دوازدهمین کنفرانس بین‌المللی انجمن کامپیوتر ایران
دانشگاه شهید بهشتی، دانشکده مهندسی برق و کامپیوتر ،تهران، ایران، ۱ تا ۳ اسفند ۱۳۸۵

یافتن مشخصه خطی در الگوریتم های رمز قطعه ای جانشینی- جایگشتی با استفاده از شیوه بهینه سازی شبکه عصبی هاپفیلد

عباس قائمی بافقی*

چکیده

تحلیل خطی روشی متداول برای ارزیابی الگوریتم های رمز قطعه‌ای است. در این مقاله، شبکه عصبی هاپفیلد برای یافتن بهترین مشخصه خطی در الگوریتم رمز قطعه‌ای بکارگرفته شده است. برای نمونه، این روش برای یافتن مشخصه های خطی در الگوریتم رمز کهکشان بکارگرفته شده است. الگوریتم رمز کهکشان یک الگوریتم رمز قطعه‌ای با طول قطعه ورودی/خروجی و طول کلید ۲۵۶ بیت می باشد که از ۳۲ دور تکرار تبدیل جانشینی-جایگشتی بدست آمده است. تا اکنون هیچ حمله مبتنی بر تحلیل خطی برای این الگوریتم رمز ارائه نشده است. در این مقاله یک مشخصه خطی برای الگوریتم رمز کهکشان ۸، ۹ و ۱۰ دوری بترتیب با تمایل احتمال 2^{-78}، 2^{-114} و 2^{-146} بدست آمده است.

کلمات کلیدی

رمز قطعه‌ای، الگوریتم رمز کهکشان، تحلیل خطی، شبکه عصبی هاپفیلد.

Finding Linear Cryptanalysis Characteristic of SP Block Cipher Using Hopfield Neural Network

Abbas Ghaemi Bafghi

Abstract

Linear cryptanalysis is a usual method to evaluation of block ciphers. In this paper, Hopfield neural network is applied to find the best linear characteristic of block ciphers. This method is performed on Kahkeshan block cipher as a case study. Kahkeshan is a SP block cipher with 256 bits block/key size and 32 rounds SP transformation. Until now, no linear cryptanalysis is published for this cipher. In this paper, 8-round, 9-round and 10-round linear characteristic with the probability of 2^{-78}, 2^{-114} and 2^{-146} are obtained.

Keywords

Block cipher, Kahkeshan cipher algorithm, Linear cryptanalysis, Hopfield neural network.

* استادیار گروه کامپیوتر، دانشکده مهندسی، دانشگاه فردوسی مشهد، GhaemiB@um.ac.ir

۱- مقدمه

تحلیل خطی یک روش بررسی روابط موجود بین تقریب خطی متن واضح، متن رمزشده و زیرکلیدها است که اولین با توسط ماتسویی[۱۰] مطرح شد. برای سهولت بررسی تئوری زیر کلیدها را مستقل در نظر می‌گیریم. در صورتیکه بین زیر کلیدها وابستگی وجود داشته باشد انجام تحلیل آسان تر می‌شود، اما بررسی تئوری آن مشکل‌تر خواهد بود. مهمترین بخش تحلیل خطی بدست آوردن بهترین مشخصه می‌باشد که سعی می‌شود، با توجه به ویژگی های اجزای داخلی و ساختار الگوریتم رمز و با شناسایی و بکار گیری آسیب پذیریها و نقاط ضعف آن، بهترین مشخصه را برای الگوریتم رمز بدست آوریم.

در این مقاله، از ابزار فلق۲ [۶] برای یافتن مشخصه های خطی استفاده شده است. در این ابزار برای یافتن مشخصه خطی مناسب در الگوریتم رمز قطعه‌ای، بهینه‌سازی با شبکه عصبی هاپفیلد، Simulated Annealing و ماشین بولتزمن استفاده شده است. برای این منظور، شبکه عصبی معادل یک تابع جانشینی، که براساس آن شبکه عصبی معادل هر تعداد دور از الگوریتم رمز قابل بیان می‌باشد، تعریف شده و الگوریتم های آموزش شبکه عصبی حاصل جهت یافتن جواب بهینه برای تابع هزینه بیان می‌شود. دراین مقاله بخش شبکه عصبی هاپفیلد مورد توجه قرار می گیرد. لازم بذکر است با توجه به فضای بسیار بالای مشخصه‌های ممکن، بررسی کل فضا میسر نمی‌باشد و این مشخصه‌ها با بکارگیری شیوه‌های هوشمند بدست آمده است. لذا نمی‌توان ادعا کرد مشخصه‌هایی بهتر از آنچه در اینجا مطرح می‌شود وجود ندارد و ممکن است به شیوه‌ای دیگر و یا با صرف زمان بیشتر بتوان به مشخصه‌های بهتری دست یافت.

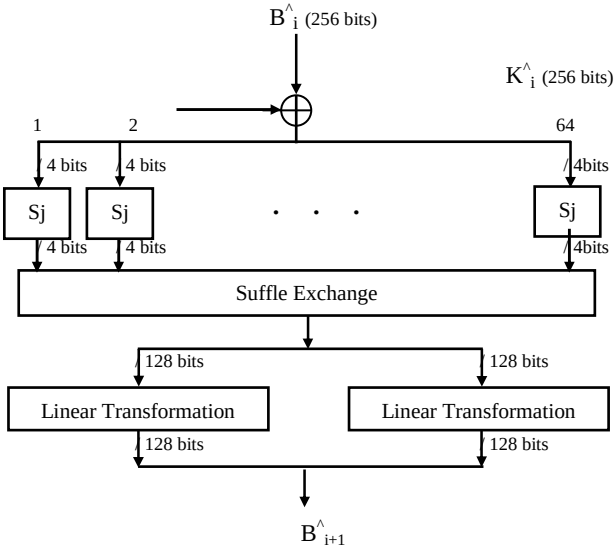
دراین مقاله ابتدا الگوریتم رمز کهکشان را معرفی کرده و سپس نحوه بکارگیری شبکه عصبی در یافتن مشخصه مناسب در الگوریتم رمز تشریح می شود. در انتها مشخصه های خطی بدست آمده برای الگوریتم رمز کهکشان بیان می‌گردد.

۲- معرفی رمز قطعه ای کهکشان

این الگوریتم یکی از چهار الگوریتم رمز شرکت کننده در مسابقه "بررسی الگوریتم‌های رمز قطعه‌ای" می‌باشد[۱]، که با اقتباس از الگوریتم رمز سرپنت [۷] و توسعه آن طراحی شده است. در این الگوریتم از همان S-Boxهای سرپنت استفاده شده و تبدیلات اولیه و انتهایی با توجه به طول ورودی/خروجی ۲۵۶ طراحی شده است. برای بکارگیری تبدیل خطی سرپنت با ورودی ۱۲۸ بیتی در رمز کهکشان با ورودی ۲۵۶ بیتی از یک تبدیل جابجایی ضربدری استفاده کرده‌ایم.

در این الگوریتم از هشت S-Box با ورودی و خروجی ۴ بیت که با $S_0 , \ldots , S_7$ مشخص می‌شوند، استفاده شده است ، بطوریکه در تابع دور iام (شکل۱)، $i \in \{0, \ldots , 31\}$، فقط از تکرار یک S-Box مشخص ($S_j , j \in \{0, \ldots , 7\}$) استفاده می‌شود که شماره آن(j) طبق رابطه مقابل مشخص می شود :

در دور i ام، $i \in \{0, \ldots , 31\}$ ، دو ورودی ۲۵۶ بیتی $B^{\wedge}_i$ و $K^{\wedge}_i$ با هم Xor شده و به ۶۴ عدد S-Box مشابه و مشخص اعمال می‌شوند. آنگاه بردار میانی ابتدا تحت تبدیل جابجایی ضربدری و سپس توسط تبدیل خطی تغییر یافته و $B^{\wedge}_1$ را تولید می‌کند.



شکل (۱): توابع دور ($Ri , 0 \le i \le 30$) در رمز کهکشان

تابع دور مرحله آخر (R_{31}) اندکی با بقیه تفاوت دارد، بطوریکه پس از اعمال توابع جانشینی S_7 روی $B^{\wedge}_{31} \oplus K^{\wedge}_{31}$، بجای اعمال تبدیل جابجایی ضربدری و تبدیل خطی، بردار میانی حاصل با $K^{\wedge}_{32}$ بیت به بیت Xor شده و $B^{\wedge}_{32}$ تولید می‌شود. پس از اعمال نگاشت FP بر روی $B^{\wedge}_{32}$، متن رمز C بدست می‌آید.

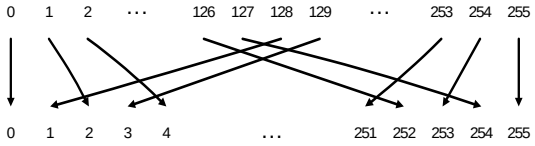
در تبدیل خطی ورودی ۱۲۸ بیتی بصورت ۴ کلمه ۳۲ بیتی X_0، X_1، X_2، و X_3 درنظرگرفته شده و بصورت زیر با هم ترکیب می‌شوند:

$X_0 = X_0 <<< 13$
$X_2 = X_2 <<< 3$
$X_1 = X_0 \oplus X_1 \oplus X_2$
$X_3 = X_3 \oplus X_2 \oplus (X_0 <<< 3)$
$X_1 = X_1 <<< 1$
$X_3 = X_3 <<< 7$
$X_0 = X_0 \oplus X_1 \oplus X_3$
$X_2 = X_2 \oplus X_3 \oplus (X_1 <<< 7)$
$X_0 = X_0 <<< 5$
$X_2 = X_2 <<< 22$

که X<<<k بیانگر دوران X به اندازه k بیت به چپ و X<<k بیانگر انتقال X به اندازه k بیت به چپ و X⊕Y بیانگر Xor بیت به بیت X و Y است.

تبدیل جابجایی ضربدری مطابق شکل(۲) یک جایگشت منظم روی بیتهای ورودی اعمال کرده و خروجی را بدست می دهد. بطوریکه بیت اول و آخر(۲۲۵ام) را ثابت نگه داشته و در بقیه بیت‌ها، بیت i ام ورودی را به بیت 2i ام (در پیمانه ۲۵۵) خروجی می‌نگارد.توابع

جانشینی بکارگرفته شده در الگوریتم رمز کهکشان در جدول(۱) آمده است.



شکل(۲): تبدیل جابجایی ضربدری

جدول (۱): توابع جانشینی در الگوریتم رمز کهکشان

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

۳- یافتن مشخصه خطی با استفاده از شبکه عصبی

دراین بخش شبکه عصبی معادل یک تابع جانشینی، که براساس آن شبکه عصبی معادل هر تعداد دور از الگوریتم رمز قابل بیان می‌باشد، تعریف می شود. در این شبکه عصبی تمایل احتمال تقریب خطی در الگوریتم رمز قطعه‌ای، توسط تابع هزینه مشخص می‌شود. بنابراین جهت یافتن مشخصه خطی مناسب لازم است تابع هزینه در شبکه عصبی حداقل گردد. در ادامه این بخش ابتدا شبکه عصبی معادل توابع جانشینی ارائه شده و نحوه بیان شبکه عصبی معادل هر تعداد دور از الگوریتم رمز ارائه می‌شود. سپس الگوریتم آموزش شبکه عصبی حاصل جهت یافتن جواب بهینه برای تابع هزینه بیان می‌گردد.

۳-۱- شبکه عصبی معادل توابع جانشینی

هر تابع جانشینی $S: \{0,1\}^m \rightarrow \{0,1\}^n$ توسط یک شبکه هاپفیلد حاوی n+m نورون ارائه می‌شود، که m نورون اول آن متناظر بیتهای تقریب خطی ورودی تابع جانشینی می‌باشد که با Ii با اندیس‌های ۰ تا m-۱ نشان داده می‌شود، و n نورون بعدی متناظر بیتهای تقریب خطی خروجی تابع جانشینی می‌باشد که با Oi با اندیس‌های ۰ تا n-۱ نشان داده می‌شود. با توجه به مؤثر بودن هر بیت تقریب خطی ورودی Sbox در بیتهای تقریب خطی خروجی آن و نیز موثر بودن هر بیت تقریب خطی خروجی Sbox در بیتهای تقریب خطی ورودی آن، در این شبکه هر نورون به تمامی نورون‌های دیگر متصل می‌باشد.

اگر نورونهای I_j و O_k ، که $0 \le j \le m-1$ و $0 \le k \le n-1$ است ، بترتیب دارای مقادیر i_j و o_k باشد، مقدار تابع هزینه بصورت زیر محاسبه می‌شود, که تابع $LAT_S: \{0,1\}^m \times \{0,1\}^n \rightarrow R$ بیانگر توزیع تقریب خطی ورودی/خروجی در تابع جانشینی S می‌باشد و هر زوج تقریب خطی ورودی/خروجی $(X,Y) \in \{0,1\}^m \times \{0,1\}^n$ را به تمایل احتمال تقریب خطی خروجی Y تحت تابع جانشینی S با فرض تقریب خطی ورودی X می‌نگارد.

$$Cost1_S(o_{n-1}, o_{n-2}, ..., o_1, o_0, i_{m-1}, i_{m-2}, ..., i_1, i_0) = -Log_2\left(2LAT_S\left(i_{m-1}\times 2^{m-1} + i_{m-2}\times 2^{m-2} + ... + i_1\times 2 + i_0 \ , \ o_{n-1}\times 2^{n-1} + o_{n-2}\times 2^{n-2} + ... + o_1\times 2 + o_0\right)\right)$$

بنابر این تابع هزینه شبکه معادل تابع جانشینی S برای مقادیر دلخواه نورون ها بصورت $Cost_S: \{0,1\}^m \times \{0,1\}^n \rightarrow R$ خواهد بود :

$$Cost_S(O_{n-1}, O_{n-2}, O_{n-3}, ..., O_1, O_0, I_{m-1}, I_{m-2}, I_{m-3}, ..., I_1, I_0) = \sum_{o_{n-1}=0}^{1}\sum_{o_{n-2}=0}^{1}\cdots\sum_{o_1=0}^{1}\sum_{o_0=0}^{1}\sum_{i_{m-1}=0}^{1}\sum_{i_{m-2}=0}^{1}\cdots\sum_{i_1=0}^{1}\sum_{i_0=0}^{1}\left(\prod_{j=0}^{m-1}(1-i_j+(2\times i_j-1)\times I_j)\right.$$
$$\left.\times\prod_{k=0}^{n-1}(1-o_k+(2\times o_k-1)\times O_k)\times Cost1_S(o_{n-1}, o_{n-2}, ..., o_1, o_0, i_{m-1}, i_{m-2}, ..., i_1, i_0)\right)$$

بعنوان مثال، تابع جانشینی S_q $(0 \le q \le 7)$ بکارگرفته شده در الگوریتم رمز کهکشان، یک تابع جانشینی ۴×۴ با تابع هزینه زیر است:

$$Cost_{Sq}(O_3, O_2, O_1, O_0, I_3, I_2, I_1, I_0) = \sum_{o_3=0}^{1}\sum_{o_2=0}^{1}\sum_{o_1=0}^{1}\sum_{o_0=0}^{1}\sum_{i_3=0}^{1}\sum_{i_2=0}^{1}\sum_{i_1=0}^{1}\sum_{i_0=0}^{1}\left(\prod_{j=0}^{m-1}(1-i_j+(2\times i_j-1)\times I_j)\right.$$
$$\left.\times\prod_{k=0}^{3}(1-o_k+(2\times o_k-1)\times O_k)\times Cost1_{Sq}(o_3, o_2, o_1, o_0, i_3, i_2, i_1, i_0)\right)$$

که : $Cost1_{S_q}(o_3, o_2, o_1, o_0, i_3, i_2, i_1, i_0) = -Log_2\left(2LAT_{S_q}\left(i_3\times 2^3 + i_2\times 2^2 + i_1\times 2 + i_0 \ , \ o_3\times 2^3 + o_2\times 2^2 + o_1\times 2 + o_0\right)\right)$

۳-۲- شبکه عصبی معادل تعداد دور دلخواه از رمز جانشینی-جایگشتی

جهت یافتن یک مشخصه k دوری در یک الگوریتم رمز قطعه‌ای با ساختار جانشینی-جایگشتی و اندازه ورودی/خروجی n بیت ، یک شبکه عصبی بازگشتی تک‌لایه با ۲×k×n نورون خواهیم داشت. جهت سهولت بیان توابع هزینه در شبکه حاصل، نورونها را در دسته های n تایی درنظر می‌گیریم که هر دسته مربوط به ورودی/خروجی توابع جانشینی در یک مرحله است. بطور دقیق تر دسته pام $(0 \le p \le 2k-1)$ را با بردار $\underline{N}_p = (N_{p\times n+n-1}, N_{p\times n+n-2}, N_{p\times n+n-3}, \ldots, N_{p\times n+1}, N_{p\times n}) \in \{0,1\}^n$ نشان می‌هیم که N_ℓ بیانگر نورون ℓ ام است. اگر p زوج باشد، بردار $\underline{N}_p$ نورون‌های متناظر ورودی تابع جانشینی دور rام است، که r = p/۲ و اگر p فرد باشد، بردار $\underline{N}_p$ نورون‌های متناظر خروجی تابع جانشینی دور r ام است، که r = ⌊p/۲⌋ .

۳-۳- الگوریتم آموزش شبکه عصبی

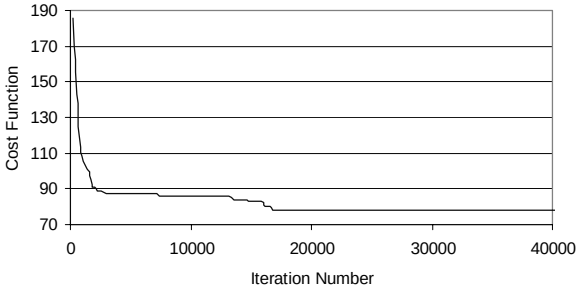
برای یافتن جواب بهینه برای تابع هزینه فوق از بهینه‌سازی با شبکه عصبی هاپفیلد طبق الگوریتم زیر استفاده گردید:

۱. مقداردهی اولیه نورون ها : مقدار نورون‌های متناظر با تقریب خطی دور میانی ممکن است توسط تحلیلگر تعیین شده و یا درحین روند بهینه سازی تعیین شود. مقدار بقیه نورون‌ها بطور بیقاعده مبتنی بر الگوریتم رمز مورد نظر مشخص می‌شود.
۲. انتخاب یک نورون بطور بیقاعده و تغییر مقدار آن.
۳. تنظیم دیگر نورون ها براساس تغییر جدید: این تنظیم با توجه به رابطه تبدیل خطی بین نورونهای متناظر با خروجی توابع جانشینی در یک دور و نورونهای متناظر با ورودی توابع جانشینی در دور بعد انجام می‌شود.
۴. محاسبه مقدار تابع هزینه با توجه به تغییر انجام شده.
۵. پذیرش وضعیت جدید، درصورتیکه مقدار هزینه در وضعیت جدید کمتر از هزینه در وضعیت قبلی باشد.
۶. بررسی شرط توقف و تکرار از گام ۲ درصورت عدم برقراری آن. شرط توقف، عدم تغییر مقدار نورون ها در یک تعداد تکرار متوالی روند بهینه‌سازی می‌باشد، که این تعداد بعنوان یک پارامتر کنترلی بهینه‌سازی بوده و هرچه عدد بزرگتری درنظر گرفته شود، جواب بهتری حاصل خواهد شد.

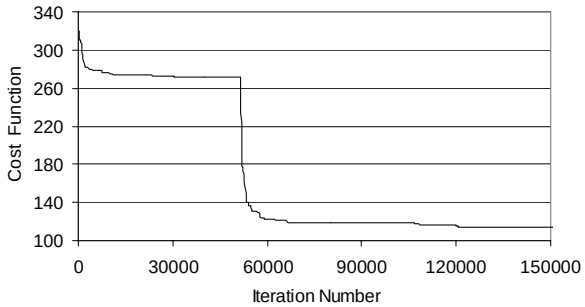
۴- مشخصه های خطی بدست آمده برای کهکشان

همانطور که گفته شد، طرح پیشنهادی را روی الگوریتم رمز کهکشان اعمال کردیم. برای این الگوریتم رمز چند تحلیل تفاضلی ارائه شده [۹،۲]، اما هیچ تحلیل خطی برای آن منتشر نشده است. ازطرفی اگرچه این الگوریتم رمز از الگوریتم رمز سرپنت اقتباس شده است، اما تحلیل خطی ارائه شده برای سرپنت[۸] ارتباطی با تحلیل خطی الگوریتم رمز کهکشان ندارد. زیرا حتی یک تغییر کوچک در الگوریتم رمز ممکن است باعث یک تغییر بزرگ در عملکرد آن (تقویت یا تضعیف) شود و بایستی الگوریتم رمز حاصل مجددا بطور کامل مورد ارزیابی و تحلیل قرار بگیرد.

برای یافتن مشخصه خطی در الگوریتم رمز کهکشان، پارامتر کنترلی بهینه‌سازی برابر ۵۰۰۰۰ درنظر گفته شد. بهترین مشخصه خطی بدست آمده برای الگوریتم رمز کهکشان ۸ دوری، ۹ دوری و ۱۰ دوری بترتیب مطابق جدول (۲) تا جدول (۴) و با تمایل احتمال 2^{-78}، 2^{-114} و 2^{-146} است. هر سطر این جداول تقریب خطی ورودی و خروجی تبدیلات جانشینی در دور مربوطه را نشان می دهد. با توجه به وجود تبدیل خطی بکارگرفته شده بعد از اعمال تبدیل جانشینی در هر دور رمز کهکشان، با اعمال تبدیل خطی بر تقریب خطی خروجی در هر دور تقریب خطی ورودی دور بعد بدست می‌آید. روند تغییرات نابع هزینه تا رسیدن به همگرایی در تعیین این مشخصه ها بترتیب درشکل (۳) تا شکل (۵) آمده است.



شکل (۳): تغییرات مقدار تابع هزینه در روند بهینه سازی در یافتن مشخصه خطی برای رمز کهکشان ۸ دوری تا رسیدن به همگرایی



شکل (۴): تغییرات مقدار تابع هزینه در روند بهینه سازی در یافتن مشخصه خطی برای رمز کهکشان ۹ دوری تا رسیدن به همگرایی

جدول (۲): مشخصه خطی برای الگوریتم رمز کهکشان ۸ دوری

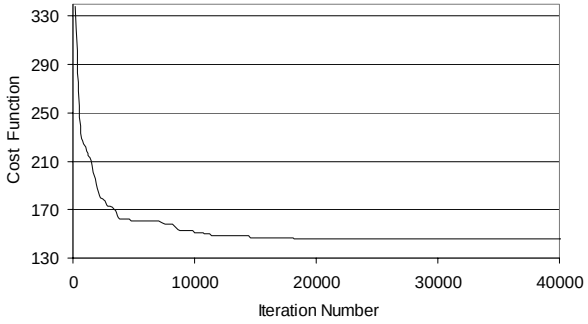
شماره دور		تقریب خطی ورودی/خروجی توابع جانشینی	تمایل احتمال
۱	ورودی	08B000000A0EB000B00F00E0A00000000006E00BF00E00000000000000E00000	$۲^{-۱۶}$
	خروجی	05B000000308100010040080300000000006800140080000000000000800000	
۲	ورودی	00060000000000440000000008000500200000A000000000400000000000500000	$۲^{-۱۶}$
	خروجی	00030000000000CC000000000300080020000800000000020000000000080000	
۳	ورودی	00000040400000000040000000000000000000000000000100008000000000000	$۲^{-۱۱}$
	خروجی	00000020400000000030000000000000000000000000000100008000000000000	
۴	ورودی	00000000000100000000000000000000000000000000040000000000000000000	$۲^{-۵}$
	خروجی	00000000000300000000000000000000000000000000080000000000000000000	
۵	ورودی	04000000000000000000000000000000000000000000000000000000000000000	$۲^{-۳}$
	خروجی	04000000000000000000000000000000000000000000000000000000000000000	
۶	ورودی	02000000000000000000000000001000000000000000000000000000000000000	$۲^{-۳}$
	خروجی	0E000000000000000000000000009000000000000000000000000000000000000	
۷	ورودی	02000440000000000000011000890000000000000001000080100002000000	$۲^{-۲۱}$
	خروجی	01000440000000000000007C000C10000000000000001000040400000A0000000	
۸	ورودی	00A0100102000000000000000000000000000000000A00410000360000000000	$۲^{-۱۰}$
	خروجی	04000000000000000000000000000000000000000000000000000000000000000	
		تمایل احتمال کل مشخصه	$۲^{-۷۸}$

جدول (۳): مشخصه خطی برای الگوریتم رمز کهکشان ۹ دوری

شماره دور		تقریب خطی ورودی/خروجی توابع جانشینی	تمایل احتمال
۱	ورودی	60AA0B0DA000A008E5008F0B80808000D00000B0A0F00A08D0D00A000F0D00E0	$۲^{-۲۹}$
	خروجی	60E30B023000E00F8C00D40150D0700020000010304003052020003000A020080	
۲	ورودی	8418000001E0000002810000C00040B104000000EA0500002000B00E0D000000	$۲^{-۲۷}$
	خروجی	F25600000B10000007250000C000604506000000110800002000100103000000	
۳	ورودی	A1002000000000001000000000000400002000200000000000000000B000000A0	$۲^{-۱۹}$
	خروجی	4D002000000000001000000000000C000020001000000000000000004000000020	
۴	ورودی	00A000000000000000000000000010000000040000000000000000000000001000	$۲^{-۹}$
	خروجی	00300000000000000000000000000C0000000080000000000000000000000002000	
۵	ورودی	00000000000000004000000000000000004000000000000000000000000000000000	$۲^{-۵}$
	خروجی	00000000000000000C0000000000000000020000000000000000000000000000000000	
۶	ورودی	00000000400000000000000000000000000000000000000000000000000000000000	$۲^{-۳}$
	خروجی	00000000400000000000000000000000000000000000000000000000000000000000	
۷	ورودی	00000000001000020040000000000000000000000000000000000000000000000000	$۲^{-۷}$
	خروجی	00000000004000020040000000000000000000000000000000000000000000000000	
۸	ورودی	00400000000000010000300408000000000020000000000000000000000000000010	$۲^{-۱۳}$
	خروجی	00C0000000000010000400E040000000000020000000000000000000000000000010	
۹	ورودی	00000000000000040000000010000200400000A10000300440000000000000000	$۲^{-۱۰}$
	خروجی	00000000000000F00000000E0000E00F00000EE0000D00FF0000000000000000	
		تمایل احتمال کل مشخصه	$۲^{-۱۱۴}$

جدول (۴): مشخصه خطی برای الگوریتم رمز کهکشان ۱۰ دوری

شماره دور		تقریب خطی ورودی/خروجی توابع جانشینی	تمایل احتمال
۱	ورودی	8800080AF00B00880E0FEF0880E8008000FE00F00E00000D00D000D0F90005B6	$۲^{-۳۰}$
	خروجی	7D000503A00100770804840750870050000A8004008000002002000020A9000C16	
۲	ورودی	000000000AA40000000540A09000A2060F0000000005580000004A000400A000	$۲^{-۳۰}$
	خروجی	000000000B1F0000000D2060C000420D0400000000082800000021000200100 0	
۳	ورودی	4400000000000000010000000000004000000000A1000000000000000A00000020	$۲^{-۱۷}$
	خروجی	4500000000000000010000000000000C0000000011000000000000000400000020	
۴	ورودی	0020000000000000000000000001000000004000000000000000000000001000	$۲^{-۹}$
	خروجی	0030000000000000000000000000C0000000080000000000000000000002000	
۵	ورودی	0000000000000004000000000000000004000000000000000000000000000000	$۲^{-۵}$
	خروجی	000000000000000C0000000000000000020000000000000000000000000000000	
۶	ورودی	0000000040000000000000000000000000000000000000000000000000000000	$۲^{-۳}$
	خروجی	0000000040000000000000000000000000000000000000000000000000000000	
۷	ورودی	0000000000100002004000000000000000000000000000000000000000000000	$۲^{-۷}$
	خروجی	0000000000400002004000000000000000000000000000000000000000000000	
۸	ورودی	0040000000000010000300408000000000020000000000000000000000000010	$۲^{-۱۳}$
	خروجی	00C0000000000040000500E040000000000200000000000000000000000000010	
۹	ورودی	0000000000000040000000100002004001000A300003004400000000000000000	$۲^{-۱۸}$
	خروجی	000000000000000C0000000800009002 00B0008D0000C008200000000000000000	
۱۰	ورودی	81C010600000400005A41E00E804450C500008000010000C000000A0000000000	$۲^{-۲۳}$
	خروجی	FBD0B0D00000F0000FEFBA00AF0FFF0DF0000F0000B0000D000000E0000000000	
		تمایل احتمال کل مشخصه	$۲^{-۱۴۶}$



شکل (۵): تغییرات مقدار تابع هزینه در روند بهینه سازی در یافتن مشخصه خطی برای رمز کهکشان ۱۰ دوری تا رسیدن به همگرایی

۵- جمع بندی

در این مقاله، نحوه بکارگیری شبکه عصبی هاپفیلد برای یافتن مشخصه های خطی در الگوریتم رمز قطعه‌ای معرفی شد. برای این منظور، شبکه عصبی معادل یک تابع جانشینی، که براساس آن شبکه عصبی معادل هر تعداد دور از الگوریتم رمز قابل بیان می‌باشد، تعریف شده و الگوریتم آموزش شبکه عصبی حاصل جهت یافتن جواب بهینه برای تابع هزینه بیان شد. بهترین مشخصه خطی بدست آمده برای این الگوریتم رمز کهکشان، مشخصه های ۸، ۹ و ۱۰ دوری بتریب با تمایل احتمال $۲^{-۷۸}$، $۲^{-۱۱۴}$ و $۲^{-۱۴۶}$ است.

بررسی نشان می دهد که با افزایش تعداد دور مشخصه، احتمال گیرکردن در بهینه‌های محلی در هنگام بهینه‌سازی افزایش می‌یابد. جهت جلوگیری از این امر می‌توان از شیوه‌های آموزش احتمالی و ایده Annealing استفاده کرد و با بکارگیری شبکه های عصبی SA و ماشین بولتزمن به کارایی بیشتری دست یافت.

با توجه به شباهت طرح پیشنهادی در این مقاله با آنچه قبلا برای یافتن مشخصه های تفاضلی توسط مولف ارائه شده [۳-۵] و برای انواع الگوریتم های رمز قطعه ای ازجمله کهکشان، معماگر، آی ای اس ۸۰ ، سرپنت و رایندال بکارگرفته شده است بنظر می رسد بتوان این طرح را نیز برای انواع الگوریتم های رمز بکارگرفت.

مراجع

[۱] ع.قائمی‌بافقی، " الگوریتم رمزقطعه‌ای کهکشان"، *مستندات الگوریتم های نامنویسی شده در مسابقه بررسی الگوریتم های رمز قطعه‌ای*، انجمن رمز ایران، ۱۳۸۰.

[۲] ع.قائمی بافقی، ب.صادقیان، "تحلیل تفاضلی الگوریتم رمز کهکشان ۸ دوری"، هشتمین کنفرانس سالانه انجمن کامپیوتر ایران، ۱۳۸۱.

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

[۴] ع.قائمی بافقی، ب.صادقیان،"یک مدل بازنمایی عملکرد تفاضلی الگوریتم‌های رمز قطعه‌ای با ساختار جانشینی- جایگشتی"، نشریه علمی-پژوهشی امیرکبیر، ارسال۱۳۸۱، چاپ ۱۳۸۳.

[۵] ع.قائمی بافقی، ب.صادقیان و ر.صفابخش،"تعیین مشخصه تفاضلی در الگوریتم‌های رمز قطعه ای با شبکه هاپفیلد و ماشین بولتزمن"، مجله فنی مهندسی تربیت مدرس، ارسال ۱۳۸۲، چاپ ۱۳۸۴.

[۶] ع.قائمی‌بافقی، "فلق۲: ابزار تحلیل خطی الگوریتم های رمز قطعه ای" ، ۱۳۸۵.

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

[8] E.Biham, O.Dunkelman and N.Keller, "Linear Cryptanalysis of Reduced Rounds Serpent", 2002.

[9] A.Ghaemi Bafghi, B.Sadeghiyan, "A Differential Boomerang Attack Against 10-round Kahkeshan", IST2005-3rd Biannual International Symposium on Telecommunication, Iran, Shiraz, 2005.

[10] M. Matsui, "Linear Cryptanalysis Method for DES Cipher", Advances in Cryptology - EUROCRYPT ’93 (Lecture Notes in Computer Science no. 765), Springer-Verlag, pp. 386-397, 1994.