یک مدل بازنمایی عملکرد تفاضلی الگوریتم‌های رمز قطعه‌ای با ساختار جانشینی ـ جایگشتی

عباس قائمی بافقی
دانشجوی دکتری

بابک صادقیان
دانشیار

دانشکده مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر

چکیده

تحلیل تفاضلی روشی متداول برای ارزیابی الگوریتم‌های رمز قطعه‌ای است. در این مقاله یک مدل بازنمایی عملکرد تفاضلی الگوریتم‌های رمز قطعه‌ای با ساختار جانشینی ـ جایگشتی ارائه می‌نماییم، که توسط آن الگوریتم رمز مورد نظر به یک گراف جهت‌دار وزن دار تبدیل می‌شود و یافتن بهترین مشخصه تفاضلی معادل یافتن کوتاهترین مسیر بین دو گره مشخص در این گراف است. برای یافتن کوتاهترین مسیر در گراف حاصل شیوه بهینه‌سازی اجتماع مورچگان را بکار می‌بریم.

در این مقاله با بکارگیری مدل ارائه شده برای الگوریتم رمز سرپنت، مشخصه‌های تفاضلی برای ٤، ٥ و ٦ دور از آن را پیدا نموده و با نتایج منتشر شده از تحلیل تفاضلی آن در دیگر مقالات مقایسه نموده‌ایم. این مقایسه نشان می‌دهد در شش مورد نتایج این مقاله بهتر از مقالات دیگر است و در دو مورد احتمال مشخصه تفاضلی بدست آمده برابر احتمال مشخصه‌های نظیر در مقالات دیگر می‌باشد. این بررسی بیانگر کارایی این مدل در یافتن مشخصه تفاضلی با احتمال بالا است.

کلمات کلیدی

تحلیل تفاضلی، ساختار جانشینی ـ جایگشتی، الگوریتم رمز قطعه‌ای سرپنت، شیوه اجتماع مورچگان.

A Model for Representation of Differential Operation of SP-Structure Block Ciphers

A. Ghaemi Bafghi
PhD. Student

B. Sadeghiyan
Associate Professor

Computer Engineering Department,
Amirkabir University of Technology

Abstract

Differential cryptanalysis is a common method which can be applied for the evaluation of bolck ciphers security. In this paper, we introduce a model for representing a SP-Structure block cipher's mapping differential characteristics. This model represents the differential operation of the cipher algorithm through a weighted directed graph, while finding the best differential characteristics of the cipher will be equivalent to finding the shortest path between the source and destination nodes of that graph. We then employ ant colony technique to find the shortest path of the graph.

Through applying this method, we managed to find some differential chararcteristics of 4-round, 5-round and 6-round Serpent block cipher. These characteristics are compared with other published chararcteristics. We show that our characteristics give a better probability than those published in six cases, and have the same probability in two other cases. This comparison explains the efficacy of our method to finding differential characteristics with high probability.

Key words

Differential Cryptanalysis, Substitution-Permutation Structure, Serpent Block Cipher, Ant Colony Technique.

مقدمه

تحلیل تفاضلی در سال ۹۰ توسط بیهام و شامیر ابداع شد[8]. این روش تحلیل در دو مرحله انجام می‌شود که ما آنها را مرحله طراحی حمله و اجرای حمله می‌نامیم. در مرحله طراحی حمله، تحلیلگر با بکارگیری ویژگی‌ها و نقاط ضعف الگوریتم رمز بدنبال یافتن یک مشخصه تفاضلی با احتمال بالا است. در مرحله اجرای حمله، تحلیلگر بایستی به اندازه کافی زوج متن رمزشده با تفاضل بدست آمده در مرحله طراحی را جمع آوری کرده و توسط آنها کلیدهای موثر در مشخصه را با انجام یک شیوه شمارش بدست آورد. این دو مرحله را می‌توان بصورت زیر خلاصه کرد:

الف ـ مرحله طراحی حمله

۱ـ تولید جدول توزیع تفاضلات توابع جانشینی بکاررفته در الگوریتم رمز

۲ـ محاسبه احتمال مشخصه برای تمامی مشخصه‌های یک دوری مختلف

۳ـ بررسی ترکیبات مختلف مشخصه‌های یک دوری برای یافتن یک مشخصه مناسب برای تمام دورهای الگوریتم رمز

ب ـ مرحله اجرای حمله

۴ـ جمع آوری تعداد کافی زوج متن رمزشده با تفاضل بدست آمده در مرحله الف

۵ـ انجام طرح شمارش و شناسایی بیت‌های موثر از زیرکلید دور آخر در مشخصه بدست آمده در مرحله الف

در مقالات بسیار متعددی این روش برای تحلیل الگوریتم‌های رمز قطعه‌ای بکارگرفته شده است. از آن جمله می‌توان از [4]، [7]، [8]، [9]، [10]، [11]، [13]، [16]، [24]، [25]، [33]، [34] نام برد. اما در اغلب اینها تنها به ذکر اجرای حمله پرداخته شده و از روشهای طراحی حمله و بهبود آن هیچگونه صحبتی نشده است و یا بطور خیلی اجمالی از روشهای بسیار ابتدایی و اولیه ذکر شده است و طراحی حملات تنها براساس تجربیات شخص تحلیلگر و با صرف وقت و دقت زیاد انجام می‌شود.

با بررسی الگوریتم‌های رمز با ساختار جانشینی– جایگشتی ملاحظه می‌شود که پس از چند دور انتشار ورودی/خروجی کامل شده و تمامی بیتهای خروجی با احتمال ۱/۲ تغییر می‌کند. با درنظر گرفتن یک Sbox فعال در دور میانی، یک مشخصه از دور میانی تا دور انتهایی و یک مشخصه از دور میانی تا دور ابتدایی می‌توان بدست آورد، این دو مشخصه را بترتیب مشخصه پیشرو و پسرو می‌نامیم. از الحاق این دو مشخصه به یکدیگر یک مشخصه از دور ابتدایی تا دور انتهایی بدست خواهد آمد. این شیوه بدست آوردن مشخصه تفاضلی را شیوه پیشرو-پسرو نامیدیم، که خواننده علاقمند به توضیحات بیشتر را به مقاله [۳] ارجاع می‌دهیم.

در [۳] روشهای الگوریتمی مانند برنامه ریزی پویا و بازگشت به عقب برای دست یافتن به یک مشخصه مناسب برای طراحی حمله مبتنی بر تحلیل تفاضلی مورد بررسی قرار گرفت. اگر چه در [۳] نتایج مناسبی بدست آمده است، اما بعلت تعیین توابع محدود کننده جستجو توسط تحلیلگر، محدودیت‌هایی از جمله : حذف ناخواسته جواب‌های مطلوب، پیچیدگی محاسباتی بالا، وابستگی به شخص تحلیلگر وجود دارد. برای فائق آمدن به این محدودیت‌ها مدل بازنمایی الگوریتم‌های رمز قطعه‌ای ارائه می‌شود که توسط آن بتوان شیوه‌های بهینه‌سازی هوشمند را برای یافتن مشخصه تفاضلی با احتمال بالا بکارگرفت. البته باید توجه داشت که این شیوه‌ها تنها یک جواب مناسب بدست می‌دهند که لزوما بهترین جواب نخواهد بود، درعوض این شیوه‌ها نسبت به شیوه‌های الگوریتمی دارای پیچیدگی محاسباتی کمتری هستند.

ما این مدل را مدل بازنمایی عملکرد تفاضلی الگوریتم رمز قطعه‌ای می‌نامیم. در این مدل هریک از توابع جانشینی و جایگشتی توسط یک گراف جهت دار وزن دار نشان داده می‌شود. از ترکیب گرافهای متناظر با توابع جانشینی و جایگشتی در الگوریتم رمز قطعه‌ای مورد نظر، یک گراف جهت دار وزن دار بدست می‌آید، بطوریکه جهت یافتن یک مشخصه تفاضلی k دوری، یک گراف $2k$ سطحی خواهیم داشت. مساله یافتن بهترین مشخصه برای یک الگوریتم رمز معادل یافتن مسیری از سطح اول به سطح انتهایی گراف حاصل از بازنمایی است بطوریکه جمع وزن یال‌های آن کمترین مقدار ممکن باشد. برای یافتن مسیر مناسب در گراف حاصل از بازنمایی می‌توان یکی از شیوه‌های هوشمند مانند الگوریتم ژنتیک، شبکه‌های عصبی، اجتماع مورچگان و ... را بکارگرفت. در این مقاله، ما نحوه بکارگیری اجتماع مورچگان را بعنوان نمونه تشریح می‌نماییم. بیان کلی این مدل برای الگوریتم رمز قطعه‌ای جانشینی ـ جایگشتی ارائه می‌گردد و بطور نمونه بر روی الگوریتم رمز قطعه‌ای

سـرپنت [5] بطـور کامل اعمال و پیاده‌سازی شده است. با کمی تغییر می‌توان این مدل را برای الگوریتم‌های رمز با ساختارهای دیگـر ازجملـه فیسـتل، کلوس و ترکیبی نیز بکارگرفت. چگونگی بکارگیری شیوه‌های بهینه‌سازی الگوریتم ژنتیک و شبکه‌های عصبی و نتایج حاصل از این دو شیوه برای الگوریتم رمز سرپنت را نیز در [۱] و [۲] ارائه نمودیم.

در ادامـه ایـن مقاله ابتدا نحوه بازنمایی توابع جانشینی و جایگشتی در قالب یک گراف جهت‌دار وزن‌دار ارائه و براساس آنها مـدل بازنمایـی الگوریـتم رمـز قطعـه‌ای ارائـه می‌گردد. در ادامه این مدل را برای رمز سرپنت اعمال کرده و با بکارگیری شیوه اجـتماع مورچگان مشخصه‌های ۴، ۵ و ۶ دوری را برای آن بدست می‌آوریم. سپس نتایج بدست آمده را با نتایج منتشر شده در دیگر مقالات [6]، [23] و [34] مقایسه می‌نماییم. نتایج بدست آمده بیانگر کارایی این مدل در یافتن مشخصه مناسب است. در انـتها مـدل را توسـعه مـی‌دهیم بطوریکه بهترین مقدار تفاضل برای دور میانی نیز توسط مدل تعیین گردد و نیازی به مشخص کردن آن توسط تحلیلگر نباشد.

۱ـ اندازه فضای مورد بررسی

بادقـت در مـراحل طراحـی حملـه مبتنـی بر تحلیل تفاضلی می‌توان گفت گلوگاه اصلی در طراحی حمله، بررسی ترکیبات مخـتلف مشخصـه‌های یک دوری جهت حصول بهترین مشخصه کل آلگوریتم است، زیرا این بررسی به معنی جستجوی فضای فـوق العـاده بزرگـی مـی‌باشـد. بـرای نشـان دادن بزرگـی اندازه فضای مورد بررسی، فضای مشخصه‌های تفاضلی سه دوری در الگوریـتم رمـز سرپنت از دور سوم تا پنجم را مرور می‌نماییم. این فضا یک درخت انتخاب چهار سطحی بصورت شکل(۱) است که هر گره و وزن یال متصل به آن بیان کننده یک مشخصه و احتمال وقوع آن است.

در اولیـن گـام بردار ۳۲ تایی از مولفه‌های ۴ بیتی را بعنوان بردار تفاضل ورودی مشخصه انتخاب کردیم که تنها شامل یک مولفـه غیرصـفر بـوده و بقـیه مولفـه‌های آن صفرمی باشد. لذا در سطح اول درخت جستجو(۱-$۲^۴$)×۳۲ گره خواهیم داشت. با توجـه به جدول توزیع تفاضلات سرپنت هر تفاضل غیر صفر در ورودی Sboxها می‌تواند به ۴ الی ۸ تفاضل غیرصفر در خروجی آن نگاشـت شـود، بـنابر ایـن در هر یک از مراحل دوم به بعد اگر تعداد Sboxهای فعال k باشد در سطح متناظر آن در درخت جسـتجو ۴^k الـی ۸^k ($۲^{۲k}$ الی $۲^{۳k}$) گره خواهیم داشت. در این مثال تعداد گره‌های سطح دوم تا چهارم بترتیب $۲^۲$ الی $۲^۳$، $۲^{۱۰}$ الی $۲^{۱۵}$،$۲^{۳۴}$ الی $۲^{۵۱}$ می‌باشد. بنابراین فضای جستجو برای یافتن یک مشخصه ۳ دوری $۲^{۴۶}$ الی $۲^{۶۹}$ است. با فعال شدن تمامی Sboxها پس از دور سوم به ازای افزایش هر دور دیگر فضای جستجو $۲^{۶۴}$ الی $۲^{۹۶}$ برابر می‌شود، یعنی اندازه فضای مورد بررسی با افزایش تعداد دور الگوریتم رمز بطور نمایی افزایش می‌یابد.

۲ـ نحوه بازنمایی توابع جانشینی و جایگشتی در مدل بازنمایی عملکرد تفاضلی

هـر الگوریتم رمز قطعه‌ای از اجزایی تشکیل می‌گردد که اندازه ورودی/خروجی آنها معمولا کوچکتر از اندازه قطعه الگوریتم رمـز می‌باشد. در الگوریتم‌های رمز قطعه‌ای جانشینی ـ جایگشتی، این اجزاء به دو گره کلی توابع جانشینی و جایگشتی تقسیم می‌گردد. در این بخش نحوه بازنمایی هریک از این توابع تشریح می‌گردد.

۲ـ۱ـ توابع جانشینی

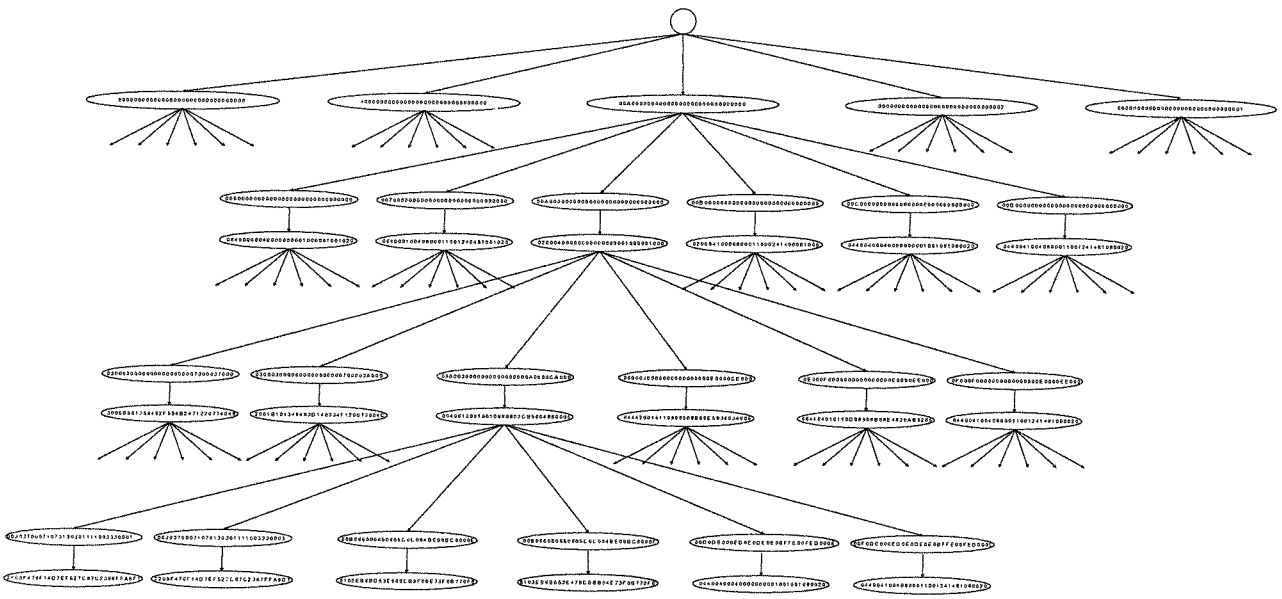
هـر تـابع جانشـینی m×n را می‌توان بصورت $S: \{0,1\}^m \rightarrow \{0,1\}^n$ نشان داد که یک دنباله m بیتی را با یک دنباله n بیتی مـی‌نگارد. لازم به توجه است که یک تابع جانشینی را می‌توان با ماتریس متناظر با آن نمایش داد. این ماتریس دارای ۲^m سطر و n سـتون بصـورت زیـر اسـت. سـتون iام در ایـن ماتـریس، شـامل ۲^m تـابع بولـی بصـورت $f_{i,j}: \{0,1\}^m \rightarrow \{0,1\}$ اسـت، که $0 \le i \le n-1$ و $0 \le j \le 2^m - 1$.

توزیـع تفاضلات ورودی/خروجی در یک تابع جانشینی را می‌توان توسط تابع $DD: \{0,1\}^m \times \{0,1\}^n \rightarrow R$ نشان داد، که هر زوج تفاضـل ورودی/خروجـی $(X,Y) \in \{0,1\}^m \times \{0,1\}^n$ را بـه احـتمال رخـداد تفاضـل خروجی Y تحت تابع جانشینی با فرض ورودی X می‌نگارد. معمولا این تابع را توسط جدول توزیع تفاضلات با ۲^m سطر و ۲^n ستون نشان می‌دهند، که مولفه سطر Xام سـتون Yام متـناظر DD(X,Y) است. در مدل بازنمایی عملکرد تفاضلی، توزیع تفاضلات ورودی/خروجی در یک تابع جانشینی

توسط یک گراف جهت‌دار دوبخشی $G(V,E,W)$ با 2^m+2^n گره بیان می‌شود. 2^m گره بعنوان گره‌های آغازی که با اندیس‌های دودویی ۰ تا 2^m-1 نامگذاری می‌شود و 2^n گره بعنوان گره‌های پایانی که با اندیس‌های دودویی ۰ تا 2^n-1 نامگذاری می‌شود. یالهای این گراف بر اساس جدول توزیع تفاضلات تعیین می‌گردد و وزن هر یال برابر قرینه لگاریتم (در مبنای ۲) مقدار متناظر با آن در جدول توزیع تفاضلات است. بعبارت دیگر برای هر زوج تفاضل ورودی/خروجی $(X,Y)\in\{0,1\}^m\times\{0,1\}^n$، وزن یال متناظر با آن بصورت $W_{X,Y}=-\mathrm{Log}_2(DD(X,Y))$ خواهد بود.

بطور مثال توابع جانشینی بکارگرفته شده در الگوریتم رمز سرپنت توابع جانشینی ۴×۴ مطابق جدول(۱) است. Sbox3 را درنظر می‌گیریم، توزیع تفاضلات این تابع جانشینی مطابق جدول(۲) است.

$$M=\begin{bmatrix} f_{n-1,0} & f_{n-2,0} & \cdots & f_{1,0} & f_{0,0} \\ f_{n-1,1} & f_{n-2,1} & \cdots & f_{1,1} & f_{0,1} \\ f_{n-1,2} & f_{n-2,2} & \cdots & f_{1,2} & f_{0,2} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ f_{n-1,2^m} & f_{n-2,2^m} & \cdots & f_{1,2^m} & f_{0,2^m} \end{bmatrix}$$



شکل(۱) درخت انواع مشخصه‌های سه دوری پیشرو در رمز سرپنت.

جدول(۱) توابع جانشینی در الگوریتم رمز سرپنت.

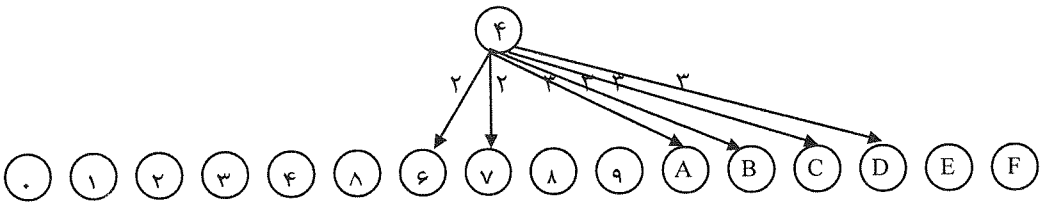
Sbox# \ Input	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	3	8	F	1	A	6	5	B	E	D	4	2	7	0	9	C
1	F	C	2	7	9	0	5	A	1	B	E	8	6	D	3	4
2	8	6	7	9	3	C	A	F	D	1	E	4	0	B	5	2
3	0	F	B	8	C	9	6	3	D	1	2	4	A	7	5	E
4	1	F	8	3	C	0	B	6	2	5	4	A	9	E	7	D
5	F	5	2	B	4	A	9	C	0	3	E	8	D	6	7	1
6	7	2	C	5	8	4	6	B	E	9	1	F	D	3	A	0
7	1	D	F	0	E	8	2	B	7	4	C	A	9	3	5	6

اگر مقدار ۴ را برای تفاضل ورودی این Sbox درنظر بگیریم با توجه به جدول توزیع تفاضلات Sbox3 مقادیر ۶، ۷، A، B، C و D را می‌توان بعنوان خروجی این Sbox درنظر گرفت. این مقادیر بترتیب با احتمال ۴/۱۶، ۴/۱۶، ۲/۱۶، ۲/۱۶، ۲/۱۶ و

۲/۱۶ در خروجی Sbox رخ می‌دهند. این انتخاب‌ها را می‌توان بصورت شکل(۲) بیان کرد. در این شکل گره سطر اول بیانگر مقدار ورودی Sbox و گره‌های سطر دوم تمامی مقادیر ممکن خروجی می‌باشد که هر گره ای که رخداد آن در خروجی Sbox بازای مقدار ورودی ۴ محتمل می‌باشد، توسط یک یال به گره ۴ متصل شده است.

جدول(۲) توزیع تفاضلات تابع جانشینی سوم در الگوریتم رمز سرپنت.

X \ Y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰
1	۰	۰	۰	۲/۱۶	۰	۴/۱۶	۲/۱۶	۰	۰	۰	۰	۲/۱۶	۲/۱۶	۲/۱۶	۰	۲/۱۶
2	۰	۰	۰	۰	۰	۲/۱۶	۰	۲/۱۶	۰	۲/۱۶	۴/۱۶	۲/۱۶	۰	۰	۰	۴/۱۶
3	۰	۰	۲/۱۶	۲/۱۶	۴/۱۶	۰	۰	۰	۲/۱۶	۲/۱۶	۰	۰	۰	۰	۰	۴/۱۶
4	۰	۰	۰	۰	۰	۰	۴/۱۶	۴/۱۶	۰	۰	۲/۱۶	۲/۱۶	۲/۱۶	۲/۱۶	۰	۰
5	۰	۲/۱۶	۰	۲/۱۶	۰	۰	۰	۰	۲/۱۶	۲/۱۶	۲/۱۶	۲/۱۶	۲/۱۶	۰	۲/۱۶	۰
6	۰	۲/۱۶	۰	۲/۱۶	۰	۰	۲/۱۶	۲/۱۶	۴/۱۶	۰	۰	۰	۲/۱۶	۰	۰	۲/۱۶
7	۰	۰	۲/۱۶	۴/۱۶	۴/۱۶	۲/۱۶	۰	۰	۰	۲/۱۶	۰	۰	۰	۰	۲/۱۶	۰
8	۰	۰	۰	۲/۱۶	۰	۰	۲/۱۶	۰	۰	۲/۱۶	۰	۰	۲/۱۶	۴/۱۶	۴/۱۶	۰
9	۰	۲/۱۶	۲/۱۶	۲/۱۶	۰	۰	۲/۱۶	۰	۲/۱۶	۰	۲/۱۶	۲/۱۶	۰	۰	۰	۲/۱۶
A	۰	۰	۲/۱۶	۰	۲/۱۶	۰	۲/۱۶	۲/۱۶	۰	۴/۱۶	۰	۲/۱۶	۲/۱۶	۰	۰	۰
B	۰	۲/۱۶	۲/۱۶	۰	۲/۱۶	۲/۱۶	۰	۰	۰	۲/۱۶	۲/۱۶	۰	۲/۱۶	۲/۱۶	۰	۰
C	۰	۲/۱۶	۰	۰	۲/۱۶	۰	۲/۱۶	۲/۱۶	۴/۱۶	۰	۲/۱۶	۰	۰	۰	۲/۱۶	۰
D	۰	۲/۱۶	۲/۱۶	۰	۲/۱۶	۴/۱۶	۰	۲/۱۶	۰	۰	۰	۰	۰	۴/۱۶	۰	۰
E	۰	۴/۱۶	۲/۱۶	۰	۰	۲/۱۶	۰	۰	۰	۰	۰	۲/۱۶	۰	۲/۱۶	۲/۱۶	۲/۱۶
F	۰	۰	۲/۱۶	۰	۰	۰	۰	۲/۱۶	۲/۱۶	۰	۲/۱۶	۲/۱۶	۲/۱۶	۰	۴/۱۶	۰



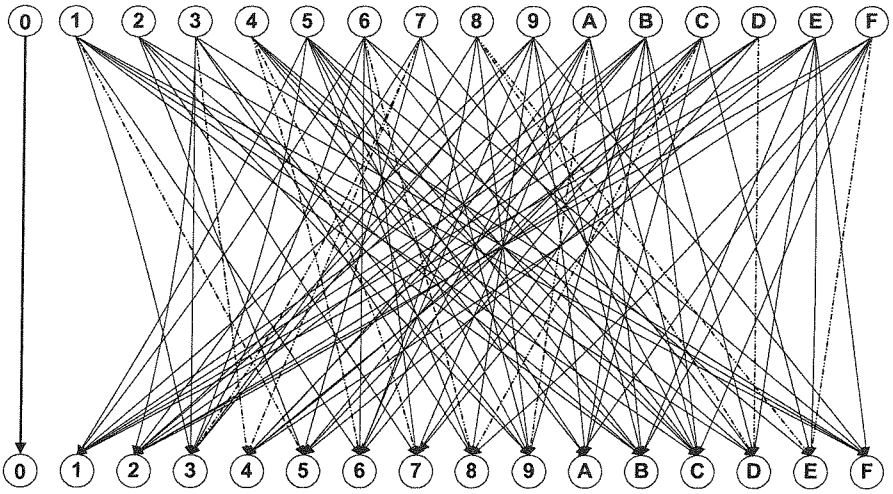
شکل(۲) تفاضلات ممکن خروجی Sbox3 در صورتیکه تفاضل ورودی آن ٤ باشد.

درصورتیکه در شکل(۲) علاوه بر مقدار ۴ برای تمامی مقادیر ممکن تفاضلات ورودی Sbox3 را رسم نماییم، شکل(۳) را خواهیم داشت. در واقع این شکل تمامی انتخاب‌های ممکن تفاضل خروجی Sbox3 به ازای هر یک از تفاضلات ۰ تا F در ورودی آن را بدست می‌دهد.

در گراف شکل(۳) هر گره از سطح اول به ۴ تا ۸ گره در سطح دوم متصل است. بعبارت دیگر با فرض یک مقدار دلخواه غیرصفر بعنوان تفاضل ورودی Sbox3 مقادیر ممکن در تفاضل خروجی آن ۴ تا ۸ مورد است. در این گراف مفاهیم تفاضل ورودی، تفاضل خروجی و منجر شدن و احتمال رخداد بصورت زیر تعریف می‌شود:

تفاضل ورودی/خروجی: برای یک تابع جانشینی m×n، اندیس هر گره آغازی بیانگر یک تفاضل ورودی است. ما مجموعه همه گره‌های آغازی را Vi می‌نامیم و داریم $\|Vi\| = 2^m$. اندیس هر گره پایانی بیانگر یک تفاضل خروجی است. ما مجموعه همه گره‌های پایانی را Vo می‌نامیم و داریم $\|Vo\| = 2^n$. بنابراین داریم: $Vi \cap Vo = \varnothing$ ، $Vi \cup Vo = V$.

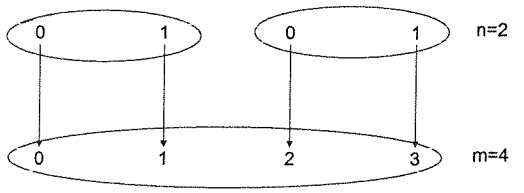
منجر شدن: اگر بین گره Vi_X و گره Vo_Y از گراف G یک یال وجود داشته باشد، می‌گوییم تفاضل خروجی Y از تفاضل ورودی X منجر می‌شود و بصورت $X \rightarrow Y$ نشان می‌دهیم. اگر وزن یال (Vi_X, Vo_Y) برابر $W_{X,Y}$ باشد به این معنی است که احتمال رخداد $X \rightarrow Y$ برابر $2^{-W_{X,Y}}$ می باشد.



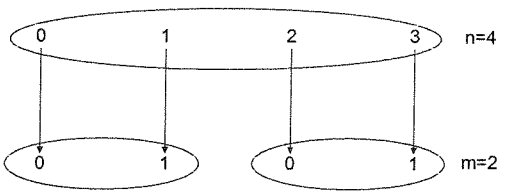
شکل(۳) تفاضلات ممکن خروجی Sbox3 به ازای هر یک از تفاضلات ورودی ۰ تا F در ورودی آن.
در این شکل وزن یال‌های پررنگ صفر و وزن یال‌های نقطه چین و خط ممتد بترتیب ۲ و ۳ است.

۲ـ۲ـ اتصال بین گرافهای دو تابع جانشینی

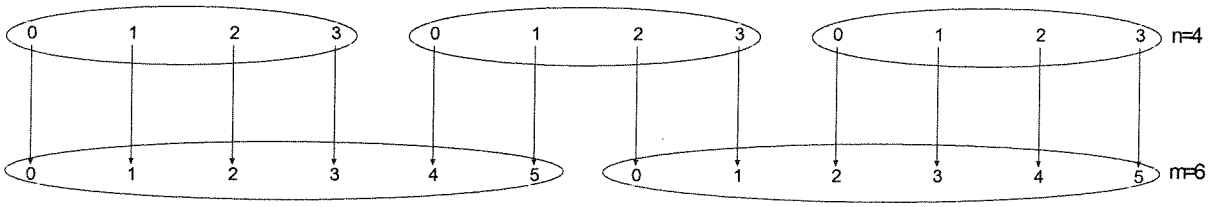
با توجه به اینکه در برخی از ساختارهای رمز مانند ساختار کلوس از توابع جانشینی با اندازه متفاوت استفاده می‌شود، در این بخش مدلی برای بیان ارتباط دو تابع جانشینی با اندازه دلخواه ارائه می‌نماییم. فرض نماییم در یک الگوریتم رمز توابع جانشینی با اندازه ورودی m بعد از توابع جانشینی با اندازه خروجی n قرار گرفته باشد. سه حالت مختلف برای m و n می‌توان درنظر گرفت. حالت اول اینکه n مضرب m باشد. حالت دوم اینکه m مضرب n باشد. حالت دیگر اینکه m و n هیچکدام مضرب دیگری نباشند. در شکل(۴) مثالی از این سه حالت آورده شده است. در شکل(۴ـالف) توابع جانشینی ۲بیتی بعد از توابع جانشینی ۴بیتی قرار گرفته‌اند. بنابراین خروجی هر تابع جانشینی ۴بیتی به دو بخش تقسیم شده و بعنوان ورودی دو تابع جانشینی ۲بیتی درنظرگرفته می‌شود. در شکل(۴ـ ب) توابع جانشینی ۴بیتی بعد از توابع جانشینی ۲بیتی قرار گرفته اند. بنابراین خروجی هر دو تابع جانشینی ۲بیتی مجموعا بعنوان ورودی یک تابع جانشینی ۴بیتی درنظرگرفته می‌شود. در شکل(۴ ـ ج) توابع جانشینی ۶بیتی بعد از توابع جانشینی ۴بیتی قرار گرفته اند. بنابراین خروجی هر سه تابع جانشینی ۴بیتی به دو بخش تقسیم شده و بعنوان ورودی دو تابع جانشینی ۶بیتی درنظرگرفته می‌شود. در ادامه نحوه بازنمایی هر یک از این حالات را تشریح می‌نماییم.



ب ـ اتصال یک تابع جانشینی ٤بیتی به دو تابع جانشینی ۲بیتی.



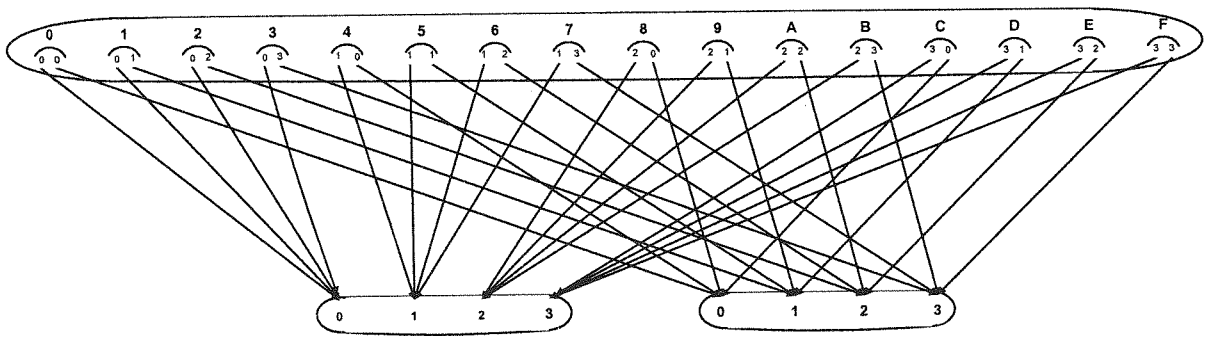
الف ـ اتصال دو تابع جانشینی ۲بیتی به یک تابع جانشینی ٤بیتی.



ج ـ اتصال دو تابع جانشینی ٦بیتی به سه تابع جانشینی ٤بیتی

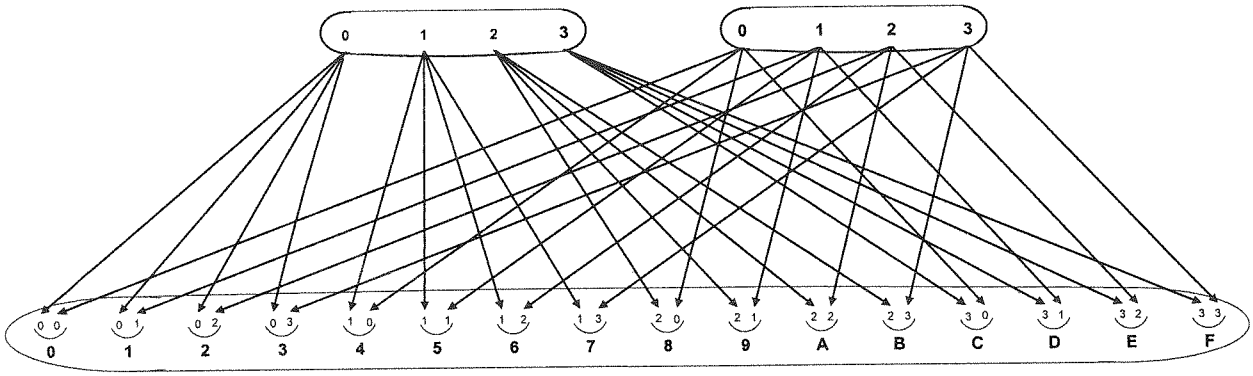
شکل(٤) حالات مختلف اتصال توابع جانشینی با اندازه‌های متفاوت.

الف ـ n مضرب m است: در ایـن حالت n بیت را می‌توان بصورت $\frac{n}{m}$ دسته m بیتی درنظر گرفت و لازم است ارتباط بین آنهـا معیـن گردد. برای این منظور هریک از 2^n حالت مختلف مربوط به n بیت را در مبنای ارقام m بیتی بیان می‌نماییم، یعنی یـک عـدد n بیتـی بصـورت یک عدد $\frac{n}{m}$ رقمی با ارقام m بیتی بیان می‌شود، که هر یک از ارقام متناظر با یک دسته m بیتی خواهـد بـود. در گراف مرتبط کننده هر گره از سطح اول به $\frac{n}{m}$ گره از سطح دوم متصل می‌شود که هر اتصال بر اساس یکی از ارقـام m بیتـی آن اسـت. ایـن گـراف یـک گـراف جهت‌دار دوبخشی G(V,E,W) با $2^m \times \frac{n}{m}$ گره متشکل از 2^n گره بعنوان گـره‌هـای آغازی و $2^m \times \frac{n}{m}$ گره بعنوان گره‌های پایانی است وزن تمامی یالها صفر است. بطور مثال در شکل(۵) گراف ارتباط ۴ بیت به ۲بیت نشان داده شده است.



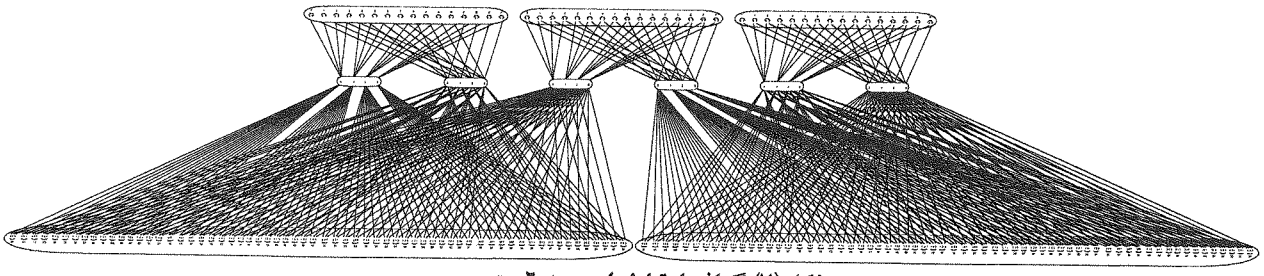
شکل(۵) گراف ارتباط ٤بیت به ۲بیت.

ب ـ m مضرب n است: در این حالت از ادغام $\frac{m}{n}$ دسته n بیتی یک دسته m بیتی بدست می‌آید و لازم است ارتباط بین آنهـا معیـن گـردد. بـرای این منظور هریک از 2^m حالت مختلف مربوط به m بیت را در پایه ارقام n بیتی بیان می‌نماییم، یعنی یـک عـدد m بیتـی بصـورت یـک عدد $\frac{m}{n}$ رقمی با ارقام n بیتی بیان می‌شود، که هر یک از ارقام متناظر با یک دسته n بیتی خواهـد بود. در گراف مرتبط کننده هر گره از سطح اول به 2^{m-n} گره از سطح دوم متصل می‌شود که این اتصالات بر اساس یکی از ارقام n بیتی آن است. این گراف یک گراف جهت‌دار دوبخشی G(V,E,W) با $2^n \times \frac{m}{n}+2^m$ گره متشکل از $2^n \times \frac{m}{n}$ گره بعنوان گره‌های آغازی و 2^m گره بعنوان گره‌های پایانی است وزن تمامی یالها صفر است. بطور مثال در شکل(۶) گراف ارتباط ۲بیت به ۴بیت نشان داده شده است.



شکل(٦) گراف ارتباط ۲بیت به ٤بیت.

ج ـ m و n هـیچکدام مضرب دیگری نیست: در این حالت فرض می‌کنیم k=gcd(m,n). ابتدا به شیوه (الف) یک گراف بـرای m و k و به شیوه (ب) یک گراف برای k و n بدست می‌آوریم. از ترکیب این دوگراف، گراف ارتباط بین حالات mبیتی و n بیتی بدست می‌آید. برای مثال در شکل(۷) نحوه ارتباط ۴بیت و ۶بیت نشان داده شده است.



شکل(۷) گراف ارتباط ٤بیت به ٦بیت.

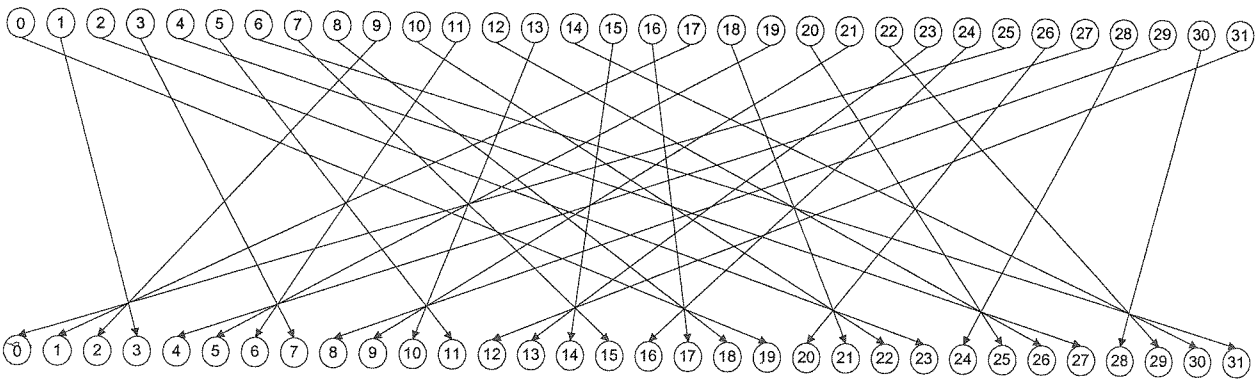
۲ـ۲ـ توابع جایگشت بیتی

هر تابع جایگشت بیتی بر روی دنباله‌های m بیتی را می‌توان بصورت یک تابع یک به یک و پوشا P: {0,1, ... m}→{0,1, ... m} نشان داد. این تابع نحوه نگاشت بیتهای ورودی به بیتهای خروجی را مشخص می‌کند، بطوریکه P(i)=j بیانگر آن است که بیت jام خروجی برابر بیت iام ورودی است. معمولا جایگشت بیتی با جدولی، که تناظر بین بیتهای ورودی و بیتهای خروجی را نشان می‌دهد، بیان می‌گردد. در مدل بازنمایی عملکرد تفاضلی، یک تابع جایگشت بیتی را توسط یک گراف جهت‌دار دوبخشی G(V,E,W) با ۲m گره بیان می‌کنیم. m گره بعنوان گره‌های آغازی و m گره بعنوان گره‌های پایانی که بترتیب متناظر بیتهای ورودی و خروجی بوده و هریک با اندیس‌های دودویی ۰ تا m-۱ نامگذاری می‌شود. یالهای این گراف بر اساس تابع P تعیین می‌گردد و وزن تمامی یالها صفر است. لازم بذکر است که در این گراف هر گره بیانگر یک مکان بیت در دنباله مورد نظر است، درحالیکه درگراف معادل توابع جانشینی هر گره بیانگر یک مقدار از دنباله بیتی می‌باشد.

بطور مثال جایگشت اولیه بکارگرفته شده در الگوریتم رمز معماگر[29] یک جایگشت ۳۲ بیتی مطابق جدول(۳) است. این جایگشت را بصورت شکل(۸) بیان می‌کنیم.

جدول(۳) جایگشت اولیه بکارگرفته شده در الگوریتم رمز معماگر.

Output#Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Input#Bit	25	17	9	1	27	19	11	3	29	21	13	5	31	23	15	7	24	16	8	0	26	18	10	2	28	20	12	4	30	22	14	6



شکل(۸) گراف معادل جایگشت اولیه بکارگرفته شده در الگوریتم رمز معماگر.

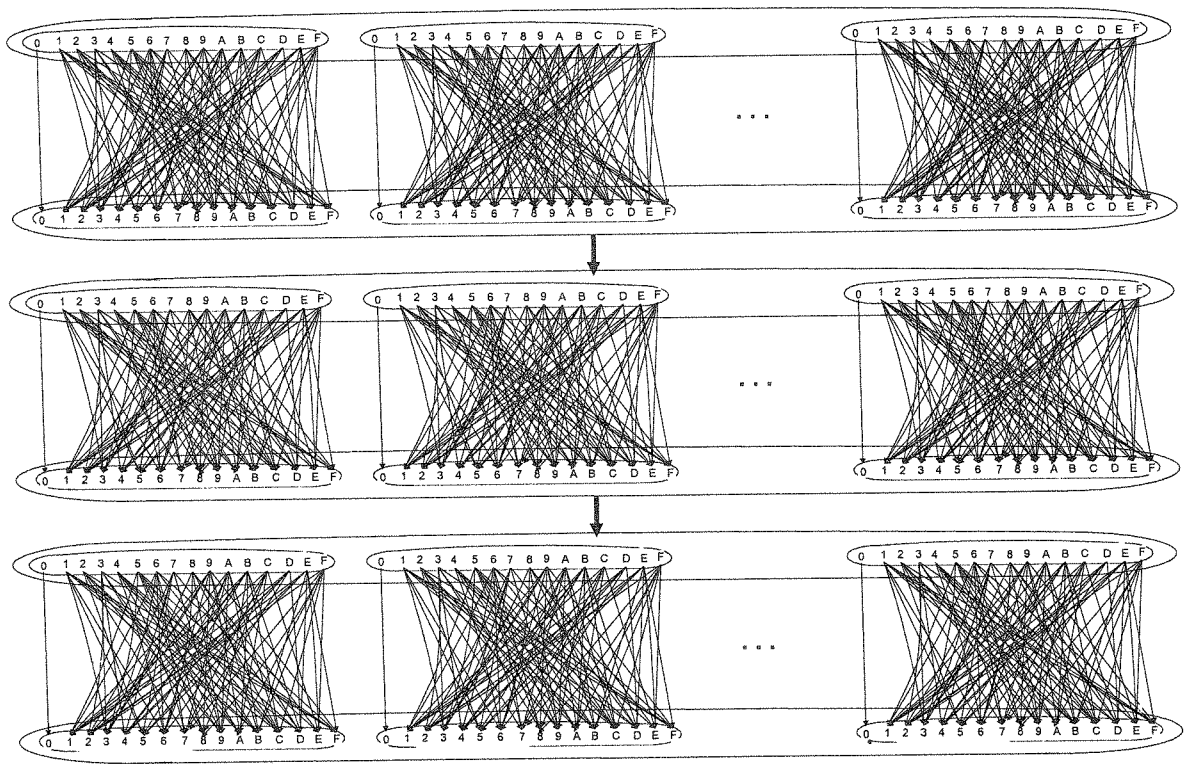
۳ـ مدل بازنمایی عملکرد تفاضلی الگوریتم رمز قطعه‌ای

برای بازنمایی یک الگوریتم رمز قطعه‌ای در این مدل کافی است به جای هر یک از اجزای الگوریتم رمز، گراف معادل آن را قرار دهیم. درنتیجه الگوریتم رمز به یک گراف جهت‌دار وزن‌دار چند سطحی تبدیل خواهد شد. در این بخش روند تبدیل درخت فضای ترکیبات ممکن مشخصه‌های سه دوری از الگوریتم رمز قطعه‌ای سرپنت به گراف حاصل از بازنمایی این الگوریتم رمز را نشان می‌دهیم.

اگر انتخاب‌های ممکن در یک سطح از درخت فضای ترکیبات ممکن مشخصه‌های سه دوری (شکل(۱)) را درنظر بگیریم، ملاحظه می‌شود که هر انتخاب از ترکیب ۳۲ انتخاب مجزا بدست می‌آید که هر یک تعیین کننده مقدار تفاضل خروجی برای

یـک Sbox مـی‌باشـد. البته توجه داریم درصورتیکه مقدار تفاضل ورودی برابر صفر باشد تنها مقدار ممکن در خروجی نیز صفر اسـت و اگـر مقـدار تفاضل ورودی غیرصفر باشد ۴ تا ۸ رخداد مختلف در تفاضل خروجی محتمل خواهد بود. از این‌رو می‌توان درخـت فضـای ترکیـبات ممکـن مشخصـه‌هـای سه دوری رمز سرپنت را توسط شکل(۹) نشان داد. در این شکل متناظر با هر Sbox یـک گـراف ۱ به k درنظر گرفته شده است که k تعداد انتخابهای ممکن تفاضل خروجی به ازای مقدار تفاضل ورودی در آن Sbox اسـت. در ایـن شـکل تعیین تفاضل خروجی هر دور براساس تفاضل ورودی آن از دو مرحله تشکیل می‌شود : مرحله اول تعییـن تفاضل خروجی هر یک از Sboxها بطور مجزا است، که براساس گراف مربوطه خواهد بود. مرحله دوم بدست آوردن ترکیـبات مخـتلف از انـتخابهای ممکن درSbox ها است، که اگر تعداد انتخابهای ممکن در $Sbox_i$ برابر k_i باشد، تعداد ترکیبات ممکن با توجه به استقلال Sboxها از یکدیگر و براساس اصل حاصلضرب برابر $\prod_{i=1}^{r} k_i$ خواهد بود.

مـی‌توان همه گره‌های هم‌سطح در درخت شکل(۹) را با هم ادغام کرده و مجموعا با یک گره نشان دهیم. دراین صورت هر یـک از مقادیـر ۰ تـا F مـی‌توانـد بعنوان تفاضل ورودی هر یک از ۳۲ تابع جانشینی درنظر گرفته شود و با توجه به توضیحات بخـش قبل، گراف تعیین کننده انتخابهای ممکن تفاضل خروجی در یک Sbox یک گراف ۱۶به ۱۶ مانند شکل(۳) می‌باشد. در ایـن صـورت شکل ساده شده درخت فضای ترکیبات ممکن مشخصه‌های توابع دور مطابق شکل(۱۰) خواهد بود، که آنرا گراف ترکیبات ممکن مشخصه‌های یک دوری می‌نامیم.



شکل(۱۰) ازنمایی عملکرد تفاضلی الگوریتم رمز قطعه‌ای سرپنت سه دوری(گراف ترکیبات ممکن مشخصه‌های یک دوری).

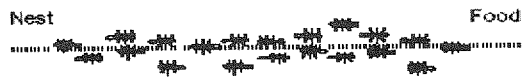
بطـور خلاصه می‌توان گفت در این مدل به جای هر یک از توابع جانشینی و جایگشتی در الگوریتم رمز، گراف معادل آن را قرار مـی‌دهـیم. درنتـیجه الگوریتم رمز به یک گراف جهت‌دار وزن‌دار چند سطحی تبدیل خواهد شد. ملاحظه می‌شود با بکارگیری ایـن مدل جهت یافتن یک مشخصه k دوری در هر الگوریتم رمز قطعه‌ای با ساختار جانشینی-جایگشتی، یک گراف ۲k سطحی خواهـیم داشـت. اگـر انـدازه ورودی/خروجـی در الگوریتم رمز مورد بررسی n و اندازه ورودی/خروجی توابع جانشینی بکار رفته درآن m باشـد تعـداد گـره گـراف حاصـل برابـر $2k\times\frac{n}{m}\times 2^m$ خواهد بود، یعنی اندازه گراف با افزایش تعداد دور بصورت خطی افزایش می‌یابد.

شکل(۹) درخت انواع مشخصه‌های پیشرو سه دوری در رمز سرپنت.

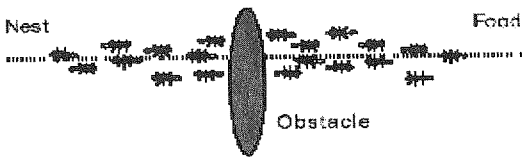
٤ـ یافتن بهترین مشخصه با استفاده از مدل بازنمایی عملکرد تفاضلی

یافتن بهترین مشخصه پیشرو برای یک الگوریتم رمز معادل یافتن مسیری از سطح اول به سطح انتهایی از گراف ترکیبات ممکن مشخصه‌های یک دوری آن است بطوریکه جمع مسیرهای آن کمترین مقدار ممکن باشد. یافتن بهترین مشخصه پسرو به معنی یافتن مسیری از سطح آخر به سطح ابتدایی این گراف است بطوریکه جمع مسیرهای آن کمترین مقدار ممکن باشد.

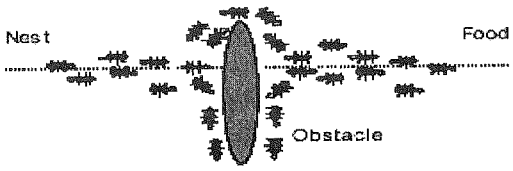
در این مقاله برای یافتن مسیر مناسب در گراف حاصل از بازنمایی الگوریتم رمز قطعه‌ای از شیوه بهینه‌سازی اجتماع مورچگان استفاده نموده ایم. این شیوه با الهام از مسیریابی مورچه‌ها در یافتن مسیر بین لانه تا محل آذوقه ابداع شده است. مورچه‌ها در هنگام پیمایش مسیر، اثری از اسید فورمیک به جای می‌گذارند که به تصمیم گیری مورچه‌های بعدی کمک می‌نماید. هر مورچه در انتخاب مسیر ابتدا بطور دلخواه و بیقاعده تصمیم می‌گیرد و پس از مدتی بطور احتمالی و براساس میزان غلظت اسید هر یک از مسیرهای موجود یکی از آنها را انتخاب می‌کند. بدین صورت پس از گذشت مدتی از شروع کار مورچه‌ها در جمع آوری آذوقه همگی از کوتاهترین مسیر فاصله بین لانه تا آذوقه را خواهند پیمود. نکته قابل توجه دراین شیوه آن است که مورچه‌ها بدون داشتن اطلاعات کامل از کل مسیرها و تنها براساس اطلاعات محلی (اسیدهای به جا مانده از مورچه‌های قبلی در هر مسیر) کوتاهترین مسیر را پیدا می‌نمایند. شکل(۱۱) نحوه انتخاب مسیر جدید توسط مورچه‌ها هنگام برخورد به یک مانع را بیان می‌کند. این شیوه بهینه‌سازی بصورت تصادفی عمل می‌کند، لذا در مسائلی که الگوریتم‌های کلاسیک مانند برنامه‌ریزی پویا کارایی لازم را ندارد به خوبی کار می‌کند. خواننده علاقمند به جزئیات این شیوه را به مقاله [20] ارجاع می‌دهیم. مسائل مختلفی که دارای فضای جستجوی بزرگی هستند با استفاده از این شیوه بهینه‌سازی حل شده است [12]، [14]، [15]، [17]، [18]، [19]، [21]،[22]، [26]،[27]، [28]، [30]، [31]، [32].



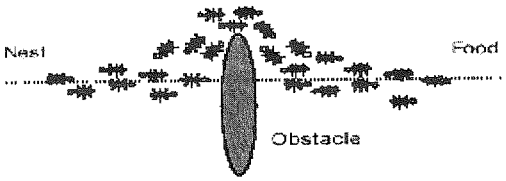
الف ـ مورچه‌ها مسیر بین لانه تا آذوقه را می‌پیمایند.



ب ـ اگر مانعی درمسیر مورچه‌ها پدید آید، بطور تصادفی یکی از دو مسیر را انتخاب می‌نماید.



ج ـ پس از مدتی مسیر کوتاهتر غلظت اسید بیشتری خواهد داشت



د ـ همه مورچه‌ها بر روی مسیر کوتاهتر راه را ادامه می‌دهند.

شکل(۱۱) نحوه انتخاب مسیر توسط مورچه‌ها.

برای مثال مدل بازنمایی عملکرد تفاضلی را برای رمز قطعه‌ای سرپنت پیاده‌سازی کرده‌ایم. گراف حاصل از بکارگیری این مدل برای رمز قطعه‌ای سرپنت مطابق شکل(۱۰) است، بطوریکه برای یافتن یک مشخصه پیشرو از دور i‌ام تا دور j‌ام بایستی وزن یالهای گراف بترتیب با توجه به Sboxهای دور i‌ام تا j‌ام تعیین شود. مورچه‌ها با حالت پیشرو از گره سطح اول شروع کرده و بسوی سطح انتهایی پیش می‌روند. هر مورچه با رسیدن به یک گره، بطور احتمالی و با توجه به وزن یال‌های خروجی یکی از یال‌ها را برای ادامه راه انتخاب می‌نمایند. همزمان با عبور از راه انتخاب شده میزان اسید یال انتخاب شده افزایش می‌یابد. پس از رسیدن همه مورچه‌ها به سطح آخر، مسیرهای پیموده شده توسط هریک ارزیابی شده و میزان اسید یال‌های بهترین مسیر مجددا افزایش می‌یابد. همین روند تا همگرا شدن مورچه‌ها بر روی یک مسیر ادامه می‌یابد. مسیریابی مورچه‌ها در دو جهت پیشرو و پسرو می‌باشد و عملکرد آنها در این دو جهت مشابه بوده و تنها جهت حرکت متفاوت می‌باشد. روند بهینه‌سازی به

شیوه اجتماع مورچگان بطور اجمالی در شبه کد زیر نشان داده شده است. روال ACO-meta-heuristic() روند کلی بهینه‌سازی را نشـان مـی‌دهـد و نحـوه عملکـرد هـر مورچه برای یافتن یک مشخصه در جهت پیشرو از دور آغاز StartRound تا دور پایان EndRound مطابق با روال Ant-activity () می‌باشد.

```
procedure ACO-meta-heuristic()
  while (termination-criterion-not-satisfied)
    for a from 1 to NumberOfAnts do
      Ants-activity()
    end for
    Pheromone-evaporation(Beta)
    Daemon-actions(Alfa)
  end while
end procedure

procedure Ant-activity () {Forward}
  {initialize ant}
  Direction=Forward
  InputChar[StartRound]= InitChar
  RoundNumber=StartRound
  while(RoundNumber<>EndRound)
    {read local ant routhing table}
    A= RoutingTables[RoundNumber]
  {Compute transition probability and Apply ant decision}
  for index from 1 to NumberOfSbox do
      CurrentInputChar=InputChar[RoundNumber][index]
      {Compute transition probability}
      TotalPhrmn=0
      for i from 1 to 2^OutputLenOfSbox do
        TotalPhrmn += A[index][CurrentInputChar][i]
      End for
      rnd=random(TotalPhrmn)
      {Apply ant decision polic}
      for CurrentOutputChar from 1 to 2^OutputLenOfSbox do
        if (rnd <=A[index][CurrentInputChar][CurrentOutputChar]
            And A[index][CurrentInputChar][CurrentOutputChar] <> 0 )
          break
        else
          rnd -=A[index][CurrentInputChar][CurrentOutputChar]
      End for
      OutputChar[RoundNumber][index]=CurrentOutputChar
    End for
    {update internal state}
    InputChar[RoundNumber+1] = LinearTrans(OutputChar[RoundNumber])
    RoundNumber++
  End while
  {evaluate solution}
  for round from StartRound to EndRound;round do
    for index from 1 to NumberOfSbox do
      PathLength += Weight[round][InputChar[round][index]] [OutputChar[round][index]]
    End for
  End for
  {Deposit pheromon on all visited arcs}
  for round from StartRound to EndRound do
    for index from 1 to NumberOfSbox do
      RoutingTables[round][index][InputChar[round][index]][OutputChar[round][index]] += 1
    End for
  End for
  {Die}
End procedure
```

در ایـن بـرنامه، متـناظر بـا هـر گـره یـک جـدول مسیریابی داریم که بیانگر میزان اسید یال‌های خروجی از آن گره است. مجموعه تمامی جداول مسیریابی با ماتریس RoutingTables نشان داده می‌شود که یک ماتریس چهار بعدی بوده و اندازه ابعاد آن بترتیـب برابر تعداد دور مشخصه مورد نظر (NumberOfRound)، تعداد توابع جانشینی در ساختار رمز (NumberOfSbox)، انـدازه فضـای ورودی توابـع جانشـینی ($۲^{InputLenOfSbox}$) و انـدازه فضـای خروجی توابع جانشینی ($۲^{OutputLenOfSbox}$) است. مولفه RoutingTables[r][i][p] جـدول مسیریابی گره p از تابع جانشینی iام از دورrام می‌باشد. جهت برازش مسیر پیموده شده، وزن یـال‌هـا در ماتـریس Weight با همان ابعاد ماتریس RoutingTables نگهداری می‌شود که Weight[r][i][p][c] متناظر وزن یال (p,c) از گراف iام از دور rام است.

بـرای هـر مورچـه علاوه بر جداول مسیریابی و برازش مسیر، یک حالت داخلی نیز درنظر گرفته شده است که از سه متغیر RoundNumber، PathLength، Direction و دو ماتـــریس دو بعـــدی $InputChar_{NumberOfRound\times NumberOfSbox}$ و $OutputChar_{NumberOfRound\times NumberOfSbox}$ تشـکیل شده است و بترتیب بیانگر شماره دور مورد بررسی توسط آن مورچه در هـر لحظـه، وزن مسـیر پیموده شده، جهت حرکت، تفاضل ورودی و تفاضل خروجی می‌باشد. مولفه‌های InputChar[r][i] و OutputChar[r][i] مشخص کننده تفاضل ورودی و خروجی در Sbox iام در دور r ام است.

روال Pheromone-evaporation(Beta) پـس از هـربار پـیمایش از گـره آغـازی تـا گـره پایانـی توسط همه مورچه‌ها انجام مـی‌شـود. در ایـن روال تمامـی مسـیرها در ماتـریس RoutingTables بـه نسـبت ضـریب تبخـیر (Beta) کاهش می‌یابد. روال Daemon-actions(Alfa) نـیز پس از هربار پیمایش از گره آغازی تا گره پایانی توسط همه مورچه‌ها انجام می‌شود. در این روال مسـیرهای پـیموده شـده توسـط مورچـه‌ها مقایسه شده و کوتاهترین مسیر تعیین می‌شود. سپس یالهای متناظر با کوتاهترین مسیر در ماتریس RoutingTables به اندازه جایزه مورچه برنده (Alfa) مجددا اسیدپاشی می‌شود.

بـرای اجـرای این الگوریتم بایستی پارامترهای تعداد مورچه ها، مقدار اولیه وزنها، میزان جایزهٔ مورچه برنده و ضریب تبخیر اسـید بایسـتی تعییـن شود، که ما بترتیب برابر ۵۰۰۰، ۱، ۵۰۰ و ۰/۰۱ درنظرگرفتیم. همچنین در این الگوریتم مشخصه اولیه یعنـی تفاضـل دور میانی را نیز بایستی تحلیلگر تعیین نماید، که ما جهت امکان مقایسه نتایج بدست آمده با دیگر مقالات، آنرا براسـاس مشخصـه‌های منتشر شده در دیگر مقالات تعیین نمودیم. البته در مدل کامل‌تری که در بخش ۷ آورده ایم این مقدار می‌تواند درحین عملیات بهینه‌سازی توسط مورچه‌ها تعیین گردد.

۵ـ مشخصه‌های تفاضلی بدست آمده برای الگوریتم رمز سرپنت

بـا تنظـیم پارامـترهای الگوریـتم بهینه‌سازی تشریح شده در بخش قبل، مشخصه‌های ۴، ۵ و ۶ دوری را برای الگوریتم رمز سرپنت بدست آوردیم. مقدار تفاضل ورودی دور میانی را بر اساس آنچه در تحلیل‌های تفاضلی منتشر شده از این الگوریتم رمز در [۶]، [23]، و [34] آمده است، تعیین نمودیم.

سـه مشخصـه ۴ دوری در [۶]، [23] و [34] ارائـه شده است. مشخصه ارائه شده در [6] مربوط به دور اول تا چهارم با دور میانی سوم است که Sbox چهارم از دور میانی فعال بوده و مقدار ۴ برای آن درنظرگرفته شده است. احتمال این مشخصه $۲^{-۲۹}$ مـی‌باشد. مشخصه‌ای را که ما با بکارگیری مدل بازنمایی عملکرد تفاضلی الگوریتم رمز قطعه‌ای سرپنت بدست آورده ایم مطابق جـدول(۴-الف) می‌باشد که دارای احتمال $۲^{-۲۹}$ است. مشخصه ارائه شده در [23] مربوط به دور اول تا چهارم با دور میانی سوم اسـت کـه Sbox دوم از دور میانـی فعـال بـوده و مقدار ۴ برای آن درنظرگرفته شده است. احتمال این مشخصه $۲^{-۳۱}$ می‌باشد. مشخصـه‌ای را کـه مـا بدست آورده ایم مطابق جدول(۴-ب) می‌باشد که دارای احتمال $۲^{-۲۹}$ است. مشخصه ارائه شده در [34] مـربوط بـه دور ششـم تـا نهم با دور میانی هشتم است که Sbox ششم از دور میانی فعال بوده و مقدار ۴ برای آن درنظرگرفته شـده اسـت. احـتمال این مشخصه $۲^{-۳۴}$ می‌باشد. مشخصه ای را که ما بدست آورده‌ایم مطابق جدول(۴ - ج) می‌باشد که دارای احتمال $۲^{-۳۲}$ است.

جدول(٤) مشخصه‌های تفاضلی ٤-دوری بدست آمده از رمز سرپنت با بکارگیری مدل بازنمایی عملکرد تفاضلی در این مقاله.

الف

Round#	Input Difference of S-boxes	Output Difference of S-boxes	Probability
1	00D0000000000000C1003009000000000	0020000000000001a00e004000000000	2^{-11}
2	00000000000000000000000000400500	00000000000000000000000000a00400	2^{-5}
3	00004000000000000000000000000000	0000A000000000000000000000000000	2^{-3}
4	00020004000000000000000010000810	0006000B000000000000000070000C70	2^{-10}
		Total Probability	2^{-29}

ب

Round#	Input Difference of S-boxes	Output Difference of S-boxes	Probability
1	D0000000000000C100300900000000000	20000000000001a00e00400000000000	2^{-11}
2	00000000000000000000000040050000	00000000000000000000000a0040000	2^{-5}
3	00400000000000000000000000000000	00A0000000000000000000000000000	2^{-3}
4	02000400000000000000001000081000	06000300000000000000070000C7000	2^{-10}
		Total Probability	2^{-29}

ج

Round#	Input Difference of S-boxes	Output Difference of S-boxes	Probability
6	04003000000006006006004006000000	0a00200000000001001000a0040000000	2^{-12}
7	00000000000000000000000000001005	00000000000000000000000000a004	2^{-5}
8	00000040000000000000000000000000	000000A0000000000000000000000000	2^{-2}
9	10000200040000000000000000100008	A0000300060000000000000000A0000E	2^{-13}
		Total Probability	2^{-32}

چهار مشخصه ۵ دوری در [6]، [23] و [34] ارائه شده است. مشخصه ارائه شده در [6] و یک مشخصه در [34] مربوط به دور پنجم تا نهم با دور میانی هشتم است که Sbox ششم از دور میانی فعال بوده و مقدار ۴ برای آن درنظرگرفته شده است. احتمال این مشخصه در[6] و [34] بترتیب 2^{-60} و 2^{-61} می‌باشد. مشخصه ای را که ما بدست آورده‌ایم مطابق جدول(۵ ـ الف) می‌باشد که دارای احتمال 2^{-60} است. مشخصه ارائه شده در [23] و یک مشخصه در [34] مربوط به دور اول تا پنجم با دور میانی سوم است که Sbox دوم از دور میانی فعال بوده و مقدار ۴ برای آن درنظرگرفته شده است. احتمال این مشخصه در[23] و [34] بترتیب 2^{-80} و 2^{-67} می‌باشد. مشخصه‌ای را که ما بدست آورده ایم مطابق جدول(۵-ب) می‌باشد که دارای احتمال 2^{-65} است.

جدول(٥) مشخصه‌های تفاضلی ٥-دوری بدست آمده از رمز سرپنت با بکارگیری مدل بازنمایی عملکرد تفاضلی در این مقاله.

الف

Round#	Input Difference of S-boxes	Output Difference of S-boxes	Probability
5	00000C0B000000050800C30D001900B3	00000301000000020c00480200650018	2^{-25}
6	0400A000000000600C000100C0000000	0a00200000000001001000a0040000000	2^{-15}
7	00000000000000000000000000001005	00000000000000000000000000a004	2^{-5}
8	00000040000000000000000000000000	000000A0000000000000000000000000	2^{-2}
9	10000200040000000000000000100008	A0000D0006000000000000000030000E	2^{-13}
		Total Probability	2^{-60}

ب

Round#	Input Difference of S-boxes	Output Difference of S-boxes	Probability
1	D000000000000C100300900000000000	20000000000001a00e00400000000000	2^{-11}
2	00000000000000000000000040050000	00000000000000000000000a0040000	2^{-5}
3	00400000000000000000000000000000	00A0000000000000000000000000000	2^{-3}
4	02000400000000000000001000081000	03000300000000000000A0000CB000	2^{-13}
5	30402900008010bc0c03ca5004070005	0B0D50000C06014040841E00908000E	2^{-33}
		Total Probability	2^{-65}

مشخصه ۶ دوری ارائه شده در [34] مربوط به دور اول تا ششم با دور میانی چهارم است که Sbox پانزدهم از دور میانی

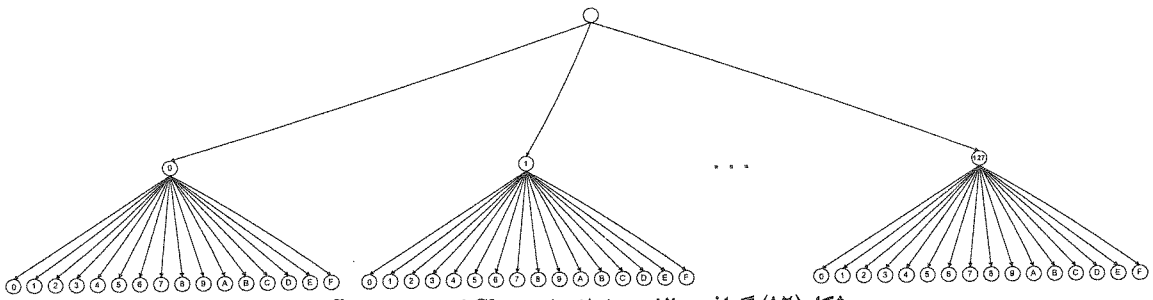
فعـال بـوده و مقـدار ۴ بـرای آن درنظرگرفـته شده است. احتمال این مشخصه 2^{-97} می‌باشد. مشخصه‌ای را که ما در این مقاله بدست آورده‌ایم مطابق جدول(۶) می‌باشد که دارای احتمال 2^{-94} است.

جدول(٦) مشخصه تفاضلی ٦-دوری بدست آمده از رمز سرپنت با بکارگیری مدل بازنمایی عملکرد تفاضلی دراین مقاله.

Round#	Input Difference of S-boxes	Output Difference of S-boxes	Probability
1	0C30090090DDD0900DE040000000000E	01e00400402220400280600000000008	2^{-24}
2	0400B000460A0005000000000000400A0	0a004000a20400080000000000a0040	2^{-21}
3	00000400A0000000000000000000000	00000a00400000000000000000000000	2^{-6}
4	00000000000000040000000000000000	00000000000000030000000000000000	2^{-2}
5	02000000010000200400000000001100	0A000000030000A00500000000006A00	2^{-17}
6	60070000200400000101008060052015	10020000700F00000E0E00B0100370E3	2^{-24}
		Total Probability	2^{-94}

۶ـ تکمیل مدل بازنمایی عملکرد تفاضلی

در ایـن بخـش مـدل ارائـه شـده را بـه گونه‌ای تکمیل می‌کنیم که بهترین مقدار تفاضل ورودی در دور میانی نیز در حین بهینـه‌سـازی توسـط مورچه‌ها تعیین شود. همانطور که گفته شد برای دستیابی به یک مشخصه بهینه تنها یک Sbox فعال در دور میانـی درنظر می‌گیریم، لذا لازم است اولا تعیین شود که کدام Sbox فعال باشد و ثانیا مقدار ورودی آن Sbox چه مقداری باشـد. برای این منظور یک گراف بصورت شکل(۱۲) درنظر می‌گیریم. گره‌های سطح اول هریک بیانگر یکی از Sboxها می‌باشد و گره‌های سطح دوم مقدار ورودی Sbox را مشخص خواهد کرد. وزن هر یک از یالهای این گراف صفر می‌باشد.



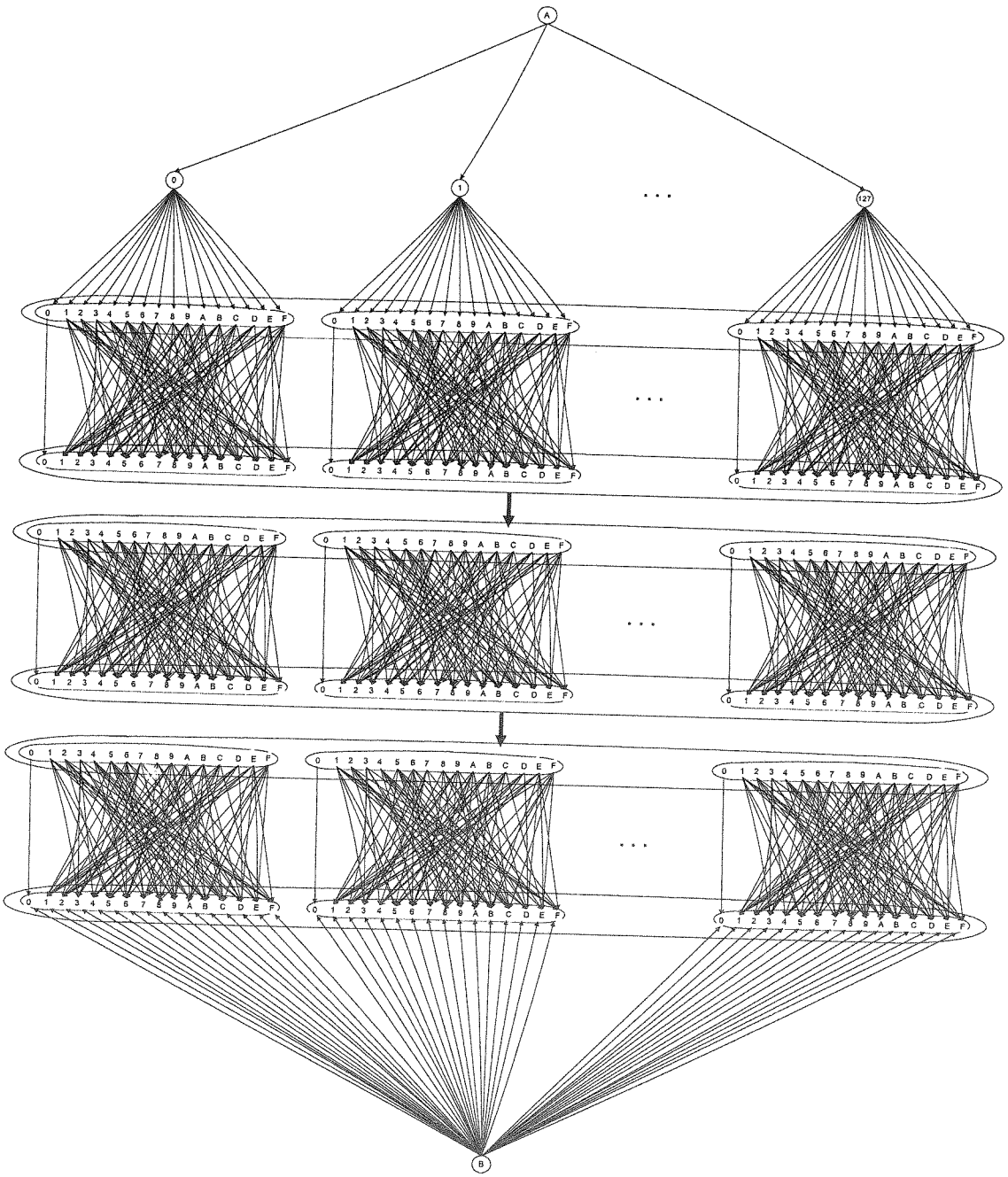
شکل(۱۲) گراف حالات مختلف از Sbox فعال و مقدار آن.

برای یافتن یک مشخصه پیشرو گراف حالات مختلف از Sbox فعال و مقدار آن را با گراف ترکیبات ممکن مشخصه‌های یک دوری ادغـام کـرده و یـک گـره مجـازی در انتهای آن می‌افزاییم که گره مجازی به تمامی گره‌های مربوط به مشخصه دور آخر متصـل بـوده و وزن هـر یـک از یـال‌هـای آن صـفر مـی‌باشـد. در نتیجه گراف حاصل برای یافتن یک مشخصه پیشرو بصورت شکل(۱۳) خواهد بود، که یافتن یک مشخصه پیشروی ۳ـ دوری معادل یافتن مسیری از گره A تا گره B است که مجموع وزن یال‌های آن کمترین مقدار ممکن باشد.

بـرای نمونـه یک مشخصه ۵ـ دوری (دور اول تا پنجم) از الگوریتم رمز سرپنت که با مدل بازنمایی عملکرد تفاضلی تکمیل شـده و بکارگـیری شـیوه بهیـنه‌سـازی اجتماع مورچگان بدست آمده است مطابق جدول(۷) می‌باشد. در این مشخصه سومین Sbox در دور میانی بعنوان Sbox فعال تعیین شده و مقدار آن ۴ تعیین شده است.

جدول(۷) مشخصه تفاضلی ۵ ـ دوری از رمز سرپنت بدست آمده با مدل بازنمایی عملکرد تفاضلی تکمیل شده.

Round#	Input Difference of S-boxes	Output Difference of S-boxes	Probability
1	0D000000000000C10030090000000000	020000000000001a00e0040000000000	2^{-11}
2	00000000000000000000000004005000	00000000000000000000000a004000	2^{-5}
3	00040000000000000000000000000000	000A0000000000000000000000000000	2^{-3}
4	00200040000000000000000100008100	00300030000000000000000A0000CB00	2^{-13}
5	530402900008010bc0c03ca500407000	E8090D50000C06014040841E00B08000	2^{-33}
		Total Probability	2^{-65}



شکل(۱۳) مدل تفاضلی از الگوریتم رمز سرپنت برای یافتن یک مشخصه پیشرو سه دوری.

۷ـ جمع بندی و کارهای آینده

در این مقاله مدلی برای بازنمایی الگوریتم رمز قطعه‌ای در قالب یک گراف جهت‌دار وزن‌دار ارائه گردید و بر اساس آن شیوه اجتماع مورچگان را برای یافتن بهترین مشخصه بکارگرفتیم. با بکارگیری این مدل جهت یافتن یک مشخصه k دوری در هر الگوریتم رمز قطعه‌ای با ساختار جانشینی-جایگشتی، یک گراف 2k سطحی خواهیم داشت و مساله یافتن بهترین مشخصه پیشرو (پسرو) برای این الگوریتم رمز معادل یافتن مسیری از سطح اول به سطح انتهایی (سطح انتهایی به سطح اول) این گراف است بطوریکه جمع وزن یال‌های آن کمترین مقدار ممکن باشد. در ادامه با بکارگیری این مدل برای الگوریتم رمز سرپنت و با استفاده از شیوه پیشرو- پسرو بکارگیری شیوه بهینه‌سازی اجتماع مورچگان چندین مشخصه را برای این الگوریتم رمز بدست آوردیم. در مدل اولیه که در بخش ۴ معرفی گردید، مقدار تفاضل دور میانی بصورت دستی و توسط تحلیلگر تعیین می‌گردد.

در بخش ۷ و افزودن گراف حالات مختلف Sbox فعال مدل ارائه شده را تکمیل نمودیم، به گونه‌ای که Sbox فعال در دور میانی و مقدار ورودی آن در حین بهینه‌سازی توسط مورچه‌ها تعیین می‌گردد.

در جدول(۸) نتایج حاصل از بکارگیری مدل بازنمایی عملکرد تفاضلی در این مقاله با مشخصه‌های منتشر شده از الگوریتم رمز سرپنت در مقالات دیگر مقایسه شده است. این مقایسه نشان می‌دهد در شش مورد نتایج حاصل از بکارگیری مدل بازنمایی عملکرد تفاضلی بهتر از نتایج منتشر شده در مقالات دیگر است و در دو مورد احتمال مشخصه تفاضلی بدست آمده برابر احتمال مشخصه‌های نظیر در مقالات دیگر می‌باشد. نتایج بدست آمده در این مقاله در مقایسه با مشخصه‌های منتشر شده در مقالات دیگر نشان دهنده کارایی مدل بازنمایی عملکرد تفاضلی در طراحی حمله مبتنی بر تحلیل تفاضلی است.

جدول(۸) مقایسه مشخصه‌های تفاضلی بدست آمده از الگوریتم رمز سرپنت در این مقاله و دیگر مقالات منتشر شده.

Number of Rounds	Starting Round #	Probability in other papers	Probability in This paper
4	1	2^{-31}[23]	2^{-29}
	6	2^{-34}[34]	2^{-32}
	1	2^{-29}[6]	2^{-29}
5	1	2^{-80}[23] 2^{-67}[34]	2^{-65}
	5	2^{-61}[34] 2^{-60}[6]	2^{-60}
6	1	2^{-97}[34]	2^{-94}

آزمایشهای مختلف انجام شده نشان می‌دهد که پیچیدگی اجرای روند بهینه‌سازی با افزایش تعداد دور الگوریتم رمز بطور خطی افزایش می‌یابد. تعداد تکرار روند بهینه‌سازی تا همگرایی مورچه‌ها برای حصول یک مشخصه ۴، ۵ و ۶ دوری بطور تقریبی ۳۰۰۰، ۴۰۰۰ و ۵۰۰۰ بار می‌باشد. البته این نتایج با توجه به مقادیر مذکور در بخش ۵ برای پارامتر این شیوه بهینه‌سازی است. با بررسی مقادیر مختلف برای این پارامترها و تعیین بهترین مقدار برای آنها می‌توان به کارایی بالاتری در روند بهینه‌سازی دست یافت.

شیوه مطرح شده در این مقاله برای یافتن مشخصه‌های تفاضلی می‌تواند از جنبه‌های مختلفی توسعه یابد، که می‌توان از سه جنبه زیر بعنوان نمونه‌هایی از این توسعه نام برد: اولا، مدل تفاضلی مطرح شده در شکل فعلی قابل بکارگیری جهت مدل کردن ساختارهای جانشینی ـ جایگشتی می‌باشد که با توسعه آن می‌توان آنرا برای ساختارهای دیگر مانند ساختارهای فیستل، کلوس و نیز الگوریتم‌های رمزی که از توابعی مانند جمع معمولی، ضرب در میدان‌های گالوا و ... استفاده کرده اند، بکارگرفت. ثانیا، معیار برازش یک مشخصه در این مقاله احتمال آن بوده است که می‌توان معیارهای دیگر مانند سیگنال به نویز، تعداد Sboxهای فعال، پیچیدگی محاسباتی حمله مبتنی بر مشخصه بدست آمده و ... را درنظر گرفت. ثالثا، می‌توان برای یافتن بهترین مسیر در گراف حاصل از بازنمایی بجای شیوه بهینه‌سازی اجتماع مورچگان، شیوه‌های بهینه‌سازی دیگر مانند الگوریتم ژنتیک، Simulated Annealing، شبکه‌های عصبی، برنامه‌ریزی تکاملی را بکار گرفت و کارایی آنها را با اعمال بر چندین الگوریتم رمز قطعه ای با یکدیگر مقایسه نمود.

مراجع

[۱] م.آبادی، ع.قائمی بافقی، ب.صادقیان و ت.اقلیدس، "یافتن مشخصه تفاضلی برای الگوریتم رمز سرپنت"، نهمین کنفرانس سالانه انجمن کامپیوتر ایران، ۱۳۸۲.

[۲] ع.قائمی بافقی، ب.صادقیان و ر.صفابخش، "یافتن مسیر مناسب در گراف حاصل از بازنمایی الگوریتم رمز قطعه ای با استفاده از شبکه عصبی هاپفیلد"، نهمین کنفرانس سالانه انجمن کامپیوتر ایران، ۱۳۸۲.

[۳] ع.قائمی بافقی، ب.صادقیان، "تحلیل تفاضلی سرپنت"، هفتمین کنفرانس سالانه انجمن کامپیوتر ایران، ۱۳۸۰.

[4] C.Adams,"On Immunity Against Biham and Shamir's "Differential Cryptanalysis"", Information Processing Letters. 41: 77-80,1992.

[5] R. Anderson, E. Biham, and L. Knudsen, "Serpent: A Proposal for the Advanced Encryption Standard", NIST Proposal, 1998.

[6] E.Biham, O.Dunkelman, and N.Keller, "The Rectangle Attack-Rectangeling the Serpent", Lecture Notes in Computer Science , 2001.

[7] E.Biham and A.Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", Advances in Cryptology-

CRYPTO '90, pp. 2-21, 1990
[8] E.Biham and A.Shamir, "Differential Cryptanalysis of Snefur, Khafre, REDOC-II, LOKI and Lucifer". Advances in Cryptology -- CRYPTO '91, pp.156-171, and Journal of Cryptology, Vol. 4, No. 1, pp. 3-72, 1991.
[9] E.Biham and A.Shamir, "Differential Cryptanalysis of the Full 16-Round DES ", Proceedings of Crypto'92, LNCS 740, pp.487-496, 1992.
[10] E.Biham, "On Matsui's Linear Cryptanalysis", Advances in Cryptology , Eurocrypto'94, 1994.
[11] E.Biham, A.Biryukov and A.Shamir, "Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials", Advances in Cryptology-Eurocrypto'99, pp 12-23, Also available at http://www.cs.technion.ac.il/biham/Reports/Skipjack/ , 1999.
[12] B.Bullnheimer, F.H.Richard and C.Straub, "A new Rank Based Version of the Ant system-A Computaional Study", Working Paper No1, April 1997.
[13] I.Ben-Aroya and E.Biham, "Differential Cryptanalysis of Lucifer", Proceedings of Crypto'93, LNCS 773, and Journal of Cryptology, Vol. 9, No. 1, pp. 21-34, 1996.
[14] A.Colorni, M.Dorigo and V.Maniezzo, "Distributed Optimization by Ant Colonies", Proceedings of ECAL9 -European Conference on Artificial Life, 134–142, 1991.
[15] A.Colorni, M.Dorigo, V.Maniezzo and M.Trubian, "Ant system for Job-Shop Scheduling", JORBEL-Belgian Journal of Operations Research, Statistics and Computer Science 34 (1), pp. 39-53, 1994.
[16] O.Dunkelman, "An Analysis of Serpent-p and Serpent-p-ns", Second AES Conference: http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm ,1998.
[17] M.Dorigo and L.M.Gambardella, "A Study of Some Properties of Ant-Q", Proceedings of PPSN IV–Fourth International Conference on Parallel Problem Solving From Nature,(Springer-Verlag, Berlin) pp. 656–665, 1996.
[18] M.Dorigo, V.Maniezzo and Colorni, A.: "Ant System: Optimization by a Colony of Cooperating Agents.", IEEE Transactions on Systems, Man, and Cybernetics ,26 (1),pp. 29-41, 1996.
[19] M.Dorigo and L.M.Gambardella "Ant Colonies for the Traveling Salesman Problem", Publication in BioSystems, 1997.
[20] M.Dorigo and G.Di Caro, "Ant Colony Optimization: A new Meta-Heuristic", IEEE Conference on Evolutionary Computation CEC99 , Vol. 2 ,1999.
[21] L.M.Gambardella and M.Dorigo, "Ant-Q: A Reinforcement Learning Approach to the Traveling Salesman Problem", Proceedings of ML-95, Twelfth Intern. Conf. on Machine Learning, pp.252–260, 1995.
[22] L.Guoying, Z.Subing, L.Zemin, "Distributed Dynamic Routing Using Ant Algorithm for Telecommunication Network", International Conference on Communication Technology Proceeding ,Vol.2 , pp. 1607-1612 , 2000.
[23] T.Kohono, J.Kelsey, and B.Schneier, "Preliminary Cryptanalysis of Reduced-Round Serpent", third AES Candidate Conference, 2000.
[24] L.R.Knudsen, "Truncated and Higher Order Differentials.", Fast Software Encryption-Second International Workshop, LNCS 1008, pp. 196-211, Springer Verlag, 1995.
[25] L.R.Knudsen and T.Berson," Truncated Differentials of SAFER.", Fast Software Encryption, Third International Workshop, LNCS 1039, pp. 15-26, 1995.
[26] V.Maniezzo, A.Colorni, "The Ant System Applied the Quadratic Assignment Problem", "IEEE Transacrion on Kniwledg and Data Enginerung , 11(5), 1999.
[27] Z.Subing, L.Zemin, "A QoS Routing Based on Ant Algorithm", Annual IEEE Conference on Local Computer Networks, PP 574-578,2000.
[28] L.Schoofs, B.Naudts, "Ant Colonies are Good at Solving Constraint Satisfaction Problem", IEEE Conference on Evolutionary Computation , Vol. 2, 2000.
[29] B.Sadeghiyan, J.Mohajery, "Moammagar : A 160-bit Block Cipher", 6th Annual CSI Computer Conference, 2001.
[30] L.Shenghong and L.Zemin ,"A general CAC Approach Using Ant Algorithm Training Based Neuarl Network ", International Joint conference on Neural Network , Vol.3, pp. 1885-1888,1999 .
[31] L.SeungGwan, J.TaeUng and C. TaeChong ,"An Effective dynamic Weighted Rule for Ant Colony System Optimization" , IEEE Congress on Evolutionary Computation , Vol. 2 ,2001.
[32] T.Stutzle and M.Dorigo, "ACO Algorithms for the Traveling Salesman Problem", To appear in Evolutionary Algorithms in Engineering and Computer Science, 1999.
[33] D.Wagner and U.C.Berkeley, "The Boomerang Attack", Fast Software Encryption, 6th International Workshop , 1999.
[34] X. Y. Wang, and et.al. "The Differential Cryptanalysis of an AES Finalist-Serpent", Technical Report TR-2000-04, 2000.