مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۱۶-۱۳

حمله تفاضلی– خطی جدید به الگوریتم‌های رمز قالبی

مسعود هادیان دهکردی[1*]، رقیه تقی‌زاده[2]

۱- استاد، دانشکده ریاضی، دانشگاه علم و صنعت ایران، ۲- دانشجوی دکتری دانشگاه علم و صنعت ایران

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۶)

چکیده

تحلیل تفاضلی و خطی دو ابزار اصلی برای بررسی امنیت الگوریتم‌های رمز قالبی است. در این مقاله، یک حمله جدید از نوع متن اصلی انتخاب‌شده به الگوریتم‌های رمز قالبی که ترکیبی از دو حمله تفاضلی و خطی است معرفی می‌شود. در این حمله از مشخصه‌های تفاضلی که در بخشی از الگوریتم رمز با احتمال ۱ ایجاد می‌شود و تقریب‌های خطی که همبستگی آنها دقیقا برابر با صفر است، استفاده می‌شود

واژه‌های کلیدی: رمز قالبی، تحلیل تفاضلی، تقریب خطی

۱- مقدمه[1]

تحلیل تفاضلی یک حمله از نوع متن اصلی انتخاب شده است که برای تحلیل الگوریتم‌های رمز قالبی معرفی شد. این حمله اولین بار در سال ۱۹۹۰ توسط بیهام و شامیر در [۱] معرفی شد. حمله خطی نیز توسط Matsui در سال ۱۹۹۳ در [۲] معرفی شد. این حمله از نوع متن اصلی- معلوم است که از تقریب‌های خطی به عنوان تمایزگر استفاده می‌کند.

حملات تفاضلی و خطی دو ابزار مهم در تحلیل و بررسی امنیت الگوریتم‌های رمز قالبی هستند. به کمک تحلیل تفاضلی و خطی حملات موثری به الگوریتم رمز قالبی DES نسبت به جستجوی جامع در کشف کلید مخفی و شکست الگوریتم رمز ارائه شد [۴-۳]. در حال حاضر نیز از این دو روش به عنوان ابزار اساسی در تحلیل الگوریتم‌های رمز قالبی مورد استفاده قرار می‌گیرد

تحلیل تفاضلی- خطی از ترکیب دو حمله تفاضلی و خطی ایجاد می‌شود. این حمله اولین بار توسط Langford در سال ۱۹۹۵ در [۵] معرفی و بر روی ۸ دور الگوریتم رمز قالبی DES اعمال شد. در این حمله از مشخصه‌های تفاضلی که در دورهایی از الگوریتم رمز با احتمال ۱ رخ می‌دهند استفاده می‌کند. اگر در ادامه این دورها، دورهایی باشند که تقریب خطی مناسب را ایجاد کنند، در این حالت امید داریم برای هر جفت متن اصلی انتخاب‌شده برای کلید درست این تقریب خطی با احتمالی برقرار باشد. این حمله در سال ۲۰۰۲ در مقاله [۶] توسط Biham و Dunkelman بهبود داده شد. در حمله معرفی‌شده مشخصه تفاضلی با احتمال کم‌تر از ۱ برقرار است. در این مقاله ما حمله جدیدی از نوع متن اصلی انتخاب‌شده را معرفی می‌کنیم که ترکیبی از حمله تفاضلی و خطی است و در آن از مشخصه‌های که با احتمال ۱ برای دورهایی از رمز برقرار است و تقریب‌های خطی خاصی که با احتمال ½ رخ می‌دهند استفاده می‌شود. . تحلیل خطی- صفر هم‌بستگی یک روش جدید حمله می‌باشد که یک نوع حمله تمایزی است و در برخی موارد منجر به یافتن کلید رمز در الگوریتم‌های رمز قالبی نیز خواهد شد. این حمله توسط Bogdanov در [۸-۷] معرفی شد.

مابقی این مقاله به این صورت سازمان‌دهی می‌شود که در بخش دوم تعاریف و مقدمات مورد نیاز آورده شده است. بخش سوم به معرفی مختصری از حمله تفاضلی و خطی اختصاص یافته است. در بخش چهارم حمله جدید تفاضلی-خطی معرفی می‌شود و در نهایت در بخش پنجم نتیجه‌گیری خواهیم کرد.

۲- تعاریف و مقدمات

فرض کنید V_n نشان‌دهنده فضای برداری باینری n - بعدی باشد. ضرب داخلی دو بردار $a = (a_1, a_2, \dots, a_n) \in V_n$ و $b = (b_1, b_2, \dots, b_n) \in V_n$ که با $a.b$ نمایش داده می‌شود به صورت زیر تعریف می‌شود:

$$a.b = a_1b_1 \oplus a_2b_2 \oplus \dots \oplus a_nb_n \qquad (1)$$

* رایانامه نویسنده مسئول: mhadian@iust.ac.ir

تابع $f: V_n \to V_1$ یک تابع بولی نامیده می‌شود.

تابع $f: V_n \to V_m$ که $f = (f_1, f_2, \dots, f_m)$ و در آن f_iها تابع بولی‌اند یک تابع بولی برداری از بعد m نامیده می‌شود.

یک تابع بولی برداری از بعد m را می‌توان توسط یک ماتریس باینری $m \times n$ مانند U نمایش داد. فرض کنید سطرهای ماتریس U با u_1، u_2،...و u_m نمایش داده شود لذا هر u_i، یک بردار باینری n- بعدی است.

فرض کنید $Y \in V_n$ یک بردار تصادفی و $p_\eta = Pr(\boldsymbol{Y} = \eta)$ در این صورت بردار $p = (p_0, \dots, p_{2^m-1})$ توزیع احتمال آن می‌باشد.

فرض کنید $f: Vn \to Vm$ یک تابع بولی برداری و $\boldsymbol{X}$ یک متغیر تصادفی در V_n باشد که توزیع آن یک‌نواخت باشد. اگر $\boldsymbol{Y} = f(\boldsymbol{X})$ آن‌گاه $\boldsymbol{Y}$ یک متغیر تصادفی در V_m با توزیع احتمال $p(f) = (p_0(f), \dots, p_{2^m-1}(f))$ می‌باشد، جایی‌که $Pr(f(\boldsymbol{X}) = \eta) = p_\eta(f), \eta \in Vm.$ این توزع احتمال، توزیع احتمال f نامیده می‌شود و با $p(f)$ نمایش داده می‌شود.

دو تابع بولی f و g را از لحاظ آماری مستقل گویند هرگاه متغیرهای تصادفی متناظر با آن‌ها از لحاظ آماری مستقل باشند.

هم‌بستگی میان یک متغیر تصادفی $\boldsymbol{X}$ و مقدار ۰ به صورت $Pr(\boldsymbol{X} = 0) - Pr(\boldsymbol{X} = 1)$ تعریف می‌شود. هم‌بستگی یک تابع بولی $g: V_n \to V_1$ با تابع ۰ که به طور خلاصه هم‌بستگی g نامیده می‌شود به صورت زیر تعریف می‌شود:

$$c(g) = 2\,Pr\,(g(\boldsymbol{X}) = 0) - 1 \qquad (۲)$$

لم: فرض کنید $f: Z_2^n \to Z_2^m$. یک تابع بولی با تابع احتمال p باشد در این صورت به ازای هر $\eta \in Z_2^m$ رابطه زیر برقرار است.

$$p_\eta = 2^{-m} \sum_{a \in F_2^m} (-1)^{a.\eta} c(a.f) \qquad (۳)$$

اثبات: اثبات این لم در مقاله [۱۳] آمده است.

۳- تحلیل تفاضلی و خطی

در این بخش برخی تعاریف و نمادگذاری‌هایی که در حمله تفاضلی و خطی مورد نیاز است آورده شده است.

۳-۱- تحلیل تفاضلی

در تحلیل تفاضلی بررسی می‌کند که یک تفاضل خاص در یک زوج متن اصلی ورودی از یک الگوریتم رمز مانند E با یک کلید ثابت، چه تاثیری در تفاضل خروجی متن رمز شده متناظر با آن می‌گذارد.

تعریف: اگر α و β دو قالب n - بیتی باشند احتمال تفاضل (α, β) برای الگوریتم رمز E که با $\Delta\alpha \to \Delta\beta$ نمایش داده می‌شود به صورت زیر محاسبه می‌شود:

$$Pr_E(\Delta\alpha \to \Delta\beta) = Pr\{E(P) \oplus E(P \oplus \alpha) = \beta\} \qquad (۴)$$

برای یک تابع تصادفی انتظار داریم که مقدار احتمال برای هر تفاضل ورودی α و تفاضل خروجی β برابر با 2^{-n} باشد. بنابراین، اگر مقدار $Pr_E(\Delta\alpha \to \Delta\beta)$ بزرگتر از 2^{-n} باشد می‌توان از تفاضل (α, β) و با در اختیار داشتن مقدار کافی جفت متن اصلی انتخاب‌شده (که هر زوج متن اصلی داری تفاضل α باشد) به‌عنوان یک تمایزگر برای تمیز الگوریتم رمز E از یک جای‌گشت تصادفی، استفاده کرد.

۳-۲- تحلیل خطی

در تحلیل خطی از هم‌بستگی میان یک تابع خطی از قالب ورودی الگوریتم و تابع خطی از قالب خروجی، استفاده می‌کند. بیش‌ترین تابع خطی که مورد استفاده قرار می‌گیرد از ضرب داخلی یک بردار خاص (که به آن ماسک ورودی گفته می‌شود) در قالب ورودی یا ضرب داخلی یک بردار خاص (که به آن ماسک خروجی گفته می‌شود) در قالب خروجی یک الگوریتم رمز ایجاد می‌شوند.

تعریف: اگر α و β دو قالب n - بیتی باشند احتمال یک تقریب خطی با ماسک ورودی α و ماسک خروجی β برای الگوریتم رمز E که گاهی با $\Gamma\alpha \to \Gamma\beta$ نیز نمایش داده می‌شود به صورت زیر تعریف می‌شود:

$$Pr_E(\Gamma\alpha \to \Gamma\beta) = Pr\{P \odot \alpha \oplus E(P) \odot \beta = 0\} \qquad (۵)$$

هم‌بستگی یک تقریب خطی $\Gamma\alpha \to \Gamma\beta$ که با ϵ نمایش داده می‌شود به صورت زیر تعریف می‌شود:

$$\epsilon = 2Pr_E(\Gamma\alpha \to \Gamma\beta) - \frac{1}{2} \qquad (۶)$$

برای یک تابع که به صورت تصادفی انتخاب شده باشد احتمال هر تقریب خطی با ماسک ورودی α و ماسک خروجی β برابر با $\frac{1}{2}$ است. بنابراین دارای هم‌بستگی ۰ است. حال اگر یک تقریب خطی با احتمال مخالف $\frac{1}{2}$ در یک الگوریتم رمز پیدا شود با در اختیار داشتن تعداد کافی زوج متن اصلی- متن رمزشده می‌توان از آن تقریب خطی به عنوان یک تمایزگر برای تمیزدادن الگوریتم رمز از یک جای‌گشت تصادفی، استفاده کرد.

۳-۲- تقریب خطی- صفر هم‌بستگی

فرض کنید E یک رمز قالبی n- بیتی باشد. یک تقریب خطی با

ماسک ورودی α و ماسک خروجی β که برای آن $P(\alpha,\beta)=Pr_E(\Gamma\alpha\to\Gamma\beta)=\frac{1}{2}$، باشد را تقریب خطی با هم‌بستگی صفر نامند. در تحلیل خطی- صفر هم‌بستگی از این نوع تقریب‌های خطی استفاده می‌شود.

۴- معرفی حمله تفاضلی- خطی جدید

در این بخش ابتدا مقدماتی از حمله تفاضلی- خطی ارائه می‌شود سپس حمله جدید را معرفی می‌کنیم.

۴-۱- حمله تفاضلی- خطی

فرض کنید الگوریتم رمز E ترکیبی از دو بخش E_0 و E_1 است، به عبارتی $E=E_0\circ E_1$. اگر $\Delta\alpha\to\Delta\beta$ یک مشخصه تفاضلی با احتمال ۱ برای E_0 باشد و $\Gamma\gamma\to\Gamma\delta$ یک تقریب خطی با اریبی ε برای E_1 باشد به قسمی که $\Delta\beta.\Gamma\gamma=0$ در این صورت تمایزگر تفاضلی- خطی زوج $(\Delta\alpha\to\Delta\beta,\Gamma\gamma\to\Gamma\delta)$ تعریف می‌شود. فرض کنید p و p^* نشان‌دهنده دو زوج متن اصلی باشد که $p\oplus p^*=\Delta\alpha$ در این صورت چون $E_0(p)\oplus E_0(p^*)=\Delta\beta$ لذا با احتمال ۱ رابطه $E_0(p).\Gamma\gamma=E_0(p^*).\Gamma\gamma$ برقرار است. تمایزگر تفاضلی- خطی برابر بررسی برقراری رابطه:

$$\delta.\mathrm{E(p)}\oplus\Gamma\delta.E(p^*)=0 \qquad (۷)$$

یا برقراری رابطه:

$$\Gamma\delta.\mathrm{E(p)}=\Gamma\delta.E(p^*) \qquad (۸)$$

تعریف می‌شود.

احتمال برقراری تمایزگر به‌دست‌آمده با فرض شرایطی که در [۵] آمده است، به صورت زیر می‌باشد:

$$\begin{aligned}&p_r(\delta.\mathrm{E(p)}\oplus\delta.E(p^*)=0)\\&=\left(\frac{1}{2}+\varepsilon\right)\left(\frac{1}{2}+\varepsilon\right)+\left(\frac{1}{2}-\varepsilon\right)\left(\frac{1}{2}-\varepsilon\right)\\&=\frac{1}{2}+2\varepsilon^2 \qquad (۹)\end{aligned}$$

برای یک جای‌گشت تصادفی احتمال برقراری هر تمایزگر تفاضلی- خطی برابر با $\frac{1}{2}$ است بنابراین اگر اریبی رابطه فوق به اندازه کافی بزرگ باشد می‌توان از رابطه فوق به عنوان یک تمایزگر استفاده کرد.

۴-۲- تمایزگر تفاضلی- خطی جدید

برای معرفی تمایزگر تفاضلی- خطی جدید از مشخطه‌های تفاضلی با احتمال ۱ و تقریب‌های خطی با هم‌بستگی صفر استفاده می‌شود.

فرض کنید الگوریتم رمز E ترکیبی از دو بخش E_0 و E_1 است، یعنی $E=E_0\circ E_1$. اگر $\Delta\alpha\to\Delta\beta$ یک مشخصه تفاضلی با احتمال ۱ برای E_0 باشد و $\Gamma\gamma\to\Gamma\delta$ یک تقریب خطی با احتمال $\frac{1}{2}$ یا هم‌بستگی صفر، برای E_1 باشد به قسمی که $\Delta\beta.\Gamma\gamma=0$ در این صورت تمایزگر تفاضلی- خطی زوج $(\Delta\alpha\to\Delta\beta,\Gamma\gamma\to\Gamma\delta)$. تعریف می‌شود. فرض کنید p و p^* نشان‌دهنده دو زوج متن اصلی باشد که $p\oplus p^*=\Delta\alpha$ در این صورت چون $E_0(p)\oplus E_0(p^*)=\Delta\beta$ لذا با احتمال ۱ رابطه $E_0(p).\Gamma\gamma=E_0(p^*).\Gamma\gamma$ برقرار است. تمایزگر تفاضلی- خطی برابر با برقراری $\delta.\mathrm{E(p)}\oplus\Gamma\delta.E(p^*)=0$ یا برقراری رابطه $\Gamma\delta.\mathrm{E(p)}=\Gamma\delta.E(p^*)$ تعریف می‌شود.

احتمال برقراری تمایزگر به‌دست‌آمده با فرض شرایطی که در [۵] آمده است، به صورت زیر می‌باشد:

$$p_r(\delta.\mathrm{E(p)}\oplus\delta.E(p^*)=0)=\frac{1}{2} \qquad (۱۰)$$

بنابراین برای الگوریتم رمز E رابطه (۱۰) با هم‌بستگی، وجود دارد. حال می‌توان از تقریب‌های خطی چندگانه استفاده کرد. فرض کنید $a\in F_2^n$ نشان‌دهنده متن اصلی و $b\in F_2^n$ نشان‌دهنده داده‌ای در فرآیند رمزنگاری باشد. حال اگر m رابطه خطی $z_i=<u_i,a>+<w_i,b>$ در یک الگوریتم رمز با احتمال $\frac{1}{2}$ وجود داشته باشد، می‌توان به‌جای درنظرگرفتن هر بیت و محاسبه توزیع احتمال آن به صورت مستقل، توزیع و m-تایی $z=(z_1,\dots,z_m)$. را به دست آود. از طرفی رابطه میان توزیع احتمال z و مقدار هم‌بستگی c_γ برای هر $\gamma\in F_2^m$ به صورت زیر می‌باشد:

$$\Pr[z]=\sum_{\gamma\in F_2^m}(-1)^{<\gamma,z>}c_\gamma \qquad (۱۱)$$

حال اگر هم‌بستگی میان تمامی تقریب‌های خطی برابر با صفر باشد، به عبارتی برای هر $\gamma\neq 0$ مقدار $c_\gamma=0$ باشد با جای‌گذاری این مقادیر در رابطه (۱۱) و محاسبه مقدار احتمال به این نتیجه خواهیم رسید که متغیر تصادفی z در F_2^m دارای توزیع یکنواخت است.

برای حمله فرض کنید N زوج متن اصلی مجزای (p,p^*) برای یک رمز قالبی$(=E_1\circ E_0)$ E n- بیتی که در آن مشخصه تفاضلی $\Delta\alpha\to\Delta\beta$ با احتمال ۱ برای E_0 و m تقریب خطی $\Gamma\gamma\to\Gamma\delta$ با احتمال $\frac{1}{2}$ یا هم‌بستگی ۰ برای E_1 رخ می‌دهد و علاوه بر این $\Delta\beta.\Gamma\gamma=0$ را در اختیار داشته باشیم. اگر برای $i=1,\dots,m$ مقدار $z_i=\Gamma\delta_i.E(p)\oplus\Gamma\delta_i.E(p^*)$ باشد آن‌گاه طبق رابطه (۱۱) متغیر تصادفی $z=(z_1,\dots,z_m)$ دارای توزیع یک‌نواخت در F_2^m است. بنابراین می‌توان رفتار غیرتصادفی N

داده را از داده‌های تصادفی تمیز داد. فرض کنید $V[z]$ نشان‌دهنده تعداد دفعاتی باشد که z مشاهده می‌شود. در ابتدا برای هر $z \in F_2^m$، $V[z]=0$ مقداردهی اولیه می‌شوند سپس برای هر جفت (p,p^*) مقدار z به کمک تقریب‌های خطی به‌دست‌آمده، محاسبه و به شمارنده آن یکی اضافه می‌شود. اکنون آماره T که در [۱۰] آمده است را محاسبه می‌کنیم

$$T=\sum_{i=0}^{2^m-1}\frac{(V[z]-N2^{-m})^2}{N2^{-m}(1-2^{-m})} \qquad (۱۲)$$

اگر N به اندازه کافی بزرگ انتخاب شده باشد آماره T برای داده‌های تصادفی و داده‌هایی که از رمز آمده‌اند دارای دو توزیع متفاوت به شرح زیر است:

۱- آماره T برای کلید صحیح دارای توزیع کای- دو (خی- دو) با میانگین و واریانس زیر است:

$$\mu_0=2^m\times\frac{2^n-N}{2^n-1} \quad \sigma_0^2=2\times 2^m\times\frac{2^n-N}{2^n-1} \qquad (۱۳)$$

۲- آماره T برای کلید نادرست دارای توزیع خی- دو با میانگین و واریانس زیر است:

$$\mu_1=2^m \quad \sigma_1^2=2\times 2^m \qquad (۱۴)$$

فرض کنید α_0 و α_1 نشان‌دهنده خطای نوع اول و دوم باشند در این صورت مقدار آستانه تصمیم به صورت زیر محاسبه می‌شود:

$$\tau=\mu_0+\sigma_0\times z_{1-\alpha_0}=\mu_1+\sigma_1\times z_{1-\alpha_1} \qquad (۱۵)$$

بنابراین مقدار داده مورد نیاز برای تمیزدادن الگوریتم رمز از یک جای‌گشت تصادفی برابر با مقدار زیر است:

$$N=\frac{2^n(z_{1-\alpha_0}+z_{1-\alpha_1})}{\sqrt{l/2}-z_{1-\alpha_1}} \qquad (۱۴)$$

که در آن، برای $0<p<1$، $z_p=\phi^{-1}(p)$ و تابع ϕ، تابع توزیع تجمعی توزیع نرمال است. احتمال موفقیت حمله برابر، $P_s=1-\alpha_0$ می‌باشد.

۵- نتیجه‌گیری

در این مقاله یک حمله جدید از خانواده حملات تفاضلی- خطی معرفی شد که در آن از تقریب‌های خطی که دارای هم‌بستگی دقیقاً صفر بودند استفاده شد. لازم به ذکر است که در این حمله از تقریب‌های خطی که هم‌بستگی آن‌ها صفر است و در حمله تفاضلی- خطی نادیده گرفته می‌شدند، استفاده شده است. از نتایج به‌دست‌آمده می‌توان الگوریتم‌های رمز قالبی که شرایط فوق را داشته باشند مورد تحلیل و بررسی قرار داد.

۶- مراجع

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," In: A. Menezes, S. A. Vanstone, (eds.) CRYPTO 1990, LNCS, vol. 537, pp. 2-21, Springer, Heidelberg, 1990.

[2] M. Matsui and A. Yamagishi, "A new method for known plaintext attack of FEAL cipher," In: R. A. Rueppel, (ed.) EUROCRYPT 1992, LNCS, vol. 658, pp. 81-91, Springer, Heidelberg, 1993.

[3] E. Biham and A. Shamir, "Differential cryptanalysis of the full 16-round DES," In: E. F. Brickell, (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 487-496, Springer, Heidelberg, 1993.

[4] M. Matsui, "Linear cryptanalysis method for DES cipher," In: T. Helleseth, (ed.) EUROCRYPT 1993, LNCS, vol. 765, pp. 386-397, Springer, Heidelberg, 1994.

[5] S. K. Langford and M. E. Hellman, "Differential-linear cryptanalysis. In: Y. Desmedt, (ed.) CRYPTO 1994, LNCS, vol. 839, pp. 17-25, Springer, Heidelberg, 1994.

[6] E. Biham, O. Dunkelman, and N. Keller, "Enhancing differential-linear cryptanalysis," In: Y. Zheng, (ed.) ASIACRYPT 2002, LNCS, vol. 2501, pp. 254-266, Springer, Heidelberg, 2002.

[7] A. Bogdanov and V. Rijmen, "Linear Hulls with Correlation Zero and Linear Cryptanalysis of Block Ciphers," Designs, Codes and Cryptography, Springer-Verlag, to appear, 2012. Preprint available as Cryptology ePrint Archive: Report 2011/123, http://eprint.iacr.org/2011/123.

[8] A. Bogdanov and M. Wang, "Zero Correlation Linear Cryptanalysis with Reduced Data Complexity," FSE'12, LNCS, Anne Canteaut (ed.), Springer-Verlag, to appear, 2012.

[9] A. Bogdanov, G. Leander, K. Nyberg, and M. Wang, "Integral and Multidimensional Linear Distinguishers with Correlation Zero," In: X. Wang, K. Sako, (eds.) ASIACRYPT 2012, LNCS, vol. 7658, pp. 244–261, Springer, 2012.

[10] A. Bogdanov, G. Leander, K. Nyberg, and M. Wang, "Integral and Multidimensional Linear Distinguishers with Correlation Zero," IACR ePrint Archive report, 2012.

[11] H. Soleimany and K. Nyberg, "Zero-correlation linear cryptanalysis of reduced-round LBlock," Designs, Codes and Cryptography, vol. 73, no. 2, pp. 683-698, 2014.

[12] E. Biham, "On Matsui's linear cryptanalysis," In Proc. The Workshop on the Theory and Application of Cryptographic Techniques, pp. 341-355, May 1994.