بازنمایی تقریبات خطی الگوریتم رمز معماگر با گراف*

شیرین نیلی‌زاده†، بابک صادقیان‡

چکیده

ارزیابی امنیتی الگوریتم‌های رمز قطعه‌ای از طریق مقاومت آنها در مقابل حملات شناخته شده، صورت می‌گیرد. یکی از مهمترین حملات، تحلیل خطی می‌باشد. یافتن یک مشخصه خطی مناسب قسمت بسیار مهمی از این حمله است.

در این مقاله، بازنمایی تقریبات خطی الگوریتم رمز معماگر با یک گراف مطرح می‌شود. این مدل، فضای تمامی تقریبات خطی الگوریتم رمز را به صورت یک گراف چندسطحی وزن‌دار یکطرفه نشان می‌دهد، بطوریکه مسئله یافتن بهترین مشخصه خطی الگوریتم رمز متناظر با یافتن کوتاهترین مسیر گراف است. جهت بدست آوردن گراف نمایش تقریبات خطی الگوریتم رمز معماگر، در ابتدا گراف متناظر با هر جز از الگوریتم رمز بدست آورده می‌شود. سپس با تعریف توابع الحاق و تقسیم، ترکیب موازی و متوالی اجزا یک دور از الگوریتم رمز تعریف می‌شود و گراف متناظر با هر دور ساخته می‌شود. در آخر گراف متناظر با تقریبات خطی کل الگوریتم رمز با توجه به دو ساختار SPN و شبه DES موجود در الگوریتم رمز معماگر بدست آورده می‌شود. در انتها چگونگی بکارگیری شیوه بهینه‌سازی اجتماع مورچه‌ها جهت جستجوی مشخصه‌های مناسب بر روی گراف تقریبات خطی الگوریتم رمز معماگر شرح داده و نتایج بدست آمده ارائه می‌شود.

کلمات کلیدی

تحلیل خطی، تقریبات خطی، مشخصات خطی، مدل‌سازی تقریبات خطی، گراف وزن‌دار یکطرفه، الگوریتم‌های رمز شبیه به DES، ساختار SPN، شیوه بهینه‌سازی اجتماع مورچه‌ها،

Linear Approximations Representation of Moamagar Block Cipher

Shirin Nilizadeh, Babak Sadeghiyan

Abstract

The security of block ciphers is assessed through their resistance to known attacks. One of the most important attacks is linear cryptanalysis. In this paper, we describe a model for presenting linear approximations for Moamagar block cipher. This graph shows the whole space of linear approximations for the block cipher algorithm is presented through its obtained multi-level weighted directed graph, such that the problem of searching for the best linear characteristic is equivalent to searching for the minimum weight path in the directed graph. We first show how to present linear approximations for different components used in this block cipher through graphs. Then we present split and merge graphs which are used to define the sequential and parallel combination operations. These operations join the obtained graphs of components to construct the graph for one round of the cipher. At last the graph for the cipher with both SPN and DES-like structure will be obtained. At the end, we use the ant colony optimization to search for efficient linear characteristics of Moamagar block cipher and we show the obtained results.

Keywords

Linear Cryptanalysis, Linear Approximations, Linear Characteristics, Weighted Directed Graph, Ant Colony Heuristic Search Algorithm.

---

* این مقاله با پشتیبانی مرکز تحقیقات مخابرات انجام شده است.

† کارشناسی ارشد مهندسی فناوری اطلاعات- امنیت اطلاعات، دانشگاه صنعتی امیرکبیر، shirin.nili@cic.aut.ac.ir

‡ عضو هیأت علمی دانشگاه، دانشگاه صنعتی امیرکبیر، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، basadegh@ce.aut.ac.ir

۱- مقدمه

یکی از ابزارهای تامین امنیت داده‌ها، الگوریتم‌های رمزنگاری هستند. ارزیابی امنیتی این الگوریتم‌ها از طریق مقاومت آنها در مقابل حملات شناخته شده، صورت می‌گیرد. یکی از مهمترین حملات، تحلیل خطی می‌باشد.

تحلیل خطی یک حمله از نوع متن واضح معلوم است که توسط ماتسویی مطرح شد[۱،۲]. تحلیل‌گر در این روش تحلیل، رابطه‌های خطی بین متن واضح، متن رمز شده و کلید مخفی را مورد مطالعه قرار می‌دهد. اولین گام در تحلیل خطی بدست آوردن مشخصات خطی موثر برای الگوریتم رمز است، بطوریکه جستجوی بهترین مشخصه خطی قسمت بسیار مهمی از این حمله می‌باشد. الگوریتم‌هایی جهت جستجوی بهترین مشخصه خطی الگوریتم‌های رمز، مطرح شده‌اند، ولی هنوز هیچ الگوریتم عملی که بهترین مشخصه را برای کل تعداد دورها بدون هیچ محدودیتی پیدا کند، ارائه نشده است. اولین روش جستجو که توسط ماتسویی ارائه شد[۳]، مشخصه‌های خطی مناسبی را برای سیستم‌های رمز شبیه به DES بدست می‌داد ولی برای بعضی از سیستم‌های رمز مانند FEAL به اندازه کافی سریع عمل نمی‌کرد. البته با اعمال بعضی محدودیتها بر روی نوع مشخصات خطی و استفاده از تکنیکهایی مانند استفاده از مشخصات خطی تکرار شونده[1] [۴،۵]، استفاده از تقریبات خطی چندگانه[۶] و با کاهش تعداد دورها، پیچیدگی جستجو کاهش می‌یابد.

الگوریتم جستجوی دیگری جهت بهبود الگوریتم جستجوی ماتسویی[۷] مطرح شده است. این الگوریتم، الگوی جستجویی را برای کاهش کاندیدهای نامناسب جستجو معرفی می‌کند. این الگوریتم نتایج بهترو سریعتری را در الگوریتم FEAL بدست می‌دهد و نتایج مشابهی با روش ماتسویی در DES حاصل می‌شود.

بدست آوردن الگوریتمی موثر برای یافتن بهترین مشخصات خطی مستقل از ساختار سیستم رمز حائز اهمیت است. در این مقاله، مدل بازنمایی تقریبات خطی الگوریتم‌های رمز قطعه‌ای با استفاده از گراف را بیان می‌کنیم، بطوریکه هر الگوریتم رمز قطعه‌ای دلخواه با ساختار SPN و نیز شبه DES، به یک گراف نگاشت می‌شود و مشخصه‌های خطی آن الگوریتم رمز قطعه‌ای توسط یک گراف جهت‌دار وزن‌دار نشان داده می‌شود. در نتیجه مشخصه‌های خطی را می‌توان بصورت سیستماتیک و با بکارگیری از الگوریتم جستجوی مناسب مانند شیوه بهینه سازی اجتماع مورچه‌ها، بدست آورد.

ایده استفاده از تئوری گراف جهت جستجوی بهترین تقریبات خطی، اولین بار در [۸] مطرح شد. در این مرجع مدل مجردی بدون ذکر جزئیات برای فقط ساختار شبه DES و نه برای همه اجزا الگوریتم بیان شده است، بطوریکه به چگونگی مدل اجزا مختلف یک الگوریتم رمز به گراف و ترکیب آنها، پرداخته نشده است. در کاری مرتبط، مدل بازنمایی عملکرد تفاضلی برای جستجوی بهترین مشخصه تفاضلی توسط آقایان قائمی و صادقیان ارائه شده است[۹].

در این مقاله، مدل بازنمایی تقریبات خطی الگوریتم رمز معماگر مطرح می‌شود. شیوه بهینه‌سازی اجتماع مورچه‌ها جهت جستجوی مشخصه‌های مناسب بر روی گراف تقریبات خطی الگوریتم رمز معماگر بکار گرفته می‌شود و نتایج بدست آمده ارائه می‌شود. این شیوه بهینه‌سازی بصورت تصادفی عمل می‌کند و در حل مسائل مختلفی که دارای فضای جستجوی بالایی هستند، بکار گرفته می‌شود[۱۰][۱۱].

در این راستا، در بخش دوم، تعاریف و مفاهیم اولیه مورد نیاز بیان می‌شود. بخش سوم شامل معرفی اجمالی الگوریتم رمز معماگر است. در بخش چهارم ایده مدل بازنمایی تقریبات خطی الگوریتم‌های رمز با اعمال آن بر روی الگوریتم رمز معماگر مطرح می‌شود. این بخش شامل زیر بخش‌های بازنمایی اجزا مختلف الگوریتم‌های رمز و بالاخص الگوریتم رمز معماگر و ترکیب گراف‌های حاصل از اعمال مدل بر روی آنها با توجه به ساختار الگوریتم رمز است. در بخش پنجم شیوه بهینه‌سازی اجتماع مورچه‌ها، نحوه بکارگیری آن بر روی گراف حاصل از بازنمایی معماگر و نتایج حاصل جهت یافتن مشخصه‌های مناسب برای این الگوریتم رمز بیان می‌شوند. در بخش ششم از مباحث مطرح شده نتیجه گیری شده و بخش هفتم شامل مراجع می‌باشد.

۲- تعاریف و مفاهیم اولیه

اولین گام در تحلیل خطی بدست آوردن مشخصات خطی موثر برای الگوریتم رمز است. به این ترتیب که در ابتدا در مرحله طراحی حمله، با استفاده از ساختار الگوریتم رمز و ویژگیهای اجزای داخلی و با شناسایی و بکارگیری آسیب پذیریها و نقاط ضعف آن، از میان تقریب‌های خطی با احتمال بالا، یک مشخصه خطی آماری مناسب بین بیتهای ورودی و خروجی هر تابع و سپس هر دور ساخته می‌شود. سپس با ترکیب مشخصه‌های یک دوری، یک مشخصه r دوری مناسب برای کل الگوریتم، که r تعداد دورهای الگوریتم رمز است، بدست می‌آید. این مشخصه خطی، رابطه‌ای خطی بین ورودی و خروجی الگوریتم رمز را نشان می‌دهد و باعث شناسایی کلید می‌شود. در انتها در مرحله اجرای حمله بایستی بتوان به تعداد کافی زوج متن رمز متناظر با مشخصه بدست آمده در مرحله قبل، بدست آورد و با بکارگیری آنها کلید رمز را شناسایی کرد. همانطور که ملاحظه می‌شود، جستجوی بهترین مشخصه خطی قسمت بسیار مهمی از این حمله می‌باشد.

در ادامه این مقاله، نمادهای P، C و K بترتیب متن واضح، رمز شده و کلید یک سیستم رمز را نشان می‌دهند. بیت‌های ورودی، کلید و خروجی توابع، S-boxها و غیره از سمت راست به چپ شماره‌گزاری می‌شوند و اولین بیت از سمت راست، شماره صفر را به خود می‌گیرد. نماد $A[i]$ ، نشان‌دهنده مقدار بیت iام از بردار یا قطعه A است. C_i مقدار رمز شده از دور iام را نشان می‌دهد بطوریکه $P=C_0$ و $C=C_r$

است. در سیستمای رمز با ساختار شبیه DES، C_i به دو قسمت C_i^H و C_i^L تقسیم می شوند و به ترتیب قطعه با بیتهای باارزش‌تر و قطعه با بیتهای کم ارزش‌تر را نشان می‌دهند. نماد ● ضرب اسکالر دو بردار دودویی را نشان می‌دهد. در این قسمت به بیان چند تعریف از مفاهیم تحلیل خطی می‌پردازیم :

تعریف ۱ - تقریب خطی. یک تقریب خطی، یک تابع خطی است که عمل یک تابع غیرخطی را تقریب می‌زند و برای یک تبدیل $m\times n$، وابستگی خطی بین بیتهای ورودی، خروجی و کلید را بدست می‌آورد.

تعریف ۲ - ماسک ورودی/ خروجی. ماسک ورودی/ خروجی، یک بردار دودویی در $GF(2)$ است، که زیرمجموعه‌ای از بیتهای ورودی/خروجی را مشخص می‌کند. بطور مثال اگر A یک بردار n بیتی باشد، ماسک بردار A، Γ_A نیز برداری است که اگر در بردار A ضرب اسکالر[۲] شود، بیتهایی از A که در Γ_A مقدار یک را به خود گرفته‌اند، انتخاب می‌کند. بطور مثال اگر $A=1011$ و $\Gamma_A=0001$ باشد، در نتیجه $A\bullet\Gamma_A=0\oplus 0\oplus 0\oplus 1=A[i_4]$ بدست می‌آید.

تعریف ۳ - جدول تقریبات خطی[۳]. جدول تقریبات خطی برای یک تابع $f:\{0,1\}^m\to\{0,1\}^n$ ، بصورت یک جدول $2^m\times 2^n$ تعریف می‌شود، بطوریکه اگر x ورودی m بیتی و $y=f(x)$ خروجی n بیتی این تابع باشد. ماسک ورودی $\Gamma_X\in\{0,1\}^m$، شماره سطر و ماسک خروجی $\Gamma_Y\in\{0,1\}^n$، شماره ستون را مشخص می‌کند. عناصر جدول $L_a(\Gamma_X,\Gamma_Y)$ که بوسیله شماره سطر و ستون ارجاع داده می‌شوند، بصورت زیر محاسبه می‌شود:

$$L_a(\Gamma_X,\Gamma_Y)=\#\{x\mid 0\le x\le 2^m,\Gamma_X\bullet x=\Gamma_Y\bullet f(x)\} \qquad (۱)$$

تعریف ۴ - مشخصه خطی یک دوری. مشخصه خطی یک دوری، رابطه‌ای خطی بین بیت‌های متن واضح، متن رمز شده و کلید است که برای یک دور از الگوریتم تعریف می شود. این مشخصه با احتمالی همراه است، که احتمال(p) وقوع چنین تقریبی را از میان کلیه تقریب‌های ممکن بیان می‌کند. گاهی به جای کمیت احتمال،کمیت بایاس(q) به همراه مشخصه بیان می‌شود، بطوریکه $q=|p-1/2|$ است. مشخصه خطی تنها در صورتی مفید است که $p\neq 1/2$ و یا $q\neq 0$ باشد. هر چه مقدار بایاس بزرگ‌تر باشد، مشخصه خطی مفیدتر است و برای تعیین مقدار کلید وابسته به مشخصه به تعداد کمتری متن واضح و رمزشده نیاز خواهد بود.

$$(C_{i-1}\bullet\Gamma C_{i-1})\oplus(C_i\bullet\Gamma C_i)=K_i\bullet\Gamma K_i\,;\quad q=|p-1/2| \qquad (۲)$$

تعریف ۵ - مشخصه خطی r دوری. با ترکیب مشخصه‌های یک دوری، یک مشخصه r دوری بدست می‌آید که r، تعداد دورهای الگوریتم رمز است.

$$\Gamma P\bullet P+\Gamma C\bullet C+\sum_z \Gamma K_z\bullet K_z=0,\quad 0\le p=|q+1/2|\le 1 \qquad (۳)$$

با استفاده از لم انباشتگی[۴][۱]، می‌توان احتمال (p) مشخصه خطی r دوری یک الگوریتم رمز را با دانستن احتمال مشخصه‌های خطی یک دوری $p_i(0\le i\le r)$ ، محاسبه نمود.

$$p=1/2+2^{r-1}\prod_{i=1}^{r}(p_i-1/2) \qquad (۴)$$

تعریف ۶ – تقریب خطی نامعتبر. یک تقریب خطی را نامعتبر می‌نامیم، اگر احتمال آن مساوی ½ باشد.

۳- معرفی الگوریتم رمز معماگر

الگوریتم رمز قطعه‌ای معماگر، یک الگوریتم رمز با اندازه قطعه و کلید ۱۶۰ بیت است[۱۲] که تاکنون یک حمله از نوع تحلیل تفاضلی[۱۳] بر روی آن گزارش شده است و نیز یک حمله خطی بر روی ۵ دور از آن [۱۴] ارائه شده است. این الگوریتم رمز بصورت زیر بیان می‌شود:

$$C=K_{13}\oplus(V_1^{-1}\circ SP^{-1}\circ T_2\circ SP\circ V_2^{-1}\circ SP^{-1}\circ T_3\circ SP\circ V_2\circ SP^{-1}\circ T_1\circ SP\circ V_1(K_0\oplus P)) \qquad (۵)$$

هر یک از توابع V_1 و V_2 متشکل از ۳۲ تابع جانشینی ۵ بیت به ۵ بیت است که به موازات یکدیگر عملیات خود را انجام می‌دهند. مجموعاً از ۶۴ تابع جانشینی در این الگوریتم رمز استفاده می‌شود، که شامل هشت تکرارِ هشت تابع جانشینی است. تابع T_3 ترکیبی از دو تابع T_1 و T_2 است و هر یک از این توابع متشکل از ۵ تابع ۳۲ بیت به ۳۲ بیت هستند که به موازات یکدیگر عمل می‌کنند و در آنها از ۸ تابع جانشینی ۶ بیت به ۴ بیت استفاده می‌شود. از میان توابع مورد استفاده، تنها دو تابع T_1 و T_2 کلیددار هستند.

همانطور که مشاهده می‌شود، الگوریتم رمز معماگر شامل هر دو ساختار SPN و شبه DES است، که تحلیل این الگوریتم را پیچیده می‌کند.

۴- ایده مدل بازنمایی تقریبات خطی الگوریتم‌های رمز

گلوگاه اصلی تحلیل خطی، بررسی فضای بسیار بزرگ تقریبات خطی مختلف یک دوری جهت حصول بهترین مشخصه خطی برای کل الگوریتم رمز است. این فضا با افزایش تعداد دور الگوریتم رمز، بطور نمایی افزایش می‌یابد. با ارائه مدل بازنمایی تقریبات خطی الگوریتم رمز، اندازه گراف با افزایش تعداد دور، بطور خطی افزایش می‌یابد. برای بیان چگونگی نمایش تقریبات خطی یک الگوریتم رمز بصورت گراف، ابتدا نحوه نگاشت اجزا آن و سپس نحوه ترکیب گراف‌های بدست آمده با توجه به ساختار الگوریتم بیان می‌شود. در نهایت برای هر الگوریتم رمز، یک گراف جهت‌دار وزن‌دار چند سطحی بدست خواهد آمد. بطوریکه مسئله یافتن بهترین مشخصه برای یک الگوریتم رمز معادل

یافتن یک راه بین دو گره معین در گراف تقریبات خطی است که شامل چندین مسیر است. در بخش‌های بعدی به ایده مدل با بیانی غیر ریاضی و بصورت کلی پرداخته می‌شود و روند نگاشت الگوریتم رمز معماگر به درخت فضای ترکیبات ممکن مشخصه‌ها نشان داده می‌شود.

۴-۱- بازنمایی تقریبات خطی اجزا الگوریتم رمز

هر الگوریتم رمز قطعه‌ای از ترکیب اجزا یا توابع کوچک بدست می‌آید. در یک دسته‌بندی، توابع به دو دسته کلی توابع خطی مانند توابع گسترش و توابع جایگشت بیتی و توابع غیرخطی مانند توابع جانشینی تقسیم می‌شوند.

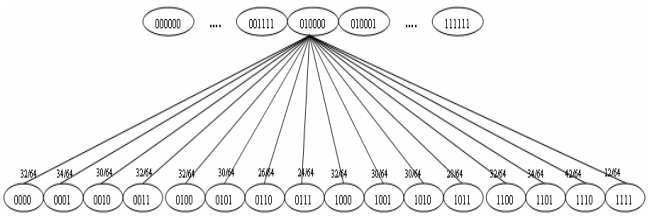
۴-۱-۱- توابع غیرخطی

معمولاً توابع غیرخطی مورد استفاده در الگوریتم‌های رمز بصورت توابع جانشینی هستند. این توابع را می‌توان بصورت $f:\{0,1\}^m \rightarrow \{0,1\}^n$ نشان داد که یک دنباله m بیتی را به یک دنباله n بیتی نگاشت می‌کند. در این مدل، توزیع تقریبات خطی ماسک‌های ورودی/خروجی در یک تابع توسط یک گراف جهت‌دار وزن‌دار دوبخشی $G(V, E, W)$ با $2^m + 2^n$ گره بیان می‌شود. 2^m گره بعنوان گره‌های آغازی با اندیس‌های دودویی ۰ تا $2^m - 1$ نامگذاری می‌شود. یالهای این گراف بر اساس جدول توزیع تقریبات خطی تابع f تعیین می‌شود و وزن هر یال برابر قرینه لگاریتم (در مبنای دو) مقدار متناظر با آن در جدول توزیع تقریبات خطی است. درنتیجه اگر مقدار متناظر با ماسک ورودی/خروجی (Γ_x, Γ_y) در جدول توزیع تقریبات خطی برابر p باشد، وزن این یال بصورت $W_{\Gamma_x,\Gamma_y} = -\log_2\left|p-\frac{1}{2}\right|$ خواهد بود.

توابع غیر خطی الگوریتم رمز معماگر شامل توابع جایگزینی V-boxها در توابع V و S-boxها در توابع T هستند. برای نمونه قسمتی از نمایش تقریبات خطی تابع جایگزینی S-box5 در تابع T الگوریتم رمز بصورت شکل ۱ است. مقدار عددی روی هر یال احتمال همراه با تقریب خطی بدست آمده از آن ماسک ورودی و خروجی را نشان می‌دهد. مقدار وزن هر یال با استفاده از این احتمال بدست می‌آید. تابع جایگزینی S-box5 در جدول ۱ بیان شده است. بهترین تقریب خطی این تابع جایگزینی شامل ماسک ورودی "0x10" و ماسک خروجی "F"است.

جدول ۱. تابع جایگزینی S-box5 در الگوریتم رمز معماگر

Input(6 bits)	00	01	02	03	04	…	3C	3D	3E	3F
Output(4 bits)	2	E	C	B	4	…	0	5	E	3



شکل (۱): نمایش تقریبات خطی تابع جایگزینی S-box5 الگوریتم رمز معماگر با ماسک ورودی "0x10".

۴-۱-۲- توابع خطی

توابع خطی نیز در بسیاری از الگوریتم‌های رمز بصورت توابع جانشینی تعریف می‌شوند، در نتیجه می‌توان نحوه بازنمایی توابع غیر خطی را بطور مشابه بر روی آنها اعمال نمود با این تفاوت که وزن هر یال از گراف برابر صفر در نظر گرفته شود. زیرا که به ازای یک ماسک ورودی، یک ماسک خروجی با احتمال یک بدست می‌آید و احتمال دیگر ماسک‌های خروجی به ازاء این ماسک ورودی برابر $1/2$ است که غیرخطی بودن تقریب‌ها را نشان می‌دهد، درنتیجه نمی‌توان آنها را در تقریبات خطی شرکت داد. در گراف متناظر با یک تابع خطی، هر گره ورودی تنها به یک گره خروجی متصل است.

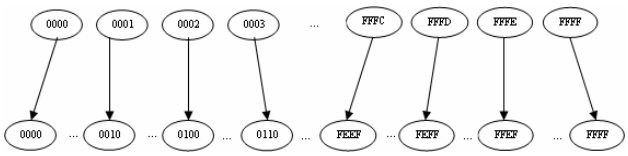
الگوریتم رمز معماگر شامل چندین تابع خطی است. این توابع عبارتند از توابع sp و sp^{-1} که بین دو دور V و T قرار می‌گیرند و توابع جابه جایی IP، FP، E و P موجود در توابع T می‌باشد. برای مثال نمایش تقریبات خطی تابع جابه‌جایی ۱۶ بیتی در این الگوریتم بصورت شکل ۲ است. تابع جابه‌جایی در جدول ۲ و نحوه نگاشت ماسک‌های ورودی و ماسک‌های خروجی آن در جدول ۳ بیان شده‌اند.

جدول ۲. تابع جابه‌جایی ۱۶ بیتی در الگوریتم رمز معماگر

تابع جابه‌جایی (P)							
۱۶	۴	۵	۱۲	۱	۱۵	۷	۱۰
۲	۸	۱۴	۱۱	۳	۹	۶	۱۳

جدول ۳. نحوه نگاشت ماسک‌های ورودی به ماسک‌های خروجی تحت تابع جابه‌جایی ۱۶ بیتی در الگوریتم رمز معماگر

Input mask	0000	0001	0002	…	FFFC	FFFD	FFFE	FFFF
Output mask	0000	0010	0100	…	FEEF	FEFF	FFEF	FFFF



شکل(۲): نمایش تقریبات خطی تابع جابه‌جایی الگوریتم رمز معماگر

۴-۲- ترکیب گراف‌های حاصل از بازنمایی اجزا

هر الگوریتم رمز شامل چندین دور است. با ترکیب گراف‌های حاصل از بازنمایی هر یک از اجزاء الگوریتم رمز، گراف بازنمایی یک دور از الگوریتم بدست می‌آید. توابع موجود در یک دور به دو صورت متوالی و موازی با هم ترکیب می‌شوند.

۴-۲-۱- گراف حاصل از ترکیب موازی دو تابع

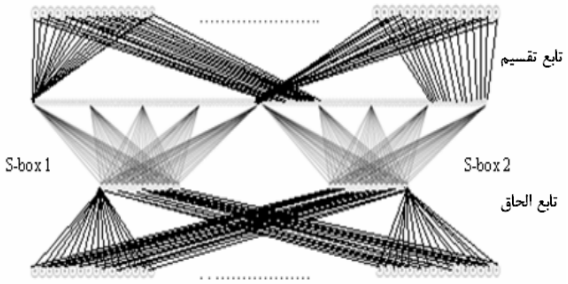
ترکیب موازی دو تابع $f_1:\{0,1\}^{m_1}\to\{0,1\}^{n_1}$ و $f_2:\{0,1\}^{m_2}\to\{0,1\}^{n_2}$ بصورت $F_P = f_2 \parallel f_1:\{0,1\}^{m_1+m_2}\to\{0,1\}^{n_1+n_2}$ تعریف می‌شود، بطوریکه اگر آرگومان $x\in\{0,1\}^{m_1+m_2}$، الحاق دو رشته $x_1\in\{0,1\}^{m_1}$ و $x_2\in\{0,1\}^{m_2}$ باشد، $F_p(x)$ از الحاق دو رشته $f_1(x_1)$ و $f_2(x_2)$ بدست می‌آید. برای نمایش گراف حاصل از ترکیب موازی دو تابع، در ابتدا بایستی دو گراف الحاق و تقسیم بیان شوند.

گراف الحاق، گرافی است که دو قطعه m و n بیتی را به یکدیگر ملحق می‌کند و یک قطعه $m+n$ بیتی را تشکیل می‌دهد. گراف الحاق شامل 2^m+2^n گره ورودی و 2^{m+n} گره خروجی است. اگر گره‌های ورودی در دو دسته در نظر گرفته شوند، که دسته اول شامل 2^m گره m بیتی و دسته دوم شامل 2^n گره n بیتی باشد، یک گره ورودی m بیتی از دسته اول به یک گره از 2^m+2^n گره خروجی $m+n$ بیتی متصل می‌شود، اگر m بیت اول از گره خروجی برابر گره ورودی m بیتی باشد و یک گره ورودی n بیتی از دسته اول به یک گره از 2^m+2^n گره خروجی $m+n$ بیتی متصل می‌شود، اگر n بیت آخر از گره خروجی برابر گره ورودی n بیتی باشد.

گراف تقسیم، گرافی است که یک قطعه $m+n$ بیتی را به دو قطعه m و n بیتی تقسیم می‌کند. گراف تقسیم شامل 2^{m+n} گره ورودی و 2^m+2^n گره خروجی است. اگر گره‌های خروجی در دو دسته در نظر گرفته شوند، که دسته اول شامل 2^m گره m بیتی و دسته دوم شامل 2^n گره n بیتی است. یک گره ورودی $m+n$ بیتی به یک گره از 2^m گره خروجی m بیتی متصل می‌شود، اگر m بیت اول از گره ورودی $m+n$ بیتی برابر گره ورودی m بیتی باشد و یک گره ورودی $m+n$ بیتی به یک گره از 2^n گره خروجی n بیتی متصل می‌شود، اگر n بیت آخر از گره ورودی برابر گره خروجی n بیتی باشد.

ترکیب موازی گرافهای حاصل از بازنمایی تقریبات خطی دو تابع f_1 و f_2، بصورت یک گراف چهارسطحی متشکل از گراف تقسیم m_1+m_2 بیتی به دو قطعه m_1 و m_2 بیتی، گراف‌های نمایش تقریبات خطی توابع f_1 و f_2 و گراف الحاق دو قطعه n_1 و n_2 بیتی است، در این صورت، گره‌های آغازی گراف ترکیب موازی، گره‌های ورودی به گراف تقسیم و گره‌های پایانی آن، گره‌های خروجی گراف الحاق است. گره‌های خروجی گراف تقسیم و گره‌های ورودی گراف الحاق، به ترتیب بر گره‌های خروجی و گره‌های ورودی گراف‌های نمایش تقریبات خطی توابع f_1 و f_2 منطبق می‌باشد. در نتیجه از هر گره آغازی دو یال خارج می‌شود و دو مسیر را تا یک گره پایانی ایجاد می‌کند. بصورت قضیه‌ای می‌توان نشان داد که هر راهی که شامل دو مسیر است، متناظر با یک مشخصه خطی تابع $f_1 \parallel f_2$ است.

از جمله ترکیبهای موازی توابع در الگوریتم رمز معماگر می‌توان به ترکیب موازی V-boxهای هر دور V، ترکیب موازی T-boxهای هر دور و ترکیب گراف‌های حاصل از S-boxها در توابع T اشاره نمود. برای مثال نمایش تقریبات خطی ترکیب موازی دو S-box بصورت شکل ۳ بدست می‌آید. در گراف حاصل، 2^{12} نود ۱۲ بیتی به دو دسته با 2^6 نود ۶ بیتی تقسیم می‌شوند که نودهای ورودی به گراف توابع S-boxها را تشکیل می‌دهند. نودهای خروجی گراف‌های S-boxها، نودهای ورودی به گراف الحاق هستند و نودهای خروجی گراف الحاق منطبق بر نودهای پایانی گراف ترکیب موازی دو تابع خواهد بود.



شکل (۳): گراف نمایش تقریبات خطی ترکیب موازی دو تابع S-box

۴-۲-۲- گراف حاصل از ترکیب متوالی دو تابع

ترکیب متوالی دو تابع $f_1:\{0,1\}^{m_1}\to\{0,1\}^{n_1}$ و $f_2:\{0,1\}^{m_2}\to\{0,1\}^{n_2}$ بصورت زیر تعریف می‌شود، بطوریکه رابطه $n_1 = m_2$ باید برقرار باشد:

$$F_s = f_2 o f_1:\{0,1\}^{m_1}\to\{0,1\}^{n_2}: \quad \forall x\in\{0,1\}^{m_1}; F_s(x) = f_2(f_1(x))$$

گراف حاصل از این ترکیب، یک گراف سه سطحی است به گونه‌ای که رئوس سطح اول آن، رئوس ورودی گراف نمایش تقریبات خطی تابع f_1 است. رئوس سطح دوم آن، رئوس خروجی گراف متناظر با تابع f_1 است. رئوس پایانی، رئوس خروجی گراف متناظر با تابع f_2 است. یالهای بین رئوس سطح اول و دوم و نیز بین رئوس سطح دوم و سوم، همان یالهای گراف نمایش تقریبات خطی تابع f_1 و تابع f_2 است. طبق قضیه‌ای نشان داده می‌شود که در گراف حاصل از ترکیب متوالی گرافهای متناظر با دو تابع f_1 و f_2، هر مسیر از یک گره آغازی به گره پایانی متناظر با یک مشخصه خطی از تابع $f_2 o f_1$ است.

ترکیب متوالی توابع در دورهای الگوریتم رمز معماگر شامل ترکیب متوالی گراف حاصل از توابع S-box و گراف حاصل از تابع جابه‌جایی از توابع T است.

۴-۳- ترکیب گراف‌های حاصل از بازنمایی اجزا با توجه به ساختار الگوریتم‌های رمز قطعه‌ای

نحوه انتشار ماسک‌ها به ساختار الگوریتم بستگی دارد. در این مرحله برای بدست آوردن مشخصه خطی کل الگوریتم رمز، می‌بایست با توجه به ساختار الگوریتم رمز، گراف‌های حاصل از بازنمایی دورها را ترکیب نمود. معمولاً در سیستم‌های رمز از دو ساختار SPN و شبه DES در ترکیب دورها استفاده می‌شود. در ادامه تقریب خطی این دو ساختار مورد مطالعه قرار می‌گیرند. در انتخاب تقریبات خطی، باید خنثی شدن تقریب‌های خطی دورهای میانی در نظر گرفته شود، بطوریکه مشخصه نهایی تنها شامل ماسک ورودی و ماسک خروجی الگوریتم باشد.

۴-۳-۱- ساختار شبه DES

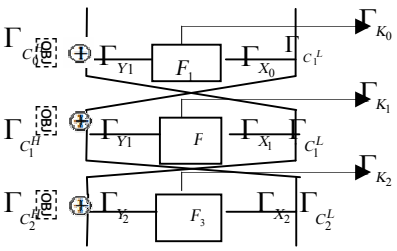
ساختار شبه DES مطابق با شکل ۴، شامل عملیات XOR و تکرار[۵] است. نحوه انتشار ماسک‌ها در این دو تابع در تحلیل خطی متفاوت از نحوه عمل معمول آنها و مکمل یکدیگر است[۱۵]. بدین معنی که مدل تقریب خطی XOR، عملگری است که به جای دو ورودی، یک ماسک ورودی دریافت می‌کند و همان ماسک ورودی را در دو ماسک خروجی خود کپی می‌کند. در حالیکه مدل تقریب خطی عملگر تکرار، عملگری است که دو ماسک ورودی را دریافت می‌کند و نتیجه حاصل از XOR آنها را به تنها ماسک خروجی خود نسبت می‌دهد. انتشار ماسک‌ها در الگوریتم‌های رمز شبه DES با توجه به خصوصیات آنها طبق روابط زیر خواهد بود[۴]:

$$\Gamma_{X_i} = \Gamma_{C_{i-1}^H} \oplus \Gamma_{C_{i+1}^H} \qquad i = 2,\ldots,r-1 \qquad (۶)$$

$$\Gamma_{Y_i} = \Gamma_{C_i^H} \qquad (۷)$$

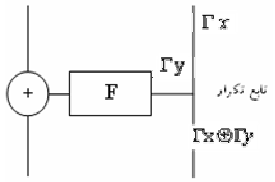
$$\Gamma_{C_i^L} = \Gamma_{C_{i-1}^H} \qquad (۸)$$

$$Y = X_{i-1} \oplus X_{i+1} \qquad (۹)$$



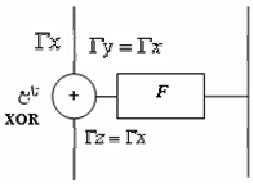
شکل (۴): سیستم رمز شبه DES

گراف بازنمایی عمل تکرار، گرافی است که سه گراف بدست آمده از بازنمایی سه دور متوالی از الگوریتم رمز را به یکدیگر متصل می‌کند(شکل ۵). واضح است که این عمل بر روی ماسک‌هایی با تعداد بیت یکسان n عمل می‌کند. این گراف دارای 2^{2n} گره آغازی است که از دو دسته 2^n گره پایانی گراف بازنمایی دور i-1 و 2^n گره ورودی گراف بازنمایی دور i تشکیل شده است. تعداد گره پایانی گراف حاصل 2^n است و متناظر با گره‌های پایانی به گراف بازنمایی دور i+1 است. در گراف بازنمایی عمل تکرار، دو گره آغازی به یک گره پایانی متصل می‌شوند، اگر XOR دو ماسک ورودی از دو دسته مختلف مساوی ماسک گره خروجی شود. در نتیجه عمل تکرار، دو مسیر متفاوت را ادغام کرده و به یک مسیر تبدیل می‌کند. بطوریکه یک مسیر به یک گره پایانی دور i+1 وجود دارد، اگر و فقط اگر دو مسیر به گره پایانی دور i-1 و گره ورودی i وجود داشته باشد و این دو ماسک برابر ماسک گره پایانی دور i+1 باشد.



شکل (۵): ساختار جریان ماسک‌ها در عملگر تکرار

گراف بازنمایی عمل XOR، نیز مشابه با عمل تکرار، محل تلاقی سه گراف حاصل از بازنمایی سه دور متوالی است(شکل ۶). به طور مشابه این عمل نیز بر روی ماسک‌هایی با تعداد بیت یکسان n عمل می‌کند. این گراف نیز دارای 2^{2n} گره آغازی است که از دو دسته 2^n گره ورودی گراف بازنمایی دور i-1 و 2^n گره خروجی گراف بازنمایی دور i تشکیل شده است. تعداد گره پایانی گراف حاصل 2^n است و متناظر با گره‌های ورودی به گراف بازنمایی دور i+1 است. در گراف بازنمایی عمل XOR، دو گره آغازی به یک گره پایانی متصل می‌شوند، اگر هر دو ماسک گره ورودی از دو دسته مختلف مساوی ماسک گره خروجی باشند. در نتیجه، عمل XOR نیز دو مسیر متفاوت را ادغام کرده و به یک مسیر تبدیل می‌کند. بطوریکه یک مسیر به یک گره پایانی دور i+1 وجود دارد، اگر و فقط اگر دو مسیر به گره ورودی دور i-1 و گره خروجی i وجود داشته باشد و هر دو ماسک‌ها برابر و مساوی ماسک گره ورودی دور i+1 باشد.



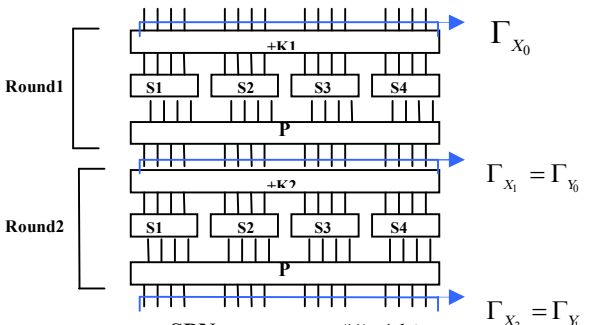
شکل (۶): ساختار جریان ماسک‌ها در تابع XOR

۴-۳-۲- ساختار جایگزینی-جابه‌جایی[۶] (SPN)

ساختار SPN مطابق با شکل ۷ است که هر دور شامل دو مرحله توابع جایگزینی و توابع جابه‌جایی است. روابط زیر با توجه به خصوصیات این ساختار، برقرار می‌باشد:

$$\Gamma_{X_i} = \Gamma_{Y_{i-1}} \qquad i = 2,\ldots,r-1 \qquad (۱۰)$$

$$X_i = Y_{i-1} \qquad (۱۱)$$



شکل (۷): سیستم رمز SPN

نحوه ترکیب گراف‌های بازنمایی هر دور با توجه به این ساختار جهت تولید گراف کل الگوریتم، مشابه با ترکیب متوالی گراف‌های متناظر با توابع است. به این ترتیب که گره‌های پایانی دور iام منطبق بر گره‌های ورودی بر تابع خطی می‌باشد. گره‌های پایانی گراف حاصل از تابع خطی منطبق بر گره‌های آغازین تابع تقسیم جهت تولید گره‌های آغازین هر یک از توابع جایگزینی دور $i+1$ است. از یک گره پایانی دور iام به یک گره آغازین دور $i+1$ مسیر وجود دارد، اگر و فقط اگر حاصل تابع جابه‌جایی بر روی ماسک گره پایانی دور iام برابر ماسک گره آغازین دور $i+1$ باشد.

با تعمیم مطالب بخش چهارم برای بیش از دو تابع، می‌توان نشان داد که گراف حاصل از ترکیب گراف‌های نمایش تقریبات خطی چند جزء از الگوریتم رمز، بیانگر فضای ترکیبات مختلف مشخصه‌های خطی ترکیب این اجزا از الگوریتم رمز است. به همین ترتیب می‌توان نشان داد که هر راه شامل چندین مسیر از نود آغازی گراف تا نود پایانی گراف، مشخصه‌ای خطی از الگوریتم رمز را نشان می‌دهد. تعداد یال‌هایی که برای بدست آوردن مشخصه خطی الگوریتم طی می‌شوند، دارای پیچیدگی $O(m\times n)$ است، که m حداکثر تعداد جز در یک دور از الگوریتم رمز و n تعداد دورهای الگوریتم رمز را نشان می‌دهد. اگر یک الگوریتم رمز n دوری که هر دور آن شامل k جز غیرخطی است، را در نظر بگیریم. تعداد کل یال‌های گراف حاصل از بازنمایی تقریبات خطی الگوریتم رمز برابر $n\times\sum_{l=1}^{k}(2^{m1_l}+2^{m2_l})$ خواهد بود. همانطور که مشاهده می‌شود، سایز گراف حاصل برابر $O(n)$ است. این در حالی است که گراف جستجوی تقریبات خطی بدون استفاده از مدل ارائه شده، دارای پیچیدگی با درجه نمایی می‌باشد. با بکارگیری این مدل، پیچیدگی گراف جستجو از درجه نمایی به درجه خطی متناسب با تعداد دور الگوریتم رمز کاهش می‌یابد.

۵- بکارگیری شیوه بهینه‌سازی اجتماع مورچه‌ها و تعیین مشخصه‌ای مناسب برای الگوریتم رمز معماگر

با استفاده از مدل بازنمایی تقریبات خطی الگوریتم، یک الگوریتم رمز به گرافی وزن‌دار و جهت‌دار تبدیل می‌شود که تمامی مشخصه‌های خطی آن را نشان می‌دهد. هر راه شامل چند مسیر از یک گره آغازی به یک گره پایانی در این گراف متناظر با یک مشخصه خطی است. بنابراین با توجه به تعریف وزن یال‌ها در این مدل، مسئله یافتن بهترین مشخصه برای این الگوریتم رمز معادل یافتن کم وزن‌ترین راه شامل چند مسیر بین یک گره ورودی به یک گره خروجی از این گراف است. می‌توان برای یافتن راه شامل چند مسیر مناسب در گراف نمایش تقریبات خطی الگوریتم رمز قطعه‌ای از شیوه بهینه‌سازی اجتماع مورچه‌ها استفاده نمود. این شیوه با الهام از مسیریابی مورچه‌ها در یافتن مسیر بین لانه تا محل آذوقه ابداع شده است. نکته قابل توجه در این شیوه، آن است که مورچه‌ها بدون داشتن اطلاعات کامل از کل مسیرها و تنها بر اساس اطلاعات محلی (اسیدهای بجا مانده از مورچه های قبلی در مسیر) کوتاهترین مسیر را پیدا می‌کنند. به این ترتیب که مورچه‌ها در هنگام پیمایش مسیر، اثری از اسید فورمیک به جای می‌گذارند و تنها کانال ارتباطی بین مورچه‌ها از طریق همین اسید فورمیک به جا مانده در مسیرها است. هر مورچه در مسیریابی، اسید فورمیک مسیرهای پیش‌رو را بو کرده و بطور احتمالی بر اساس میزان غلظت اسید هر یک از مسیرها، یکی را انتخاب می‌کند. پس از گذشت مدتی از شروع کار مورچه‌ها، همگی از کوتاهترین مسیر فاصله بین دو نقطه را طی خواهند نمود.

۵-۱- بکارگیری روش پیش‌رو- پس‌رو

گراف حاصل از بازنمایی تقریبات خطی یک الگوریتم رمز، با توجه به خصوصیات خاص آن الگوریتم قابل پالایش می باشد. با توجه به اینکه در تبدیلات خطی تنها یک انتخاب وجود دارد و وزن یال متناظر برابر صفر است، می‌توان زیرگراف‌های معادل توابع خطی را حذف نمود و دو گره متناظر با ماسک ورودی و خروجی تابع خطی را ادغام نمود و یک گره بدست آورد. با توجه به صفر بودن وزن یال‌های گراف‌های الحاق و تقسیم، می‌توان آنها را نیز در نظر نگرفت

با توجه به ویژگی مطلوب انتشار در الگوریتم‌های رمز، با انتخاب یک ماسک ورودی غیرصفر در ورودی، از یک دور به دور بعد ماسک‌های غیر صفر بیشتری انتخاب خواهند شد. بطوریکه با فعال شدن یکS-box در ورودی بعد از چند دور اغلب S-boxها فعال می‌شوند. فعال شدن بیشتر S-boxها طبق لم انباشتگی باعث انتخاب مشخصه‌ای خطی با احتمال کمتر می‌شود. در نتیجه می‌توان با محدود کردن S-boxهای فعال، مشخصه‌های مفیدتری را بدست آورد. برای دستیابی به حداقل انتشار، روش پیش‌رو- پس‌رو مطرح می‌شود. در این روش، گراف نمایش تقریبات الگوریتم رمز به دو قسمت تقسیم می‌شود و تنها یک S-box فعال در دور میانی در نظر گرفته می‌شود و یک مشخصه خطی از دور میانی تا دور پایانی(روند پیش‌رو) و یک مشخصه خطی از دور میانی تا دور آغازی(روند پس‌رو) بدست آورده می‌شود. با اتصال این مشخصه‌ها، مشخصه مطلوب بدست می‌آید.

برای مثال برای بدست آوردن مشخصه خطی سه دوری الگوریتم رمز معماگر، مورچه‌ها به صورت پیش‌رو یک دور $T1$ و یک دور $V2$ را می‌پیمایند و یک دور $V1$ بصورت پس‌رو طی می‌شود.

۵-۲- یافتن راه شامل چند مسیر در گراف نمایش تقریبات خطی الگوریتم رمز معماگر

بطور خلاصه الگوریتم‌های اجتماع مورچه‌ها دارای ۴ مولفهٔ گراف الگوریتم، مورچه‌ها، مکانیزم انتخاب گره بعدی و مکانیزم بهنگام‌سازی فورمیک است. مورچه‌ها از گره آغازی شروع کرده و بسوی گره پایانی به پیش می‌روند. به این ترتیب، هر مورچه یک راه شامل چند مسیر را

از میان راه‌های شامل چند مسیر ممکن بین گره آغازی و گره پایانی انتخاب کرده و آن را می‌پیماید.

گراف الگوریتم، متناظر با گراف حاصل از بازنمایی تقریبات خطی الگوریتم رمز معماگر است. تعداد مورچه‌ها و تعداد اجتماع مورچه‌های مورد استفاده در سرعت همگرایی مورچه‌ها موثر است و با توجه به رنج وزن یال‌ها تعریف می‌شود. مکانیزم انتخاب گره بعدی به صورتی است که مورچه با توجه به وزن یال‌های خارج شده از گره حاضر به گره‌های سطح بعدی بصورت تصادفی یک گره را انتخاب می‌کنند. تابع انتخاب تصادفی به گونه‌ای است که احتمال انتخاب یال‌های با احتمال بالاتر بیشتر می‌باشد.

مکانیزم بهنگام رسانی در شیوه اجتماع مورچه‌ها دارای پارامتر تشویق است. مکانیزم بهنگام‌سازی فورمیک، افزایش میزان اسید یال(وزن یال) انتخاب شده همزمان با عبور از راه انتخاب شده و افزایش مجدد بهترین راه پیموده شده توسط اجتماعی از مورچه‌ها است.

ساختار توابع T که شامل عملگرهای تکرار و XOR می‌باشد، در الگوریتم رمز معماگر بگونه‌ای است که ماسک خروجی توابع f و h زودتر از ماسک ورودی به این توابع بدست می‌آید. در نتیجه گراف معکوس این توابع در ترکیب گراف‌ها و گراف کل الگوریتم رمز مورد استفاده قرار می‌گیرد.

به منظور نشان دادن توانایی مدل مطرح شده در ارائه تقریبات خطی یک الگوریتم رمز، در این مقاله مشخصه‌هایی مناسب برای سه دور از الگوریتم رمز معماگر، با استفاده از گراف نمایش تقریبات خطی الگوریتم رمز معماگر و شیوه بهینه‌سازی اجتماع مورچه‌ها بدست آورده شده است. همانطور که گفته شد، مورچه‌ها به صورت پیش‌رو یک دور $T1$ و یک دور $V2$ را می‌پیمایند و یک دور $V1$ بصورت پس‌رو طی می‌شود. در ضمن گراف مورد استفاده در توابع $T1$، معکوس توابع f و h هستند. مسیرهایی که مورچه‌ها در گراف نمایش تقریبات خطی سه دور از الگوریتم رمز معماگر بایستی طی کنند، مطابق با شکل ۸ است. در شکل هر بیضی، مجموعه‌ای از نودهای ورودی به تابع و یا خروجی از تابع را نشان می‌دهد. برای ساده نمودن شکل، جزئیات گراف بازنمایی تقریبات خطی توابع f و h نمایش داده نشده‌اند.

مشخصه‌های بدست آمده از بکارگیری شیوه بهینه‌سازی مورچه‌ها بر روی یک تابع h در جدول ۴ نشان داده شده است. مشخصه بدست آمده تنها شامل یک S-box فعال می‌باشد و بهترین مشخصه را مشخص می‌کند. توابع V دارای توزیع خطی یکنواختی هستند و ماسک‌های ورودی و خروجی یا تقریب خطی نامعتبری را ایجاد می‌کنند و یا تقریب خطی با احتمال $1/2+2^{-3}$ را تشکیل می‌دهند، یک مشخصه با این احتمال از تابع $V1$ در جدول ۵ نشان داده شده است. مشخصه‌های بدست آمده برای یک دور $T1$ در جدول ۶ آورده شده است. با مطالعه مشخصه‌های بدست آمده برای $T1$ مشاهده می‌شود که ماسک ورودی و ماسک خروجی تابع f مساوی صفر بدست آمده است. با تحلیل تابع $T1$، این نکته بدست می‌آید که تنها امکان صفر شدن ماسک ورودی و خروجی یک تابع f و یا h وجود دارد و از آنجا که تابع h دارای مشخصه‌هایی خطی با بایاس بالاتری است، درنتیجه بهتر آن است که تابع f در تشکیل مشخصه نهایی شرکت نداشته باشد. این نکته می‌تواند به عنوان نقطه ضعفی در طراحی الگوریتم رمز معماگر بحساب بیاید و پیشنهاد می‌شود که نحوه بکارگیری توابع f و h جابه‌جا شود. بطوریکه از تابع f دو بار و از تابع h یکبار در تابع T استفاده شود. مشخصه‌های بدست آمده برای سه دور $V1$، $T1$ و $V2$ در جدول ۷ آورده شده است.

جدول ۴ . مشخصه‌های تابع h موجود در توابع T

احتمال	ماسک خروجی	ماسک ورودی
$\frac{1}{2}+2^{-1.678}$	0x8421	0x8000

جدول ۵ . مشخصه‌های تابع $V1$

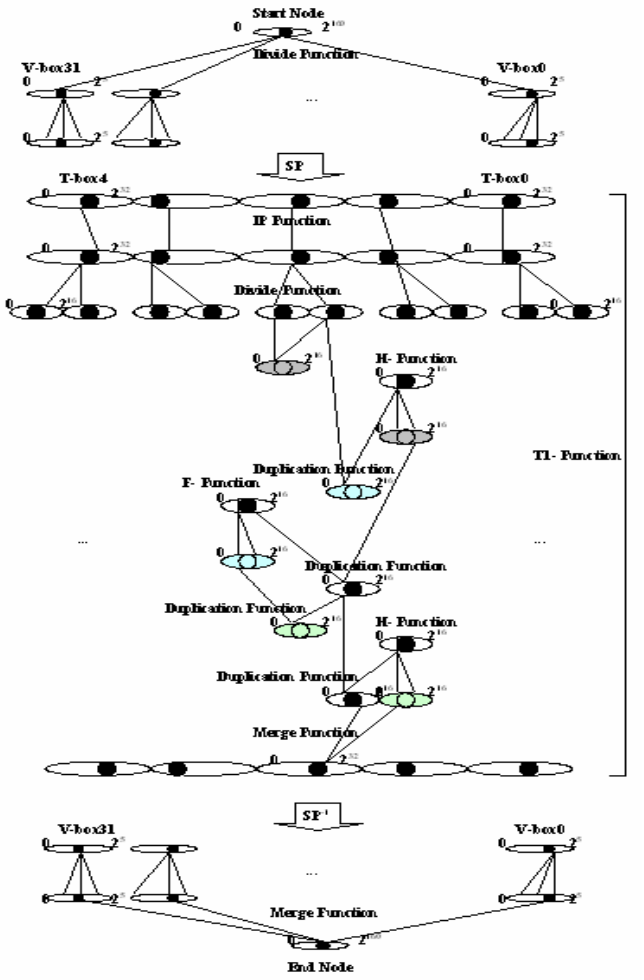
احتمال	ماسک خروجی					ماسک ورودی				
$\frac{1}{2}+2^{-3}$	0	0	0	03800000	0x0	0	0	0	8000000	0x0

جدول ۶ . مشخصه‌های تابع $T1$

احتمال	ماسک خروجی		ماسک ورودی	
$\frac{1}{2}+2^{-2.356}$	0421	8421	1080	0x104
$\frac{1}{2}+2^{-3}$	111A	1112	0003	0x5401
$\frac{1}{2}+2^{-3.093}$	0421	8421	1C40	0xC207

جدول ۷ . مشخصه‌های سه دور $V1$، $T1$ و V2

بایاس	ماسک خروجی					ماسک ورودی				
$2^{-12.415}$	0	1000	0	0	0	0	0	18006	0	0x40000000
$2^{-12.415}$	0	1200	0	0	0	0	0	01A002	0	0x0
2^{-13}	0	0	E8	0	20000000	0	0	0	0	0x0



شکل(۸):گراف نمایش تقریبات خطی سه دور از الگوریتم رمز معماگر

همانطور که مشاهده می‌شود، مشخصه بدست آمده از سه دور دارای احتمال کمتری نسبت به جمع احتمال بهترین مشخصه‌های هر یک از اجزا بصورت جداگانه است که این بدلیل این است که در ترکیب توابع انتخاب ماسک ورودی و یا ماسک خروجی بصورت آزادانه انجام نمی‌شود و به ماسک‌های دورهای قبل و بعد بستگی دارد. به طور مثال با انتخاب بهترین مشخصه خطی بدست آمده از تابع $T1$، بیش از یک تقریب خطی از هر یک از دورهای V فعال می‌شوند و در کل مشخصه‌ای با احتمال کمتری را بدست می‌دهد.

مشخصه بدست آمده برای سه دور از الگوریتم رمز دارای احتمال بالاتری نسبت به مشخصه بدست آمده از تحلیل خطی انجام شده بر روی این الگوریتم رمز در مرجع [۱۴] است. بطوریکه بایاس بدست آمده از تحلیل خطی الگوریتم رمز معماگر برابر $28.4217042\times 2^{-49.82892}$ است، درحالیکه با استفاده از روش بیان شده در این مقاله بایاس مشخصه بدست آمده برابر $2^{-12.415}$ می‌باشد. از این روش می‌توان برای بدست آوردن مشخصه‌ای مناسب برای کل الگوریتم رمز استفاده نمود.

۶- نتیجه

در این مقاله، نحوه بازنمایی تقریبات خطی الگوریتم رمز قطعه‌ای معماگر بصورت گراف بیان شد. نحوه تبدیل، بر اساس نوع اجزا الگوریتم و ساختار آن الگوریتم صورت می‌گیرد. برای یافتن مشخصه خطی کل الگوریتم بایستی گراف متناظر برای هر دور محاسبه شود و سپس بر اساس ساختار الگوریتم، گراف کل الگوریتم بدست آورده شود. بر این اساس در ابتدا اجزا الگوریتم بطور کلی به دو دسته خطی و غیر خطی تقسیم و نحوه تبدیل تقریبات خطی هر یک از این اجزا به اجزا گراف ارائه شد. با تعریف توابع الحاق و تقسیم، ترکیب موازی و متوالی اجزا در یک دور از الگوریتم رمز تعریف شد. در آخر چگونگی نگاشت دو ساختار الگوریتم‌های رمز که در الگوریتم رمز معماگر از آنها بهره برده شده و پیچیدگی تحلیل آن را بالابرده است، بیان شد. بعد از نمایش فضای تقریبات خطی الگوریتم رمز، بیان شد که مسئله یافتن بهترین مشخصه خطی الگوریتم رمز متناظر با یافتن کوتاهترین راه شامل چندین مسیر گراف است. برای یافتن بهترین راه شامل چندین مسیر، در این مقاله شیوه بهینه‌سازی اجتماع مورچه‌ها پیشنهاد شده است، که به مروری اجمالی بر این شیوه و نحوه بکارگیری آن بر روی چند جز و نیز سه دور از الگوریتم رمز معماگر پرداخته شد. در این راستا استفاده از تکنیک پیش رو و پس رو مطرح شد و نشان داده شد که با استفاده از پالایش گراف و با توجه به خصوصیات الگوریتم رمز، می‌توان فضای جستجو را کاهش داد. در پایان نتایج بدست آمده اعمال این روش طی جداولی آورده و با نتایج بدست آمده از تحلیل خطی این الگوریتم رمز در [۱۴] مقایسه شده است. به این ترتیب با بیان مدل بازنمایی تقریبات خطی الگوریتم‌های رمز قطعه‌ای، قدمی رو به جلو برای اتوماتیک‌سازی تحلیل خطی برداشته شده است.

مراجع

[1] Matsui, M., "*Linear cryptanalysis method for DES cipher*", Advances in Cryptology, Proceedings of Eurocrypt'93, LNCS 765, Springer-Verlag, pp. 16--30, 1993.

[2] Matsui, M., Yamagishi, A., "*A New Method for Known plaintext Attack on FEAL Cipher*", Advances in Cryptology, Proceedings of Eurocrypt'93, LNCS 765, Springer- Verlag, pp. 386-397, 1993.

[3] Matsui, M., "*On correlation between the order of S-boxes and the strength of DES*", Advances in Cryptology, Proceedings of Eurocrypt'94, LNCS 950, Springer-Verlag, pp. 366-375, 1995.

[4] Knudsen, L. R., "*Iterative Characteristics of DES and s2-DES*", Advances in Cryptology, Proceedings of Eurocrypt'92, LNCS 658, Springer-Verlag, 1993.

[5] Lee, S., Sung, S., Kim, K., "*An Efficient Method to Find the Linear Expressions for Linear Cryptanalysis*", JW-ISC'95. Jan.24-27, Inuyama, Japan, 1995.

[6] Burton, S., Kaliski, Jr., Robshaw, M.J.B., "*Linear Cryptanalysis Using Multiple Approximations*", Advances in Cryptology, Proceedings of CRYPTO'94, LNCS 0839, Springer-Verlag, pp. 26-39, 1994.

[7] Ohta, k., Moriai, S., Aoki, K., "*Improving the Search Algorithm for the Best Linear Expression*", Advances in Cryptology Proceedings of CRYPTO '95, L NCS 963, pp.157--170, Springer-Verlag, 1995.

[8] Buttyán, L., Vajda, I., "*Searching for the best linear approximation of DES-like cryptosystems*", IEE Electronics Letters, vol. 31, no. 11, pp. 873-874, May 1995.

[9] Ghaemi Bafghi, A., Sadeghiyan, B., "*Differential Model of Block Ciphers with Ant Colony Technique*", Proceedings of Workshop on Coding, Cryptography and Combinatorics, China, 2003.

[10] White, T., Bruchstein, A.M., "*An Ant-Inspired Heuristic for recognizing Hamiltonian Graphs*", IEEE Conference on Svolutionary Computation CEC99, Vol. 2, 1999.

[11] Guoying, L., Subing, Z., Zemin, L., "*Distributrd Dynamic routing Using Ant Algorithm for Telecommunication Network*", International Conference on Communication technology Proceeding, Vol.2, pp. 1607-1612, 2000.

[12] Sadehiyan, B., Mohajeri, J., "*Moamagar: A160-bit Block Cipher*", 6th annual CSI Computer Conference (CSICC'2001), University of Isfahan, Iran, 2001.

[۱۳] قائمی بافقی، عباس، صادقیان، بابک، "تحلیل تفاضلی الگوریتم رمز قطعه‌ای معماگر"، یازدهمین کنفرانس مهندسی برق ایران، صفحات ۷۱-۷۸، اردیبهشت ۱۳۸۲.

[۱۴] سپهی، رضا، سلماسی‌زاده، محمود، صادقیان، بابک، "تحلیل خطی الگوریتم رمز معماگر ۵ مرحله‌ای"، نهمین کنفرانس سالانه انجمن کامپیوتر ایران،دانشگاه صنعتی شریف، بهمن۱۳۸۲،صفحات۶۰۶-۶۱۷.

[15] Biham, E., "*On Matsui's Linear Cryptanalysis*", Advances in Cryptology, Proceedings of EUROCRYPT '94, LNCS 950, pp. 341-355, 1994.

زیرنویس‌ها

[1] Iterative linear characteristics
[2] Scalar Product
[3] Linear Approximations Table
[4] Pilling-Up
[5] Duplication
[6] Substitution and Permutation Networks