امنیت قابل اثبات ساختار شبه DES در برابر تحلیل تفاضلی با توابع دور غیر یکسان

زینب سادات فهیم زاد[۱]
بنت الهدی هاشمی[۲]، رقیه تقی زاده[۳]

چکیده

در راستای بررسی امنیت قابل اثبات رمزهای شبه DES در برابر حملات تفاضلی، تا کنون کران بالای احتمال تفاضلی بیشینه، با فرض یکسان بودن توابع دور ارائه گردیده است. مقاله زیر این کران را روی ساختارهایی که در آنها توابع دور غیر یکسان یک به یک و پوشا به کار رفته است به دست می دهد.

کلید واژه

رمزهای قالبی، امنیت قابل اثبات، تفاضل، حملات تفاضلی، تفاضلی بیشینه

۱.کارشناس ارشد ریاضی، دانشگاه شهید بهشتی zsfahimzad@yhoo.com
۲. دانشگاه آزاد اسلامی واحد کرج
۳.دانشکده علوم پایه دانشگاه شیراز
تاریخ دریافت:۸۹/۴/۷ تاریخ پذیرش: ۸۹/۵/۳

مقدمه

مهمترین حملات روی رمزهای بلوکی، حملات تفاضلی [۱] و خطی هستند. هدف اصلی این دو حمله پیدا کردن مشخصه یا مشخصه های احتمالی برای دورهای کاهش یافته یا دور کامل از الگوریتم رمز، جهت تمایز از یک ساختار الگوریتمی تصادفی است. حتی اگر ماکزیمم احتمال مشخصه به اندازه کافی کوچک باشد ممکن است نتواند امنیت الگوریتم رمز قالبی را در برابر حملات مذکور تضمین کند که در این حالت نمی توان ادعا نمود الگوریتم رمز دارای امنیت قابل اثبات در مقابل این حملات است. برای نشان دادن اینکه یک الگوریتم رمز قالبی در برابر حملات خطی و تفاضلی امن است، بایستی نشان دهیم که احتمال تفاضلی بیشینه (خطی)، از یک مقدار به اندازه کافی کوچک، کوچکتر است. برای رسیدن به این هدف، می توان با یافتن تعداد دورهایی از الگوریتم که احتمال مشخصه های تفاضلی و خطی آن از یک مقدار به اندازه کافی کوچک(مثلاً عکس فضای قالب ورودی)، کوچکتر باشد به امنیت قابل اثبات در برابر حملات خطی و تفاضلی دست یافت. لازم به ذکر است که امنیت قابل اثبات برای نخستین بار توسط Nyberg وKnudsen بر روی ساختارهای فیستلی مطرح شد[۲] و مفهوم امنیت قابل اثبات برای طراحی الگوریتم های رمز قالبی به طور آشکار توسط Matsui جهت طراحی ساختار الگوریتم خانوادهMISTY ارائه گردید[۳]. در این مقاله سعی بر آن است که امنیت قابل اثبات رمزهای شبه DES را در مقابل حمله تفاضلی به ازای توابع دور غیر یکسان بررسی نماییم.

رمزهای شبه DES

در این مقاله یک ساختار شبه DES به عنوان یک رمز قالبی تکرار شونده به صورت زیر تعریف میشود[۴]:

فرض کنید که:

$x=(x_L,x_R)\ ;x_L,x_R\in GF(2^n)$ متن اصلی و کلید برابر با $k=(k_1,k_2,...,k_r)\in GF(2^r)$ باشد

اگر متن رمز شده برابر با $y=(y_L,y_R)$ باشد، در r دور با فرض اینکه:

$$x_L(0)=x_L\ ,\ x_R(0)=x_R\ , \tag{۱}$$

به صورت زیر حاصل میگردد:

$$\begin{aligned} x(i)&=(x_L(i)\ x_R(i)\ \ ;i=1,2,...,\ r-1\\ x_L(i+1)&=x_R(i)\\ x_R(i+1)&=x_L(i)\oplus f(x_R(i)\ k(i)\\ y_L(i)&=x_L(i+1)\ \ y_R(i)=x_R(i+1) \end{aligned} \tag{۲}$$

به طوریکه f تابع دور است.

در مرجع[۵]بحث امنیت قابل اثبات در برابر حملات تفاضلی و خطی برای ساختارهای رمز فیستلی تعمیم یافته با فرض یکسان بودن توابع دور، بطور مفصل مطرح گردیده است.

در مقاله ای که پیش رو دارید با فرض غیر یکسان بودن توابع دور، کران بالایی روی احتمال تفاضلی بیشینه یک ساختار شبه DES ارائه میگردد که اگر به اندازه کافی کوچک باشد میتوان به امنیت قابل اثبات در مقابل حمله تفاضلی در این ساختارها دست یافت.

احتمالات تفاضلی r دور

فرض کنید $y = f(x,k)$ که $x, y \in GF(2)^n$ و $k \in GF(2)^m$ باشد. به ازای تفاضل ورودی $\Delta x \in GF(2)^n$ و تفاضل خروجی $\Delta x \in GF(2)^n$، احتمال تفاضلی تابع f به صورت زیر تعریف می شود[۶]:

$$Dp(\Delta x \xrightarrow{f} \Delta y) := \frac{\#\{f(x \oplus \Delta x, k) \oplus f(x,k) = \Delta y\}}{2^n} \quad (۳)$$

احتمال تفاضلی تابع f در رابطه زیر صدق می کند[۴]:

$$\sum_{\Delta y} Dp(\Delta x \xrightarrow{f} \Delta y) = 1 \quad (۴)$$

به ازای تفاضل ورودی $\Delta P = (\Delta P_L, \Delta P_R)$ وتفاضل خروجی $\Delta C = (\Delta C_L, \Delta C_R)$ احتمال تفاضل r-مرحله ای ساختار شبه DES به عنوان یک زنجیر مارکوف به شکل زیر تعریف می شود[۵]:

$$DP(r, \Delta P \to \Delta C) := \sum_{\Delta X, \Delta Y} \prod_{i=1}^{r} Dp(\Delta X_R(i) \to \Delta X_L(i) \oplus \Delta Y_R(i)). \quad (۵)$$

در اینجا $\sum_{\Delta X, \Delta Y}$ جمع کلی روی پارامترهایی به صورت زیر است:

$$\Delta X_L(2) \ldots, \Delta X_L(r)\ \Delta X_R(2) \ldots, \Delta X_R(r)$$
$$\Delta Y_L(1) \ldots, \Delta Y_L(r-1)\ \Delta Y_R(1) \ldots, \Delta Y_R(r-1) \quad (۶)$$

به منظور بررسی امنیت قابل اثبات در مقابل حمله تفاضلی، باید مقدار بیشینه $DP(r, \Delta P \to \Delta C)$ برآورد شود. این مقدار بیشینه به صورت زیر تعریف میگردد:

$$DP(r) := \max_{\Delta P \neq 0, \Delta C} DP(r, \Delta P \to \Delta C) \quad (۷)$$

در بخش بعد، $DP(r)$ به وسیله احتمال تفاضلی بیشینه تابع دور هر مرحله که به صورت زیر تعریف میگردد، برآورد میشود:

$$Max\ Dp_f := \max_{\Delta x \neq 0, \Delta y} Dp(\Delta x \xrightarrow{f} \Delta y) \quad (۸)$$

خاصیت زیر امنیت قابل اثبات را برآورد میکند:

$$DP(r+1) \leq DP(r), \qquad \forall r \geq 1 \quad (۹)$$

این خاصیت نشان میدهد که با افزایش تعداد دورهای الگوریتم، احتمال تفاضلی بیشینه کاهش مییابد.

امنیت قابل اثبات روی رمزهای شبه DES

اگر تفاضل ورودی و خروجی r دور الگوریتم را با $\alpha = (\alpha^L, \alpha^R)$ و $\beta = (\beta^L, \beta^R)$ نشان دهیم، آنگاه با فرض $\alpha = (\alpha^L, \alpha^R) \neq 0$ و یک به یک و پوشا بودن توابع دور، احتمال تفاضلی بیشینه روی سه دور و چهار دور را به صورت زیر برآورد میکنیم :

امنیت قابل اثبات به ازای سه دور

با توجه به رابطه (۵) و شکل ۱ داریم:

$$DP(\alpha \to \beta) = \sum_{\varepsilon_1} DP(\alpha_R \xrightarrow{f_1} \alpha_L \oplus \varepsilon_1) \times DP(\varepsilon_1 \xrightarrow{f_2} \alpha_R \oplus \beta_L) \times DP(\beta_L \xrightarrow{f_3} \varepsilon_1 \oplus \beta_R) \quad (۱۰)$$

با این فرض که $\alpha = (\alpha_L, \alpha_R) \neq 0$، حالات زیر در نظر گرفته میشود:

حالت اول: $\alpha_L \neq 0, \alpha_R = 0$ (از این شرط نتیجه میشود $\varepsilon_1 = \alpha_L \neq 0$)

$$DP(\alpha \to \beta) \leq 1.MaxDP_{f_2} \sum_{\varepsilon_1} DP(\beta_L \xrightarrow{f_3} \varepsilon_1 \oplus \beta_R) = MaxDP_{f_2} \quad (۱۱)$$

حالت دوم: $\alpha_L = 0, \alpha_R \neq 0$ (نتیجه میشود $\varepsilon_1 \neq 0$)

$$DP(\alpha \to \beta) \le \sum_{\varepsilon_1 \neq 0} MaxDP_{f_1} MaxDP_{f_2} DP(\beta_L \xrightarrow{f_3} \varepsilon_1 \oplus \beta_R) \quad (۱۲)$$
$$= MaxDP_{f_1} MaxDP_{f_2} \sum_{\varepsilon_1 \neq 0} DP(\beta_L \xrightarrow{f_3} \varepsilon_1 \oplus \beta_R)$$
$$= MaxDP_{f_1} MaxDP_{f_2}$$

حالت سوم: $\alpha_L \neq 0, \alpha_R \neq 0$

$$DP(\alpha \to \beta) \le MaxDP_{f_1} \sum_{\varepsilon_1} DP(\varepsilon_1 \xrightarrow{f_2} \alpha_R \oplus \beta_L) \quad (۱۳)$$
$$\times DP(\beta_L \xrightarrow{f_3} \varepsilon_1 \oplus \beta_R)$$
$$\le MaxDP_{f_1}[1 \times MaxDP_{f_3} + \sum_{\varepsilon_1 \neq 0} DP(\varepsilon_1 \xrightarrow{f_2} \alpha_R \oplus \beta_L)$$
$$\times DP(\beta_L \xrightarrow{f_3} \varepsilon_1 \oplus \beta_R)]$$
$$\le MaxDP_{f_1}[MaxDP_{f_3} + MaxDP_{f_2}]$$

در حالت کلی برای سه دور رمز شبه DES خواهیم داشت:

$$DP(\alpha \to \beta) \le \max\{MaxDP_{f_2}, MaxDP_{f_1}(MaxDP_{f_2} \quad (۱۴)$$
$$+ MaxDP_{f_3})\}$$

با استناد به مطالب بالا میتوان ادعا نمود که ماکزیمم احتمال تفاضلی رمزهای شبهDES با توابع دور غیر یکسان، روی سه دور، به شرطی که توابع به کار رفته در دورهای آن یک به یک و پوشا باشند، با رابطه (۱۴) کران دار خواهد شد.

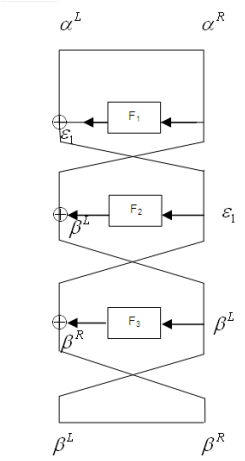
با همان مفروضات بالا می توان امنیت دورهای دیگر را نیز حساب نمود.

امنیت قابل اثبات به ازای چهار دور

$$DP(\alpha \to \beta) = \quad (۱۵)$$
$$\sum_{\varepsilon_1, \varepsilon_2} DP(\alpha_R \xrightarrow{f_1} \varepsilon_1 \oplus \alpha_L) \times DP(\varepsilon_1 \xrightarrow{f_2} \alpha_R \oplus \varepsilon_2)$$
$$\times DP(\varepsilon_2 \xrightarrow{f_3} \varepsilon_1 \oplus \beta_L) \times DP(\beta_L \xrightarrow{f_4} \varepsilon_2 \oplus \beta_R)$$

با فرض اینکه $\alpha = (\alpha_L, \alpha_R) \neq 0$ حالات زیر در نظر گرفته میشود:

حالت اول: $\alpha_L \neq 0, \alpha_R = 0$ (از این شرط $\varepsilon_1 \neq 0$ نتیجه میشود، لذا $\varepsilon_2 \neq 0$).



شکل ۱- الگوی تفاضلی سه دور ساختار شبه DES

$$DP(\alpha \to \beta) \le 1 \times MaxDP_{f_2} MaxDP_{f_3} \sum_{\varepsilon_2} DP(\beta_L \xrightarrow{f_4} \varepsilon_2 \oplus \beta_R) \le MaxDP_{f_2} MaxDP_{f_3} \quad (۱۶)$$

حالت دوم: $\alpha_L = 0, \alpha_R \neq 0$ (از این شرط $\varepsilon_1 \neq 0$ نتیجه میشود:

$$\begin{aligned} DP(\alpha \to \beta) &\le MaxDP_{f_1} \times MaxDP_{f_2} \sum_{\varepsilon_1,\varepsilon_2} DP(\varepsilon_2 \xrightarrow{f_3} \varepsilon_1 \oplus \beta_L) \\ &\times DP(\beta_L \xrightarrow{f_4} \varepsilon_2 \oplus \beta_R) \\ &\le MaxDP_{f_1} MaxDP_{f_2} [\sum_{\varepsilon_1} \sum_{\varepsilon_2} DP(\varepsilon_2 \xrightarrow{f_3} \varepsilon_1 \oplus \beta_L) \\ &\times DP(\beta_L \xrightarrow{f_4} \varepsilon_2 \oplus \beta_R)] \\ &\le MaxDP_{f_1} MaxDP_{f_2} \end{aligned} \quad (۱۷)$$

حالت سوم: $\alpha_L \neq 0, \alpha_R \neq 0$:

$$\begin{aligned} DP(\alpha \to \beta) &\le MaxDP_{f_1} [\sum_{\varepsilon_1} DP(\varepsilon_1 \xrightarrow{f_2} \alpha_R \oplus \varepsilon_2) \\ &\times DP(\varepsilon_2 \xrightarrow{f_3} \varepsilon_1 \oplus \beta_L) \sum_{\varepsilon_2} DP(\beta_L \xrightarrow{f_4} \varepsilon_2 \oplus \beta_R)] \\ &\le MaxDP_{f_1} [\sum_{\varepsilon_1} DP(\varepsilon_1 \xrightarrow{f_2} \alpha_R \oplus \varepsilon_2) \times DP(\varepsilon_2 \xrightarrow{f_3} \varepsilon_1 \oplus \beta_L)] \\ &\le MaxDP_{f_1} [1 \times MaxDP_{f_3} + \sum_{\varepsilon_1 \neq 0} DP(\varepsilon_1 \xrightarrow{f_2} \alpha_R \oplus \varepsilon_2) \\ &\times DP(\varepsilon_2 \xrightarrow{f_3} \varepsilon_1 \oplus \beta_L)] \\ &\le MaxDP_{f_1} [MaxDP_{f_3} + MaxDP_{f_2} \sum_{\varepsilon_1 \neq 0} DP(\varepsilon_2 \xrightarrow{f_3} \varepsilon_1 \oplus \beta_L)] \\ &\le MaxDP_{f_1} [MaxDP_{f_3} + MaxDP_{f_2}] \end{aligned} \quad (۱۸)$$

در حالت کلی برای چهار دور رمز شبه DES خواهیم داشت:

$$DP(\alpha \to \beta) \le \max\{MaxDP_{f_2} MaxDP_{f_3},\ MaxDP_{f_1} MaxDP_{f_2}, MaxDP_{f_1}(MaxDP_{f_2} + MaxDP_{f_3})\} \quad (۱۹)$$

نتیجه گیری

با استناد به مطالب بالا و با توجه به رابطه (۹)، به ازای ساختارهای شبه DES با توابع دور غیر یکسان خواهیم داشت:

$$DP(\alpha \to \beta) \le \max\{MaxDP_{f_2} MaxDP_{f_3},\ MaxDP_{f_1} MaxDP_{f_2}, MaxDP_{f_1}(MaxDP_{f_2} + MaxDP_{f_3})\} \quad \forall r \ge 4$$

که r معرف تعداد دورهاست.

بحث

ارزشمندی کران ارائه شده در این مقاله روی ساختارهای شبه DES زمانی آشکار میگردد که توابع دور متفاوت باشند، زیرا تاکنون مقاله ای در این رابطه ارائه نشده است.

روش ارائه شده در این مقاله در راستای به دست آوردن کران بالا روی احتمال تفاضلی بیشینه، یک روش کلی است و میتوان آن را روی دیگر ساختارهای فیستلی با کمی تغییرات اعمال نمود.

تشکر و قدردانی

در نهایت از گروه تحلیل و ارزیابی الگوریتم های رمز و مدیریت محترم مرکز طراحی و تحلیل الگوریتمهای رمز گروه صافاوا به علت همکاریهای بی دریغ کمال تشکر را داریم.

مراجع

1.E. Biham, A. Shamir, "Differential Cryptanalysis of the Data Encryption Standard", Springer-verlag, 1993.

2.K. Nyberg, L, R Knudsen, “ provable security against a Differential attack,” Crypto’92, 1992.

3.M. Matsui, “New Block Encryption Algorithm MISTY”, FSE’97, Springer-Verlag,1997.

4.Y. Kaneko, S. Moriai, K. Ohta, “On Strict Estimation Method of

ProvableSecurity against Differential and Linear Cryptanalysis", Springer-Verlag, 1997.

5.Y. Kaneko, F. Sano, K. Sakurai, "On provable security against Differential and Linear Cryptanalysis in Generalized Feistel Ciphers with Multiple Random Functions," SAC'97, Springer-Verlag, 1997.

6.Js. Kang, S. Hong, S. Lee, O. Yi, C. Park, J. Lim, "practical and provable security against differential and linear cryptanalysis for Substitution-Permutation network," ETRI Journal, 2001.