS , pp. 196-210, Springer –Verlag , 1995.

[١١]National Bureau of Standards , " Data Encryption Standard" , Federal Information Processing Standard 46 , 1977.
[١٢] Wagner,D., " The boomrange attack" , *in Fast Software Encryption* '99,Vol 1636 of LNCS,pp. 156-170 , Springer-Verlag,1999.
[١٣] Matsui,M., "Linear cryptanalysis method for DES cipher" , *Advanced in Cryptology-EOUROCRYPT ' 93*,LNCS 765,1993.
[١٤] Matsui.M. , " The first experimental cryptanalysis of data encryption standard" *Advanced in Cryptology-CRYPTO'9*4,LNCS,No.839,Springer-Verlag,pp.1-11,1994.
[١٥] Lai.X. , Massey,J., and Murphy,S. , " Markov ciphers and differential cryptanalysis " , *Advanced in Cryptology-EUROCRYPT '91* ,LNCS,No. 547,Springer-Verlag , pp.17-38,1991.
[١٦] Wallen,J. , " Design principles of the KASUMI Block Cipher" , www.niksula.cs.hut.fi/~jwallen/kasumi/kasumi.html.
[١٧] Nyberg, K. , "Perfect nonlinear S-box ",*Advanced in Cryptology-EOUROCRYPT ' 91*,pp.378-386,Springer-Verlag,1992.