

تعیین مشخصه تفاضلی در الگوریتم‌های رمز قطعه‌ای با شبکه هاپفیلد و ماشین بولتزمن

عباس قائمی بافقی^۱، بابک صادقیان^{۲*}، رضا صفا بخش^۳

۱- دانشجوی دکتری، دانشکده مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر

۲- دانشیار دانشکده مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر

۳- استاد دانشکده مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر

* تهران، صندوق پستی ۴۴۱۳-۱۵۸۷۵

Basadegh@ce.aut.ac.ir

چکیده- در این مقاله نشان می‌دهیم که چگونه با به‌کارگیری شبکه‌های عصبی می‌توان مشخصه تفاضلی مناسبی برای الگوریتم‌های رمز قطعه‌ای یافت. به این منظور عملکرد تفاضلی الگوریتم رمز قطعه‌ای مورد بررسی با یک گراف وزندار جهت‌دار نمایش داده می‌شود. با این نمایش، یافتن بهترین مشخصه تفاضلی، معادل با یافتن کم‌وزن‌ترین مسیر چند-شعبه بین دو گره آغازی و پایانی در گراف حاصل است. در این مقاله، ابتدا شبکه هاپفیلد برای یافتن بهترین مسیر چند-شعبه در گراف نمایش عملکرد تفاضلی الگوریتم رمز قطعه‌ای سرپنت به‌کار رفته است. با این شیوه، افزایش تعداد دور مشخصه، باعث افزایش احتمال رسیدن به بهینه‌های محلی در هنگام بهینه‌سازی می‌شود. سپس به‌منظور کاهش این مشکل از شیوه‌های آموزش احتمالی و ایده تابکاری شبیه‌سازی‌شده، استفاده شده و با به‌کارگیری ماشین بولتزمن، کارایی بیشتری به‌دست آمده است. روند بهینه‌سازی برای یافتن یک مشخصه ۴، ۵ و ۶ دوری از الگوریتم رمز سرپنت، ۱۰۰ بار تکرار شده است. در این آزمایشها، جواب مطلوب با به‌کارگیری شبکه هاپفیلد، به ترتیب ۱۰۰، ۲۰ و ۱ بار و با به‌کارگیری ماشین بولتزمن، به ترتیب ۱۰۰، ۹۹ و ۳۰ بار به‌دست آمده است. نتایج بررسیهای انجام شده بیانگر تاثیر مثبت آموزش احتمالی در روند بهینه‌سازی توسط شبکه عصبی است. مقایسه احتمال‌های مشخصه‌های به‌دست آمده با شیوه پیشنهادی در این مقاله با احتمال‌های هشت مشخصه گزارش شده در مقالات دیگر نشان می‌دهد که در شش مورد، نتایج ارائه شده در این مقاله بهتر از نتایج گزارش شده در سایر مقالات است و در دو مورد، احتمال‌های مشخصه‌های تفاضلی به‌دست آمده برابر با احتمال مشخصه‌های نظیر در سایر مقالات است. همچنین یک مشخصه تفاضلی برای الگوریتم رمز سرپنت ۷ دوری با استفاده از ماشین بولتزمن به‌دست آمده که احتمال 2^{-125} دارد. این مشخصه، با صرف‌نظر کردن از مشخصه‌های بومرنگ گزارش شده از این الگوریتم رمز، اولین مشخصه تفاضلی برای بیش از ۶ دور از آن است. این مقایسه نشان دهنده کارایی و کارآمدی شبکه‌های عصبی برای یافتن مشخصه تفاضلی مناسب است، به طوری که کارایی در هاپفیلد بیشتر از ماشین بولتزمن است و کارآمدی در ماشین بولتزمن بیشتر است.

کلید واژگان: تحلیل تفاضلی، ساختار جانشینی-جایگشتی، رمز قطعه‌ای سرپنت، شبکه هاپفیلد، ماشین بولتزمن.

۱- مقدمه

تحلیل تفاضلی در سال ۱۹۹۰ توسط بیهام و شامیر ابداع شد [۳]. این روش تحلیل در دو مرحله طراحی حمله و اجرای حمله انجام می‌شود. در مرحله طراحی حمله، تحلیلگر با به‌کارگیری ویژگیها و نقاط ضعف الگوریتم رمز، به دنبال یافتن یک مشخصه تفاضلی با احتمال بالا است. در مرحله اجرای حمله، تحلیلگر باید به اندازه کافی زوج متن رمز شده با تفاضل به دست آمده در مرحله طراحی را جمع‌آوری کرده و توسط آنها بیت‌های کلید مؤثر در مشخصه را با انجام یک شیوه شمارش به دست آورد.

در [۱] برای یافتن مشخصه مناسب برای طراحی حمله مبتنی بر تحلیل تفاضلی، مدل بازنمایی عملکرد تفاضلی الگوریتم رمز قطعه‌ای ارائه شد. در این مدل هر یک از اجزای الگوریتم رمز توسط یک گراف جهتدار و زنده نشان داده می‌شود. از ترکیب گرافهای متناظر با هر یک از اجزای یک الگوریتم رمز قطعه‌ای، یک گراف جهتدار و زنده به دست می‌آید. در نتیجه، برای یافتن مشخصه تفاضلی k دوری، یک گراف $2k$ سطحی به دست آمده و مسأله یافتن بهترین مشخصه برای این الگوریتم رمز، معادل با یافتن مسیری چند-شعبه از گره آغازی به گره پایانی در این گراف است، به طوری که جمع مسیرهای آن کمترین مقدار ممکن باشد. در [۵،۴،۱] شیوه بهینه‌سازی اجتماع مورچگان برای یافتن بهترین مسیر چند-شعبه در گراف نمایش عملکرد تفاضلی الگوریتم رمز قطعه‌ای به کار رفته شده است.

در این مقاله، قابلیت به‌کارگیری شبکه‌های عصبی هاپفیلد و ماشین بولتزمن برای یافتن بهترین مسیر چند-شعبه در گراف نمایش عملکرد تفاضلی الگوریتم رمز قطعه‌ای بررسی و چگونگی به‌کارگیری آنها مطرح می‌شود. به بیان دیگر به دنبال پاسخگویی به این سوالات هستیم که آیا شبکه‌های عصبی را می‌توان برای یافتن بهترین مسیر چند-شعبه در گراف نمایش عملکرد

تفاضلی به کار برد یا خیر؟ میزان کارایی و کارآمدی آنها چقدر است؟ برای این منظور، روند بهینه‌سازی توسط هر یک از دو شیوه ۱۰۰ مرتبه برای هر یک از موارد مورد بررسی، تکرار شده و بهترین جواب انتخاب شد. در ادامه عملکرد دو شبکه را از نظر کارایی و کارآمدی مقایسه کردیم. کارایی را با توجه به زمان لازم برای حصول نتیجه مطلوب در هر شیوه تعریف می‌کنیم و "یک شیوه بهینه‌سازی را کارتر می‌گوییم اگر در زمان کمتری نتیجه مطلوب آزمایش را به دست دهد". به بیان دیگر، کارایی با توجه به پیچیدگی اجرا تعیین شده و شیوه‌ای را کارتر می‌گوییم که پیچیدگی اجرای کمتری دارد. کارآمدی را براساس نتیجه بخشی هر شیوه تعریف می‌کنیم و "یک شیوه بهینه‌سازی را برای حل یک مسأله کارآمدتر می‌گوییم که در تعداد موارد بیشتری، جواب مطلوب را به دست دهد".

در بخش ۲، الگوریتم رمز قطعه‌ای سرپنت، به عنوان یک نمونه الگوریتم رمز قطعه‌ای و بستری برای نشان دادن چگونگی به‌کارگیری شبکه‌های عصبی هاپفیلد و ماشین بولتزمن برای یافتن بهترین مشخصه تفاضلی، به طور اجمالی معرفی می‌شود. در بخش ۳، مدل بازنمایی عملکرد تفاضلی الگوریتم رمز قطعه‌ای و نحوه به‌کارگیری شبکه‌های عصبی در تعیین مسیر چند-شعبه مناسب در گراف نمایش عملکرد تفاضلی الگوریتم رمز تشریح می‌شود. در بخشهای ۴ و ۵ مشخصه‌های تفاضلی به دست آمده برای الگوریتم رمز سرپنت با به‌کارگیری شبکه هاپفیلد و ماشین بولتزمن بیان می‌شود. در بخش ۶، با توجه به نتایج به دست آمده، کارایی به‌کارگیری شبکه هاپفیلد و ماشین بولتزمن با یکدیگر مقایسه و پیشنهادهایی برای ادامه پژوهش مطرح می‌شود.

۲- معرفی سرپنت

سرپنت یک شبکه جانشینی-جایگشتی با اندازه قطعه ورودی/خروجی ۱۲۸ بیت و اندازه کلید از ۱۲۸ تا ۲۵۶

۳- بیان مسأله در قالب شبکه عصبی

در [۱] برای یافتن مشخصه تفاضلی مناسب به منظور طراحی حمله مبتنی بر تحلیل تفاضلی، مدل بازنمایی عملکرد تفاضلی الگوریتم‌های رمز قطعه‌ای ارائه شد. در این مدل هر یک از اجزای الگوریتم رمز توسط یک گراف جهتدار وزندار نمایش داده می‌شود. از ترکیب گرافهای متناظر با هر یک از اجزای الگوریتم رمز قطعه‌ای، یک گراف جهتدار وزندار به دست می‌آید. در نتیجه، برای یافتن مشخصه تفاضلی k دوری، یک گراف $2k$ سطحی به دست آمده و مسأله یافتن بهترین مشخصه برای این الگوریتم رمز، معادل با یافتن یک مسیر چند-شعبه از گره آغازی به گره پایانی در این گراف است؛ به طوری که جمع مسیرهای آن کمترین مقدار ممکن باشد. در [۵،۴،۱] شیوه بهینه‌سازی اجتماع مورچگان برای یافتن بهترین مسیر چند-شعبه در گراف نمایش عملکرد تفاضلی الگوریتم رمز قطعه‌ای به کار رفت.

بهینه‌سازی با شبکه‌های عصبی برای حل مسائل متعدد و متنوعی از جمله جایگذاری قطعات در طراحی VLSI [۸،۷]، n وزیر [۹]، خوشه بندی [۱۰-۱۲]، برش و بسته‌بندی [۱۳،۱۴]، افراز گراف [۱۵]، رنگ آمیزی گراف [۱۶-۱۹]، مسیریابی ترافیک شبکه [۲۰]، یافتن کوتاهترین مسیر [۲۱-۲۶] و فروشنده دوره‌گرد [۲۷-۳۱] به کار رفته است.

در این مقاله یک شبکه عصبی بازگشتی برای یافتن بهترین مسیر چند-شعبه در گراف نمایش عملکرد تفاضلی الگوریتم رمز قطعه‌ای معرفی شده و شبکه‌های عصبی هاپفیلد و ماشین بولتزمن برای یافتن بهترین مسیر چند-شعبه در این گراف به کار می‌رود. برای این منظور، شبکه عصبی معادل با هر تابع جانشینی - که براساس آن شبکه عصبی معادل هر تعداد دور از الگوریتم رمز قابل بیان است - تعریف شده است. در این شبکه عصبی طول هر مسیر در گراف نمایش عملکرد تفاضلی الگوریتم رمز قطعه‌ای، توسط تابع هزینه مشخص می‌شود. بنابراین برای

بیت است [۶]. ساختار رمز بخشهای جایگشت اولیه، ۳۲ بار تکرار تابع دور و جایگشت نهایی را دارد. در این الگوریتم از هشت تابع جانشینی با ورودی و خروجی ۴ بیتی، که مطابق جدول ۱ با S_1 تا S_7 مشخص می‌شوند، استفاده شده است. در تابع دور Am ، $i \in \{0, \dots, 31\}$ فقط از تکرار یک تابع جانشینی مشخص استفاده می‌شود که شماره آن (j) بر طبق رابطه (۱) تعیین می‌شود:

$$j = i \bmod 8, \quad i \in \{0, \dots, 31\} \quad (1)$$

جدول ۱ توابع جانشینی به کار رفته در الگوریتم رمز سرینت

شماره ورودی تابع جانشینی	۰	۱	۲	۳	۴	۵	۶	۷	۸	۹	A	B	C	D	E	F
۰	C	۹	۰	۷	۲	۴	D	E	B	۵	۶	A	۱	F	۸	۳
۱	۴	۳	D	۶	۸	E	B	۱	A	۵	۰	۹	۷	۲	C	F
۲	۲	۵	B	۰	۴	E	۱	D	F	A	C	۳	۹	۷	۶	۸
۳	E	۵	۷	A	۴	۲	۱	D	۳	۶	۹	C	۸	B	F	۰
۴	D	۷	E	۹	A	۴	۵	۲	۶	B	۰	C	۳	۸	F	۱
۵	۱	۷	۶	D	۸	E	۳	۰	C	۹	A	۴	B	۲	۵	F
۶	۰	A	۳	D	F	۱	۹	E	B	۶	۴	۸	۵	C	۲	۷
۷	۶	۵	۳	۹	A	C	۴	۷	B	۲	۸	E	۰	F	D	۱

در تابع دور Am ، $i \in \{0, \dots, 31\}$ ، ابتدا ورودی B_i^{\wedge} با کلید K_i^{\wedge} تحت عمل XOR ترکیب شده و سپس ۳۲ تابع جانشینی مشابه به طور موازی به آن اعمال می‌شود. به عنوان مثال در تابع دور اول فقط از ۳۲ بار تکرار موازی S_1 استفاده می‌شود. آنگاه بردار میانی با استفاده از تبدیل خطی تغییر یافته و B_1^{\wedge} را تولید می‌کند. به طور مشابه تابع دور دوم نیز ۳۲ نسخه موازی S_1 روی $(B_1^{\wedge} \oplus K_1^{\wedge})$ اعمال شده و بردار میانی حاصل، با اعمال تبدیل خطی بر روی خروجی B_2^{\wedge} تبدیل می‌شود. دور آخر اندکی با بقیه تفاوت دارد، به طوری که ابتدا S_7 بر روی $(B_{31}^{\wedge} \oplus K_{31}^{\wedge})$ اعمال شده و سپس به جای اعمال تبدیل خطی بر بردار میانی حاصل، آن تحت عمل XOR با K_{32}^{\wedge} ترکیب و B_{32}^{\wedge} را تولید می‌کند.

در این مدل، در نمودار جریان داده الگوریتم رمز به جای هر یک از اجزای آن، گراف‌های معادل آنها را قرار می‌دهیم. در نتیجه الگوریتم رمز به یک گراف جهت‌دار وزندار چند سطحی تبدیل خواهد شد.

ملاحظه می‌شود که به‌کارگیری این مدل برای یافتن مشخصه k دوری در هر الگوریتم رمز قطعه‌ای با ساختار جانشینی - جایگشتی یک گراف $2k+3$ سطحی خواهیم داشت. برای مثال بازنمایی عملکرد تفاضلی الگوریتم رمز قطعه‌ای سرپنت سه دوری مطابق شکل ۲ خواهد بود. در این شکل پیکان‌های پررنگ، بیانگر تبدیل خطی است که نوعی نگاشت ثابت است.

فرض کنید M و N به‌ترتیب گره‌های آغازی و پایانی در گراف نمایش عملکرد تفاضلی الگوریتم رمز قطعه‌ای باشد. متناظر با هر یال خروجی گره M می‌توان مسیرهای مختلفی را از گره M تا گره N در نظر گرفت. اگر $path_i(M,N)$ یک مسیر دلخواه از گره M به گره N و شامل یال خروجی i ام گره M باشد، مجموعه $\left\{ path_i(M,N) \mid 1 \leq i \leq \text{Outdegree}_M \right\}$ را یک مسیر چند-شعبه از گره M به گره N تعریف می‌کنیم. وزن هر مسیر چند-شعبه را برابر با وزن تمام مسیرهای آن در نظر می‌گیریم. هر مسیر چند-شعبه در این گراف، معادل با یک مشخصه تفاضلی از الگوریتم رمز بوده و مسیر چند-شعبه با حداقل وزن، معادل با مشخصه تفاضلی با حداکثر احتمال است. بنابراین یافتن بهترین مشخصه برای الگوریتم رمز، معادل با یافتن مسیری چند-شعبه با حداقل وزن از گره آغاز تا گره پایان در گراف نمایش عملکرد تفاضلی آن است.

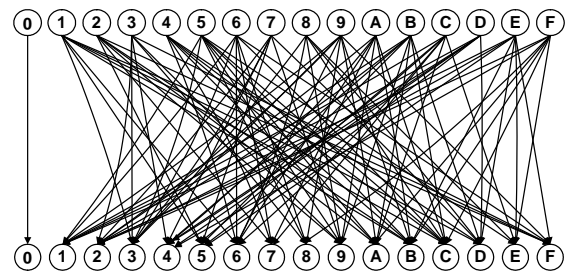
۲-۳- شبکه عصبی بازگشتی معادل با توابع جانشینی

هر تابع جانشینی $S: \{0,1\}^m \rightarrow \{0,1\}^n \rightarrow R$ توسط یک شبکه بازگشتی حاوی $n+m$ نورون با مقدار دودویی معادل‌سازی می‌شود، که m نورون اول آن متناظر بیت‌های

یافتن مسیر چند-شعبه مناسب در گراف مربوط، لازم است تابع هزینه در شبکه عصبی معادل آن حداقل شود. در ادامه این بخش ابتدا مدل بازنمایی عملکرد تفاضلی الگوریتم رمز قطعه‌ای را به اختصار معرفی و سپس شبکه عصبی معادل توابع جانشینی و نحوه ارائه شبکه عصبی معادل با هر تعداد دور از الگوریتم رمز را مطرح می‌کنیم.

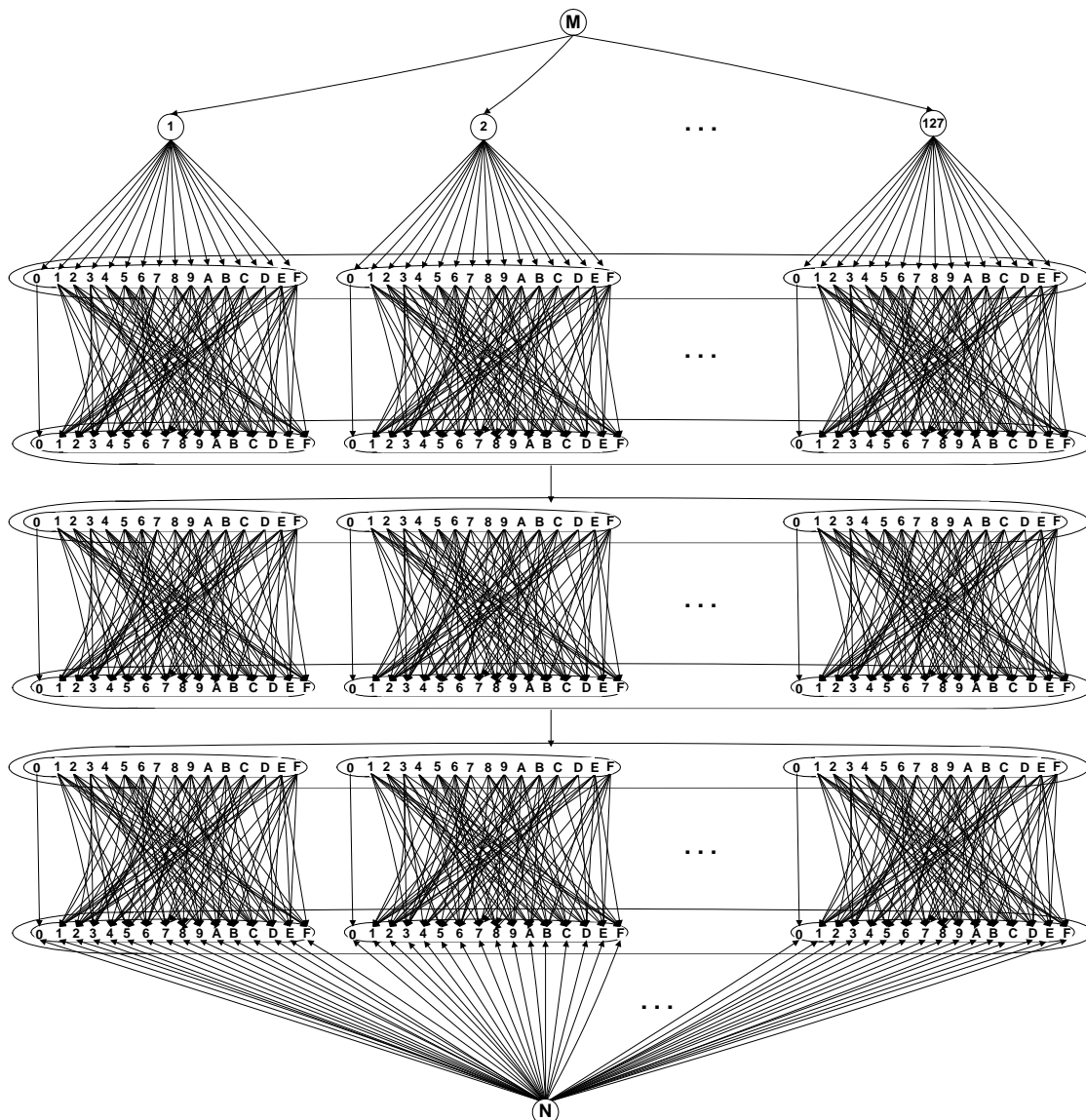
۳-۱- مدل بازنمایی عملکرد تفاضلی رمز قطعه‌ای

معرفی کامل این مدل در [۱] آمده است. در این مدل توزیع تفاضلات ورودی/خروجی در هر تابع جانشینی توسط یک گراف جهت‌دار وزندار دوبخشی $G(V,E,W)$ با 2^m+2^n گره بیان می‌شود، که m و n به‌ترتیب اندازه ورودی و خروجی تابع جانشینی است. 2^m گره به‌عنوان گره‌های آغازی که با اندیس‌های دودویی 0 تا 2^m-1 نامگذاری می‌شود و 2^n گره به‌عنوان گره‌های پایانی که با اندیس‌های دودویی 0 تا 2^n-1 نامگذاری می‌شود. یالهای این گراف بر اساس جدول توزیع تفاضلات تعیین می‌شود و وزن هر یال برابر منهای لگاریتم مقدار متناظر با آن در جدول توزیع تفاضلات در مبنای ۲ است. به بیان دیگر اگر مقدار متناظر با یال (X,Y) در جدول توزیع تفاضلات برابر p باشد، وزن این یال $W_{X,Y} = -\log_2(p)$ خواهد بود. برای مثال نمایش عملکرد تفاضلی تابع جانشینی Sbox3 در الگوریتم رمز سرپنت به‌صورت شکل ۱ است، که در آن وزن یال‌ها نشان داده نشده است.



شکل ۱ نمایش عملکرد تفاضلی Sbox3 در الگوریتم رمز

سرپنت



شکل ۲ بازنمایی عملکرد تفاضلی الگوریتم رمز قطعه‌ای سرپنت سه دوری

اگر نورون‌های I_j و O_k ، $0 \leq k \leq n-1$ و $0 \leq j \leq m-1$ ، به ترتیب دارای مقادیر I_j و O_k باشند، تابع هزینه را به صورت رابطه (۲) تعریف می‌کنیم. که در این رابطه، تابع ورودی/خروجی در تابع جانشینی S بوده و هر زوج تفاضل ورودی/خروجی $(X, Y) \in \{0,1\}^m \times \{0,1\}^n$ را به احتمال رخداد تفاضل خروجی Y تحت تابع جانشینی S با فرض تفاضل ورودی X می‌نگارد. بنابراین تابع هزینه

تفاضل ورودی تابع جانشینی است و با I_j ، $0 \leq i \leq m-1$ نشان داده می‌شود، و n نورون بعدی متناظر بیت‌های تفاضل خروجی تابع جانشینی می‌باشد و با O_i ، $0 \leq i \leq n-1$ ، نشان داده می‌شود. با توجه به مؤثر بودن هر بیت تفاضل ورودی S_{box} در بیت‌های تفاضل خروجی آن و نیز مؤثر بودن هر بیت تفاضل خروجی S_{box} در بیت‌های تفاضل ورودی آن، در این شبکه خروجی هر نورون به ورودی تمامی نورون‌های دیگر متصل است.

نورونی مربوط به ورودی/خروجی توابع جانشینی در یک مرحله باشد.

به بیان دقیق تر، گروه p ($0 \leq p \leq 2k - 1$) را با بردار

$$\underline{N}_p = (N_{p \times n + n - 1}, N_{p \times n + n - 2}, N_{p \times n + n - 3}, \dots, N_{p \times n + 1}, N_{p \times n}) \in \{0, 1\}^n$$

نشان می دهیم که در آن N_ℓ بیانگر نورون ℓ ام است.

اگر p زوج باشد، بردار \underline{N}_p نورون های متناظر ورودی تابع جانشینی دور r ام است، که $r = p/2$ و اگر p فرد باشد، بردار \underline{N}_p نورون های متناظر خروجی تابع جانشینی دور r ام است، که $r = \lfloor p/2 \rfloor$.

برای مثال، شبکه عصبی لازم برای یافتن مشخصه تفاضلی k دوری در الگوریتم رمز قطعه ای سرپنت $256k$ نورون داشته و تابع هزینه آن به شکل رابطه (5) است، که در آن، $q = r \bmod 8$ است و تابع هزینه $Cost_{S_q}$ مطابق رابطه (4) تعریف شده است.

شبکه، معادل با تابع جانشینی S برای مقادیر دلخواه نورونها مطابق رابطه (3) و به صورت زیر خواهد بود.

$$Cost_S : \{0, 1\}^m \times \{0, 1\}^n \rightarrow R$$

برای مثال، تابع جانشینی S_q ($0 \leq q \leq 7$) به کار رفته در الگوریتم رمز سرپنت، یک تابع جانشینی 4×4 است، که تابع هزینه آن مطابق رابطه (4) تعریف می شود.

3-3- شبکه عصبی معادل تعداد دور دلخواه از رمز جانشینی-جایگشتی

با به کارگیری این مدل برای یافتن مشخصه k دوری در الگوریتم رمز قطعه ای با ساختار جانشینی-جایگشتی و اندازه ورودی/خروجی n بیت، شبکه عصبی بازگشتی تک لایه با $2 \times k \times n$ نورون خواهیم داشت. برای سهولت در بیان توابع هزینه در شبکه حاصل، نورونها را به صورت گروه هایی n تایی در نظر می گیریم به طوری که هر گروه n

$$Cost_{1S}(o_{n-1}, o_{n-2}, \dots, o_1, o_0, i_{m-1}, i_{m-2}, \dots, i_1, i_0) = -\log_2(DD_S(i_{m-1} \times 2^{m-1} + i_{m-2} \times 2^{m-2} + \dots + i_1 \times 2 + i_0, o_{n-1} \times 2^{n-1} + o_{n-2} \times 2^{n-2} + \dots + o_1 \times 2 + o_0)) \quad (2)$$

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

$$Cost_{S_q}(O_3, O_2, O_1, O_0, I_3, I_2, I_1, I_0) = \sum_{o_3=0}^1 \sum_{o_2=0}^1 \sum_{o_1=0}^1 \sum_{o_0=0}^1 \sum_{i_3=0}^1 \sum_{i_2=0}^1 \sum_{i_1=0}^1 \sum_{i_0=0}^1 \left(\prod_{j=0}^{m-1} (1 - i_j + (2 \times i_j - 1) \times I_j) \times \prod_{k=0}^3 (1 - o_k + (2 \times o_k - 1) \times O_k) \times Cost_{1S_q}(o_3, o_2, o_1, o_0, i_3, i_2, i_1, i_0) \right) \quad (4)$$

که :

$$Cost_{1S_q}(o_3, o_2, o_1, o_0, i_3, i_2, i_1, i_0) = -\log_2(DD_{S_q}(i_3 \times 2^3 + i_2 \times 2^2 + i_1 \times 2 + i_0), (o_3 \times 2^3 + o_2 \times 2^2 + o_1 \times 2 + o_0))$$

$$Cost(\text{Serpent}, k) \quad (5)$$

$$= \sum_{r=0}^{k-1} \sum_{j=0}^{31} Cost_{S_q}(N_{2r \times n + 4j + 3}, N_{2r \times n + 4j + 2}, N_{2r \times n + 4j + 1}, N_{2r \times n + 4j}, N_{(2r+1) \times n + 4j + 3}, N_{(2r+1) \times n + 4j + 2}, N_{(2r+1) \times n + 4j + 1}, N_{(2r+1) \times n + 4j})$$

۴- بهینه‌سازی با شبکه هاپفیلد

شبکه هاپفیلد یک شبکه عصبی انجمنی است که در سال ۱۹۸۲ ابداع شده است [۳۲]. در سال ۱۹۸۵، هاپفیلد و تانک این شبکه را توسعه داده و برای حل مسائل بهینه‌سازی به‌کار بردند [۳۳]. در این شبکه، نورون‌ها در رفتاری متقابل با یکدیگر در نوعی همبندی بازگشتی تابع هزینه را حداقل می‌کنند. شبکه هاپفیلد برای حل مسائل متنوع بهینه‌سازی از جمله در [۷، ۸، ۱۰، ۱۴، ۱۵، ۱۷، ۱۹، ۲۲، ۲۴، ۲۸، ۲۹، ۳۴-۴۱] به‌کار برده شده است. در این بخش این شبکه برای تعیین بهترین مشخصه تفاضلی به‌کار رفته است، که برای این منظور تابع هزینه تعریف شده در بخش قبل حداقل می‌شود.

۴-۱- الگوریتم آموزش شبکه هاپفیلد

- برای یافتن جواب بهینه تابع هزینه بالا، از بهینه‌سازی با شبکه هاپفیلد طبق الگوریتم زیر استفاده شد.
۱. مقداردهی اولیه نورون‌ها: مقدار نورون‌های متناظر با تفاضل دور میانی توسط تحلیلگر تعیین و مقدار سایر نورون‌ها با توجه به حالات ممکن در گراف نمایش عملکرد تفاضلی الگوریتم رمز سرپنت، به‌طور دلخواه^۱ مشخص می‌شود.
 ۲. انتخاب یک نورون به‌طور دلخواه و تغییر مقدار آن.
 ۳. تنظیم سایر نورون‌ها 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، در صورتی که مقدار تابع هزینه در وضعیت جدید کمتر از تابع هزینه در وضعیت قبلی باشد.

۶. بررسی شرط توقف و تکرار از گام ۲ در صورت عدم برقراری آن. شرط توقف، عدم تغییر مقدار نورون‌ها در یک تعداد تکرار متوالی از روند بهینه‌سازی است، که این تعداد به‌عنوان پارامتر کنترلی بهینه‌سازی عمل می‌کند و اگر عدد بزرگتری در نظر گرفته شود، جواب بهتری حاصل خواهد شد.

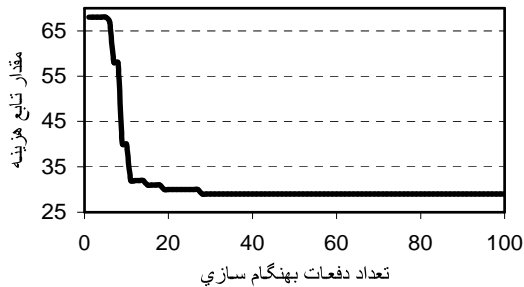
۴-۲- مشخصه‌های تفاضلی به‌دست آمده

برای الگوریتم رمز سرپنت

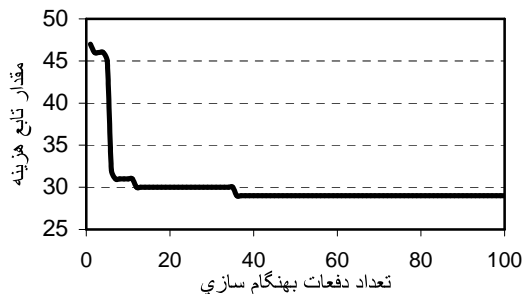
الگوریتم بهینه‌سازی تشریح شده در بخش قبل به‌منظور یافتن مشخصه‌های ۴، ۵ و ۶ دوری از الگوریتم رمز سرپنت به‌کار برده شده برای یافتن بهترین جواب، الگوریتم بهینه‌سازی ۱۰۰ مرتبه برای هر یک از موارد مورد بررسی تکرار و بهترین جواب انتخاب شد. مقدار تفاضل ورودی دور میانی، بر اساس تحلیل‌های تفاضلی منتشر شده از این الگوریتم رمز در [۴۲-۴۴] تعیین شده است، تا مشخصه‌های تفاضلی حاصل از روش پیشنهادی در این مقاله را از نظر احتمال آنها، بتوان با نتایج منتشر شده در مقالات دیگر مقایسه کرد.

سه مشخصه ۴ دوری در [۴۲-۴۴] ارائه شده است. مشخصه‌های ارائه شده در مقالات [۴۲، ۴۳] مربوط به دورهای اول تا چهارم بوده و به‌ترتیب Sbox چهارم و Sbox دوم در دور سوم آنها فعال در نظر گرفته شده است. مشخصه ارائه شده در [۴۴] مربوط به دور ششم تا نهم است، که Sbox ششم از دور هشتم در آن فعال است. مقدار ورودی تابع جانشینی فعال در هر سه مشخصه فوق مقدار ۴ بوده و احتمال این سه مشخصه در مقالات مذکور به‌ترتیب 2^{-29} ، 2^{-31} و 2^{-34} گزارش شده است. مشخصه‌های به‌دست آمده با به‌کارگیری شبکه هاپفیلد، برای دورهای ذکر شده در فوق و با همان شماره و ورودی Sbox فعال در دور میانی (مشابه موارد بالا)، در جداول ۲، ۳ و ۴ آورده شده است. این سه مشخصه به‌ترتیب دارای احتمال 2^{-29} ، 2^{-29} و 2^{-32} هستند.

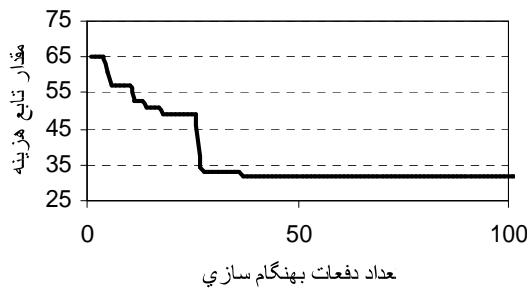
بهینه‌سازی، جواب مطلوب به دست آمده و در هیچ یک از تکرارها، در بهینه محلی جا نمانده است.



شکل ۳ تغییرات مقدار تابع هزینه در روند بهینه‌سازی در مشخصه تفاضلی جدول ۲ تا رسیدن به همگرایی



شکل ۴ تغییرات مقدار تابع هزینه در روند بهینه‌سازی در مشخصه تفاضلی جدول ۳ تا رسیدن به همگرایی



شکل ۵ تغییرات مقدار تابع هزینه در روند بهینه‌سازی در مشخصه تفاضلی جدول ۴ تا رسیدن به همگرایی

چهار مشخصه ۵ دوری در [۴۲-۴۴] ارائه شده است. مشخصه ارائه شده در [۴۲] و یک مشخصه در [۴۴] مربوط به دور پنجم تا نهم بوده و Sbox ششم از دور هشتم در آنها فعال در نظر گرفته شده است. احتمال این دو مشخصه

جدول ۲ مشخصه تفاضلی چهار دوری از رمز سرپنت به دست آمده با هاپفیلد (تابع جانشینی چهارم از دور سوم فعال است)

شماره دور	تفاضل ورودی و خروجی توابع جانشینی در مشخصه یک دوری	احتمال
۱	ورودی	۲-۱۱ 00D0000000000000CA00300D000000000
	خروجی	00200000000000001A00E004000000000
۲	ورودی	۲-۵ 0000000000000000000000000000400500
	خروجی	0000000000000000000000000000A00400
۳	ورودی	۲-۳ 000040000000000000000000000000000
	خروجی	0000A0000000000000000000000000000
۴	ورودی	۲-۱۰ 000200040000000000000000010000810
	خروجی	0006000300000000000000000070000C70
۲-۲۹	احتمال کل مشخصه	

جدول ۳ مشخصه تفاضلی چهار دوری از رمز سرپنت به دست آمده با هاپفیلد (تابع جانشینی دوم از دور سوم فعال است)

شماره دور	تفاضل ورودی/خروجی توابع جانشینی در مشخصه یک دوری	احتمال
۱	ورودی	۲-۱۱ D0000000000000CA00800900000000000
	خروجی	200000000000001A00E00400000000000
۲	ورودی	۲-۵ 00000000000000000000000000004005000
	خروجی	0000000000000000000000000000A0040000
۳	ورودی	۲-۳ 004000000000000000000000000000000
	خروجی	00A000000000000000000000000000000
۴	ورودی	۲-۱۰ 020004000000000000000000100008100
	خروجی	060003000000000000000000E0000C700
۲-۲۹	احتمال کل مشخصه	

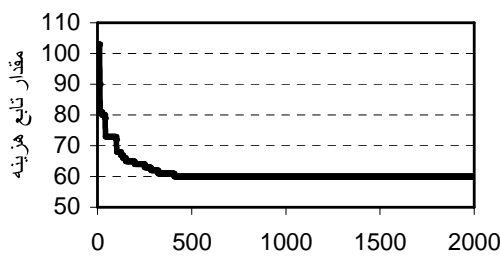
جدول ۴ مشخصه تفاضلی چهار دوری از رمز سرپنت به دست آمده با هاپفیلد (تابع جانشینی ششم از دور هشتم فعال است)

شماره دور	تفاضل ورودی/خروجی توابع جانشینی در مشخصه یک دوری	احتمال
۶	ورودی	۲-۱۲ 04007000000000006006000D0060000000
	خروجی	0A0020000000001001000A0040000000
۷	ورودی	۲-۵ 00000000000000000000000000001005
	خروجی	0000000000000000000000000000A004
۸	ورودی	۲-۲ 000000400000000000000000000000000
	خروجی	000000A00000000000000000000000000
۹	ورودی	۲-۱۳ 1000020004000000000000000100008
	خروجی	F0000C0006000000000000000050000F
۲-۳۲	احتمال کل مشخصه	

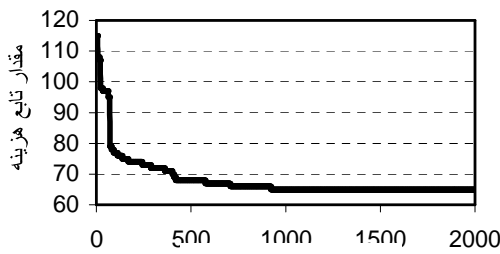
روند تغییرات مقدار تابع هزینه تا رسیدن به همگرایی در هر یک از این سه مشخصه، به ترتیب در شکل های ۳، ۴ و ۵ آورده شده است.

در هر یک از این سه مورد، در تمامی ۱۰۰ بار تکرار

این دو مشخصه به ترتیب دارای احتمال 2^{-60} و 2^{-65} می‌باشند. روند تغییرات مقدار تابع هزینه تا رسیدن به همگرایی در هر یک از موارد فوق به ترتیب در شکل‌های ۶ و ۷ آمده است. در دو مورد فوق، از میان ۱۰۰ بار تکرار بهینه‌سازی به ترتیب ۲۰ و ۱۸ مرتبه جواب مطلوب به دست آمده و در بقیه دفعات تکرار، روند بهینه‌سازی در بهینه محلی افتاده است.



شکل ۶ تغییرات مقدار تابع هزینه در روند بهینه‌سازی در مشخصه تفاضلی جدول ۵ تا رسیدن به همگرایی



شکل ۷ تغییرات مقدار تابع هزینه در روند بهینه‌سازی در مشخصه تفاضلی جدول ۶ تا رسیدن به همگرایی

مشخصه ۶ دوری ارائه شده در [۴۴] مربوط به دور اول تا ششم است که Sbox پانزدهم از دور چهارم در آن فعال بوده و مقدار ورودی ۴ برای آن در نظر گرفته شده است. احتمال این مشخصه برابر 2^{-97} است. مشخصه به دست آمده با شبکه هاپفیلد مطابق جدول ۷ است، که احتمال 2^{-94} دارد. روند تغییرات تابع هزینه تا رسیدن به همگرایی در مشخصه فوق در شکل ۸ آورده شده است. از میان ۱۰۰ تکرار بهینه‌سازی برای یافتن مشخصه فوق، فقط یک بار جواب مطلوب به دست آمده و در سایر دفعات، روند بهینه‌سازی در بهینه محلی گیر افتاده است.

در [۴۴،۴۲] به ترتیب 2^{-60} و 2^{-61} گزارش شده است. مشخصه ارائه شده در [۴۳] و یک مشخصه در [۴۴] مربوط به دور اول تا پنجم بوده و Sbox دوم از دور سوم در آنها فعال در نظر گرفته شده است. احتمال این دو مشخصه در [۴۴،۴۳] به ترتیب 2^{-80} و 2^{-67} گزارش شده است. مقدار ورودی تابع جانشینی فعال در همه مشخصه‌های فوق برابر ۴ بوده است. مشخصه‌های به دست آمده با شبکه هاپفیلد در این مقاله، برای دوره‌های ذکر شده در فوق و با همان شماره و ورودی Sbox فعال در دور میانی (مشابه موارد بالا)، به ترتیب در جداول ۵ و ۶ آورده شده است.

جدول ۵ مشخصه تفاضلی دوره‌های پنجم تا نهم از الگوریتم رمز سرپنت به دست آمده با شبکه هاپفیلد

شماره دور	تفاضل ورودی و خروجی توابع جانشینی در مشخصه یک دوری	احتمال
۵	ورودی	2^{-26}
	خروجی	
۶	ورودی	2^{-14}
	خروجی	
۷	ورودی	2^{-5}
	خروجی	
۸	ورودی	2^{-2}
	خروجی	
۹	ورودی	2^{-13}
	خروجی	
2^{-60}	احتمال کل مشخصه	

جدول ۶ مشخصه تفاضلی دوره‌های اول تا پنجم از الگوریتم رمز سرپنت به دست آمده با شبکه هاپفیلد

شماره دور	تفاضل ورودی و خروجی توابع جانشینی در مشخصه یک دوری	احتمال
۱	ورودی	2^{-11}
	خروجی	
۲	ورودی	2^{-5}
	خروجی	
۳	ورودی	2^{-3}
	خروجی	
۴	ورودی	2^{-13}
	خروجی	
۵	ورودی	2^{-33}
	خروجی	
2^{-65}	احتمال کل مشخصه	

دوری، فقط یک جواب بهینه به دست می آید، که برای حصول آن بیش از ۲۰۰۰ بار بهنگام سازی شبکه عصبی لازم است.

جدول ۸ کارایی و کارآمدی شبکه هاپفیلد در تعیین

مشخصه های تفاضلی در الگوریتم رمز سرپنت

شماره جدول	تعداد تکرار بهنگام سازی تا رسیدن به همگرایی	تعداد دفعات همگرایی به جواب مطلوب
۲	۴	۱۰۰
۳	۳۶	۱۰۰
۴	۳۷	۱۰۰
۵	۵	۲۰
۶	۹۲۲	۱۸
۷	۶	۲۰۲۵

۵- بهینه سازی با ماشین بولتزمن

برای رفع مشکل شبکه هاپفیلد و فرار از بهینه های محلی راه حل های متعددی ارائه شده که به دو دسته کلی راه حل های قطعی^۱ و اتفاقی^۲ تقسیم بندی می شوند. چند راه حل اتفاقی در ماشین بولتزمن^۳ [۴۵،۲۱]، شبکه های آشوبی^۴ [۴۷،۴۶] و ماشین گاوس^۵ [۴۸] دیده می شود. در این بخش از ماشین بولتزمن استفاده شده که در آن از ایده تابکاری شبیه سازی شده^۶ در آموزش شبکه هاپفیلد استفاده می شود. این شبکه برای حل مسائل متنوع بهینه سازی از جمله [۴۹،۵۲-۱۱] به کار برده شده است.

۵-۱- الگوریتم آموزش ماشین بولتزمن

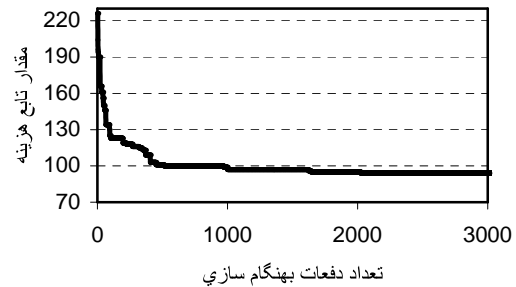
برای یافتن جواب بهینه برای تابع هزینه فوق از بهینه سازی با ماشین بولتزمن بر طبق الگوریتم زیر استفاده شد:

$$T = T_0 \quad ۱. \text{ مقداردهی اولیه دمای بهینه سازی}$$

جدول ۷ مشخصه تفاضلی شش دوری از الگوریتم رمز

سرپنت به دست آمده با شبکه هاپفیلد

شماره دور	تفاضل ورودی و خروجی توابع جانشینی در مشخصه یک دوری	احتمال
۱	ورودی	0C800900A0DD0D00DE04000000000E
	خروجی	01e0040040222040028060000000008
۲	ورودی	0400E000460A000500000000000400A0
	خروجی	0a004000a204000800000000000a0040
۳	ورودی	00000400A00000000000000000000000
	خروجی	00000a004000000000000000000000000
۴	ورودی	000000000000000400000000000000000
	خروجی	000000000000000030000000000000000
۵	ورودی	02000000010000200400000000001100
	خروجی	0A000000030000A00500000000006A00
۶	ورودی	60070000200400000101008060052015
	خروجی	10020000F00F00000E0E00B01003F0E3
۲-۹۴	احتمال کل مشخصه	



شکل ۸ تغییرات مقدار تابع هزینه در روند بهینه سازی در

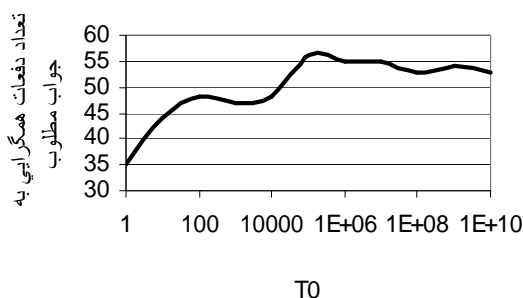
مشخصه تفاضلی جدول ۷ تا رسیدن به همگرایی

جدول ۸ میزان کارایی یعنی کمترین تعداد تکرار

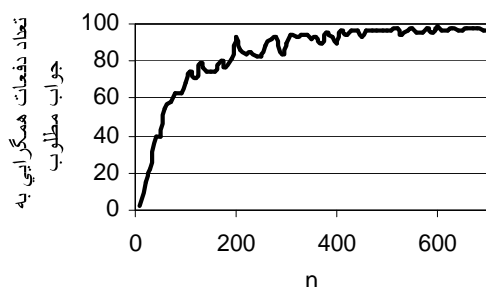
بهنگام سازی شبکه هاپفیلد تا رسیدن به همگرایی در هر یک از موارد بررسی شده و نیز میزان کارآمدی یعنی تعداد دفعات همگرا شدن به جواب مطلوب از میان ۱۰۰ تکرار روند بهینه سازی در هر مورد را نشان می دهد. چنانچه ملاحظه می شود، کارایی و کارآمدی شبکه در یافتن مشخصه های ۴ دوری الگوریتم رمز سرپنت بسیار بالا است، به طوری که با کمتر از ۴۰ بار بهنگام سازی، شبکه جواب بهینه به دست می آید و از طرفی در هیچ یک از ۱۰۰ تکرار، روند بهینه سازی در بهینه محلی جا نمانده است. اما با افزایش تعداد دور مشخصه، کارایی و کارآمدی شبکه هاپفیلد کاهش می یابد، به طوری که در تعیین مشخصه ۶

1- Deterministic
2- Stochastic
3- Boltzmann Machine
4- Cauchy
5- Gaussian Machine
6- Simulated Annealing

انتخابی برای پارامترها، روند بهینه‌سازی یکصد بار برای یافتن مشخصه ۵ دوری تکرار شده و تعداد دفعاتی که جواب مطلوب به دست آمده، شمارش شده است. نمودار تأثیر تغییر هریک از پارامترها، براساس نتایج حاصل از بررسیهای انجام شده، در شکل‌های ۹ تا ۱۲ آورده شده است. این بررسی نشان می‌دهد که بهترین مقدار برای پارامترهای T_0 ، n ، d و k به ترتیب مقادیر ۱۰۰۰۰۰، ۵۰۰، ۰/۹۴ و ۰/۱۰ است.



شکل ۹ نمودار تغییرات تعداد دفعات همگرایی شبکه عصبی به جواب مطلوب در اثر تغییر پارامتر T_0



شکل ۱۰ نمودار تغییرات تعداد دفعات همگرایی شبکه عصبی به جواب مطلوب در اثر تغییر پارامتر n

۳-۵- مشخصه‌های تفاضلی به دست آمده برای

الگوریتم رمز سرپنت با شبکه بولتزمن

الگوریتم بهینه‌سازی تشریح شده در بخش قبل به منظور یافتن مشخصه‌های ۴، ۵ و ۶ دوری از الگوریتم رمز سرپنت به کار برده شد.

۲. مقداردهی اولیه نوروها : مقدار نوروهای متناظر با تفاضل دور میانی توسط تحلیلگر تعیین و مقدار سایر نوروها با توجه به حالات ممکن در گراف نمایش عملکرد تفاضلی الگوریتم رمز سرپنت به طور دلخواه مشخص می‌شود.

۳. تکرار گامهای ۴ تا ۷ برای n مرتبه

۴. انتخاب یک نورو دلخواه و تغییر مقدار آن.

۵. تنظیم سایر نوروها براساس تغییر جدید: این تنظیم با توجه به رابطه تبدیل خطی بین نوروهای متناظر با خروجی توابع جانشینی در یک دور و نوروهای متناظر با ورودی توابع جانشینی در دور بعد انجام می‌شود.

۶. محاسبه مقدار تابع هزینه با توجه به تغییر انجام شده.

۷. پذیرش وضعیت جدید، در صورتی که رابطه

$$Pr < \frac{1}{1 + \exp\left(-\frac{\Delta E}{T}\right)}$$

برقرار باشد، که ΔE میزان

تغییر مقدار تابع هزینه در صورت پذیرش مقدار جدید و Pr عددی در فاصله صفر و یک است، که به طور تصادفی تولید می‌شود.

۸. تغییر دمای بهینه‌سازی با ضریب d : $T = d \times T$

۹. بررسی شرط توقف و تکرار از گام ۳ در صورت عدم

برقراری آن. شرط توقف عبارت است از اینکه در سه

دمای متوالی روند بهینه‌سازی، نسبت دفعات پذیرش

تغییر مقدار نوروها به کل دفعات بهنگام سازی

شبکه در یک دما کمتر از k باشد.

۲-۵- بررسی پارامترها

در شبکه فوق پارامترهای T_0 ، n ، d و k پارامترهای کنترلی بهینه‌سازی هستند که باید به نحو مطلوبی تعیین شوند. در ادامه، ابتدا به ترتیب مقادیر ۱۰۰۰، ۱۰۰، ۰/۹ و ۰/۱۵ را برای این پارامترها در نظر گرفته و سپس با بررسی مقادیر مختلف برای هر یک از آنها، مقدار مطلوب برای آن پارامتر تعیین می‌شود. متناظر با هر دسته از مقادیر

جدول ۹ مشخصه تفاضلی چهار دوری از الگوریتم رمز سرپنت به دست آمده با ماشین بولتزمن (تابع جانشینی چهارم از دور سوم فعال است)

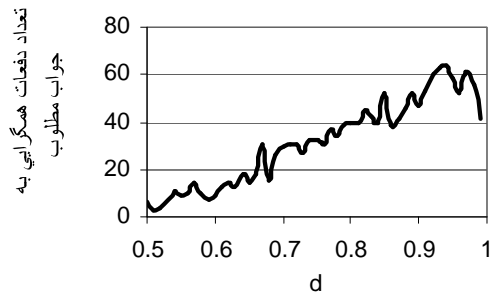
شماره دور	تفاضل ورودی و خروجی توابع جانشینی در مشخصه یک دوری	احتمال
۱	ورودی	00D0000000000000C6008009000000000
	خروجی	00200000000000001A00E0040000000000
۲	ورودی	00000000000000000000000000400500
	خروجی	00000000000000000000000000A00400
۳	ورودی	00004000000000000000000000000000
	خروجی	0000A000000000000000000000000000
۴	ورودی	000200040000000000000000010000810
	خروجی	000600030000000000000000070000C70
۲-۲۹	احتمال کل مشخصه	

جدول ۱۰ مشخصه تفاضلی چهار دوری از الگوریتم رمز سرپنت به دست آمده با ماشین بولتزمن (تابع جانشینی دوم از دور سوم فعال است)

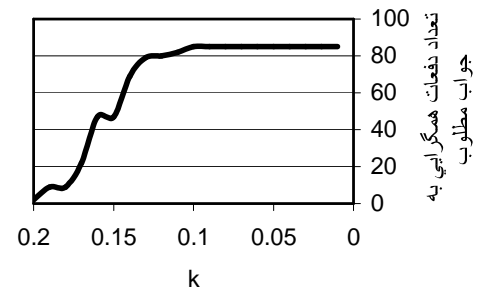
شماره دور	تفاضل ورودی/خروجی توابع جانشینی در مشخصه یک دوری	احتمال
۱	ورودی	D0000000000000F900700E00000000000
	خروجی	20000000000001A00E00400000000000
۲	ورودی	00000000000000000000000040050000
	خروجی	000000000000000000000000A0040000
۳	ورودی	00400000000000000000000000000000
	خروجی	00A00000000000000000000000000000
۴	ورودی	020004000000000000000001000081000
	خروجی	0600030000000000000000070000C7000
۲-۲۹	احتمال کل مشخصه	

مشخصه‌های ۵ دوری به دست آمده با ماشین بولتزمن مطابق جداول ۱۲ و ۱۳ و به ترتیب دارای احتمال 2^{-60} و 2^{-65} است. روند تغییرات مقدار تابع هزینه تا رسیدن به همگرایی در هر یک از این دو مشخصه به ترتیب در شکل‌های ۱۶ و ۱۷ آورده شده است. در دو مورد فوق، از میان ۱۰۰ بار تکرار بهینه‌سازی به ترتیب ۴۳ و ۹۹ مرتبه، جواب مطلوب به دست آمده است.

مشخصه ۶ دوری به دست آمده با ماشین بولتزمن مطابق جدول ۱۴ است، که احتمال 2^{-94} دارد. روند تغییرات مقدار تابع هزینه تا رسیدن به همگرایی در مشخصه فوق در شکل ۱۸ آورده شده است. از میان ۱۰۰ تکرار بهینه‌سازی برای یافتن مشخصه فوق، ۳۰ مرتبه جواب



شکل ۱۱ نمودار تغییرات تعداد دفعات همگرایی شبکه عصبی به جواب مطلوب در اثر تغییر پارامتر d

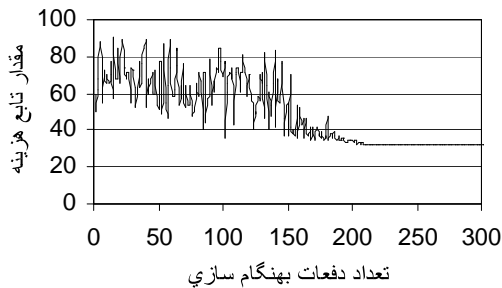


شکل ۱۲ نمودار تغییرات تعداد دفعات همگرایی شبکه عصبی به جواب مطلوب در اثر تغییر پارامتر k

برای یافتن بهترین جواب، الگوریتم بهینه‌سازی ۱۰۰ مرتبه برای هر یک از موارد مورد بررسی تکرار و بهترین جواب انتخاب شد. به هدف امکانپذیری مقایسه کارایی ماشین بولتزمن با شبکه هاپفیلد، مقدار تفاضل ورودی دور میانی و شماره و مقدار تابع جانشینی فعال در این دور- مانند آنچه در بخش ۴-۲ ذکر شد- بر اساس آنچه در تحلیل‌های تفاضلی منتشر شده از الگوریتم رمز سرپنت در [۴۲-۴۴] است، تعیین شد.

سه مشخصه ۴ دوری به دست آمده با ماشین بولتزمن مطابق جداول ۹، ۱۰ و ۱۱ و به ترتیب دارای احتمال 2^{-29} ، 2^{-29} و 2^{-32} است. روند تغییرات مقدار تابع هزینه تا رسیدن به همگرایی در هر یک از موارد فوق به ترتیب در شکل‌های ۱۳، ۱۴ و ۱۵ آورده شده است. در هر یک از سه مورد فوق، تمامی ۱۰۰ بار تکرار بهینه‌سازی جواب مطلوب به دست آمده و در هیچ یک از تکرارها در بهینه محلی جا نمانده است.

مطلوب به دست آمده است.



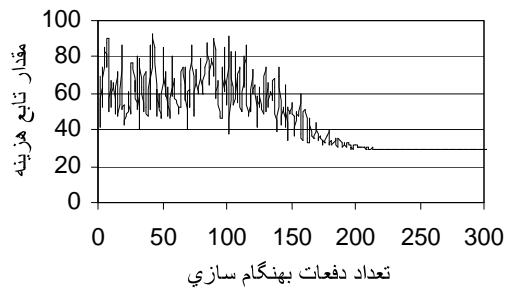
جدول ۱۱ مشخصه تفاضلی چهار دوری از الگوریتم رمز سرپنت به دست آمده با ماشین بولتزمن (تابع جانشینی ششم از دور هشتم فعال است)

شماره دور	تفاضل ورودی/خروجی توابع جانشینی در مشخصه یک دوری	احتمال
۶	ورودی	0400A0000000006006000D0060000000
	خروجی	0A0020000000001001000A0040000000
۷	ورودی	0000000000000000000000000001005
	خروجی	000000000000000000000000000A004
۸	ورودی	0000040000000000000000000000000
	خروجی	000000A000000000000000000000000
۹	ورودی	1000200040000000000000000100008
	خروجی	300003000700000000000000030000E
۳-۳۲	احتمال کل مشخصه	

شکل ۱۵ تغییرات مقدار تابع هزینه در روند بهینه سازی در مشخصه تفاضلی جدول ۱۱ تا رسیدن به همگرایی

جدول ۱۲ مشخصه تفاضلی دوره‌های پنجم تا نهم از الگوریتم رمز سرپنت به دست آمده با ماشین بولتزمن

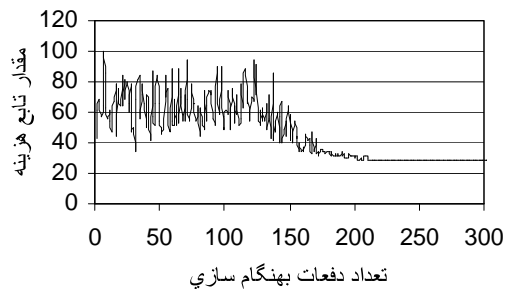
شماره دور	تفاضل ورودی و خروجی توابع جانشینی در مشخصه یک دوری	احتمال
۵	ورودی	00000704009000000800C00600C901B3
	خروجی	0000030B005000000C00400200450618
۶	ورودی	0400E000000000C00C00010090000000
	خروجی	0A002000000001001000A0040000000
۷	ورودی	0000000000000000000000000001005
	خروجی	000000000000000000000000000A004
۸	ورودی	0000040000000000000000000000000
	خروجی	000000A000000000000000000000000
۹	ورودی	1000200040000000000000000100008
	خروجی	900005000700000000000000030000E
۳-۶۰	احتمال کل مشخصه	



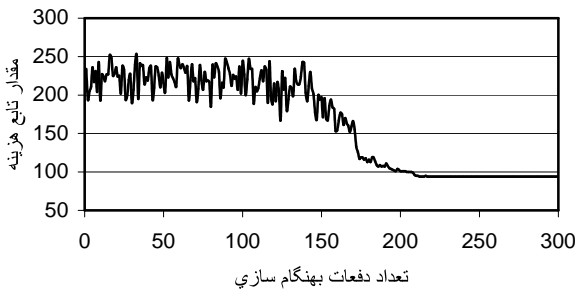
جدول ۱۳ مشخصه تفاضلی دوره‌های اول تا پنجم از الگوریتم رمز سرپنت به دست آمده با ماشین بولتزمن

شکل ۱۳ تغییرات مقدار تابع هزینه در روند بهینه سازی در مشخصه تفاضلی جدول ۹ تا رسیدن به همگرایی

شماره دور	تفاضل ورودی و خروجی توابع جانشینی در مشخصه یک دوری	احتمال
۱	ورودی	D000000000000FA00F00A0000000000
	خروجی	20000000000001a00e0040000000000
۲	ورودی	00000000000000000000000040050000
	خروجی	000000000000000000000000a0040000
۳	ورودی	0040000000000000000000000000000
	خروجی	00A0000000000000000000000000000
۴	ورودی	020004000000000000000001000081000
	خروجی	0300030000000000000000A0000CB000
۵	ورودی	30402900008010bc0c03ca5004070005
	خروجی	80B0E50000C060B4040841E00908000F
۳-۶۵	احتمال کل مشخصه	



شکل ۱۴ تغییرات مقدار تابع هزینه در روند بهینه سازی در مشخصه تفاضلی جدول ۱۰ تا رسیدن به همگرایی



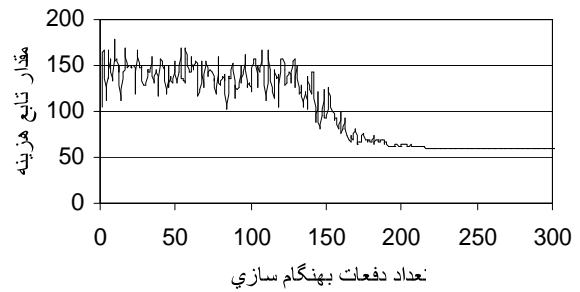
شکل ۱۸ تغییرات مقدار تابع هزینه در روند بهینه‌سازی در مشخصه تفاضلی جدول ۱۴ تا رسیدن به همگرایی

این مشخصه مطابق جدول ۱۵ بوده و احتمال رخداد آن برابر 2^{-125} است. روند تغییرات مقدار تابع هزینه تا رسیدن به همگرایی در مشخصه فوق در شکل ۱۹ آورده شده است.

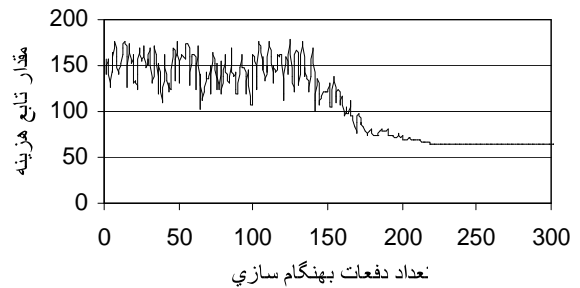
جدول ۱۵ مشخصه تفاضلی هفت دوری از الگوریتم رمز سرپنت به دست آمده با ماشین بولتزن

شماره دور	تفاضل ورودی و خروجی توابع جانشینی در مشخصه یک دوری	احتمال
۱	ورودی	0C30090090DD0900DE040000000000E
	خروجی	01e00400402220400280600000000008
۲	ورودی	0400B000460A000500000000000400A0
	خروجی	0a004000a2040008000000000000a0040
۳	ورودی	00000400A00000000000000000000000
	خروجی	00000a00400000000000000000000000
۴	ورودی	00000000000000400000000000000000
	خروجی	00000000000000300000000000000000
۵	ورودی	020000000100002004000000000001100
	خروجی	0A000000030000B005000000000006A00
۶	ورودی	40070000200400000101008060043015
	خروجی	A0040000B0030000A0A00C0100A8074
۷	ورودی	0000055A009000090C00C10005260000
	خروجی	00000448005000050E00E30004C20000
2^{-125}	احتمال کل مشخصه	

جدول ۱۶ میزان کارایی و کارآمدی روند بهینه‌سازی با ماشین بولتزن را نشان می‌دهد. در تمام موارد با کمتر از ۳۰۰ تکرار در روند بهینه‌سازی، همگرایی حاصل می‌شود.



شکل ۱۶ تغییرات مقدار تابع هزینه در روند بهینه‌سازی در مشخصه تفاضلی جدول ۱۲ تا رسیدن به همگرایی



شکل ۱۷ تغییرات مقدار تابع هزینه در روند بهینه‌سازی در مشخصه تفاضلی جدول ۱۳ تا رسیدن به همگرایی

علاوه بر مشخصه‌های فوق یک مشخصه ۷ دوری با به‌کارگیری ماشین بولتزن برای الگوریتم رمز سرپنت به دست آمده است.

جدول ۱۴ مشخصه تفاضلی شش دوری از الگوریتم رمز سرپنت به دست آمده با ماشین بولتزن

شماره دور	تفاضل ورودی و خروجی توابع جانشینی در مشخصه یک دوری	احتمال
۱	ورودی	0C30090090DD0900DE040000000000E
	خروجی	01e00400402220400280600000000008
۲	ورودی	0400B000460A000500000000000400A0
	خروجی	0a004000a2040008000000000000a0040
۳	ورودی	00000400A00000000000000000000000
	خروجی	00000a00400000000000000000000000
۴	ورودی	00000000000000400000000000000000
	خروجی	00000000000000300000000000000000
۵	ورودی	020000000100002004000000000001100
	خروجی	0A000000030000A005000000000006A00
۶	ورودی	60070000200400000101008060052015
	خروجی	10020000700A00000E0E00B0900370E3
2^{-94}	احتمال کل مشخصه	

ماشین بولتزن برای یافتن بهترین مسیر چند-شعبه در گراف نمایش عملکرد تفاضلی ارائه و ثابا با اعمال آن بر روی الگوریتم رمز قطعه‌ای سرپنت به‌عنوان رمز نمونه، کارایی و کارآمدی آنها بررسی شد.

جدول ۱۷ کارایی و کارآمدی روند بهینه‌سازی توسط شبکه هاپفیلد و ماشین بولتزن را در هر یک از موارد بررسی شده نشان می‌دهد. با توجه به اینکه اعداد گزارش شده در جدول ۱۶، تعداد تکرار بدنه اصلی روند بهینه‌سازی ماشین بولتزن تا رسیدن به همگرایی (تعداد دفعات تغییر دما) است، برای آنکه میزان کارایی در دو شبکه قابل مقایسه باشد، باید اعداد گزارش شده در جدول ۱۶ در تعداد دفعات بهنگام‌سازی در هر دما (۵۰۰) ضرب شود. چنانچه ملاحظه می‌شود استفاده از ایده تابه‌کاری شبیه‌سازی شده، باعث افزایش کارآمدی شبکه عصبی می‌شود، اما کارایی در ماشین بولتزن کاهش می‌یابد، به‌بیان دیگر پیچیدگی اجرای روند بهینه‌سازی با ماشین بولتزن بیشتر از هاپفیلد است.

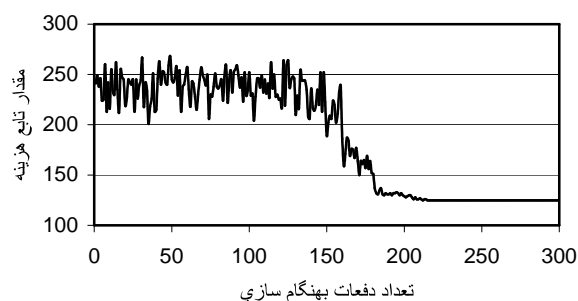
جدول ۱۷ مقایسه کارایی و کارآمدی شبکه هاپفیلد و ماشین

بولتزن در تعیین مشخصه‌های تفاضلی در الگوریتم رمز

سرپنت

تعداد دور مشخصه	تعداد تکرار بهنگام‌سازی تا رسیدن به همگرایی		تعداد دفعات همگرایی به جواب مطلوب	
	شبکه هاپفیلد	ماشین بولتزن	شبکه هاپفیلد	ماشین بولتزن
۴	۲۸	۱۰۸۵۰۰	۱۰۰	۱۰۰
	۳۶	۱۰۶۵۰۰	۱۰۰	۱۰۰
	۳۷	۱۰۴۵۰۰	۱۰۰	۱۰۰
۵	۴۰۸	۱۰۸۰۰۰	۲۰	۴۳
	۹۲۲	۱۰۹۰۰۰	۱۸	۹۹
۶	۲۰۲۵	۱۰۸۵۰۰	۱	۳۰
۷	---	۱۰۷۵۰۰	---	۲۴

از طرفی در جدول ۱۸ مشخصه‌های به‌دست آمده با شیوه پیشنهادی در این مقاله با مشخصه‌های گزارش شده در مقالات دیگر، از نظر احتمال رخداد آنها مقایسه شده



شکل ۱۹ تغییرات مقدار تابع هزینه در روند بهینه‌سازی در مشخصه تفاضلی جدول ۱۵ تا رسیدن به همگرایی

چنانچه ملاحظه می‌شود علی‌رغم افزایش کارآمدی روند بهینه‌سازی با به‌کارگیری ماشین بولتزن نسبت به به‌کارگیری شبکه هاپفیلد، بازم با افزایش تعداد دور مشخصه، کارایی شبکه عصبی کاهش می‌یابد.

جدول ۱۶ کارایی و کارآمدی ماشین بولتزن در تعیین

مشخصه‌های تفاضلی در الگوریتم رمز سرپنت

شماره جدول	تعداد دور	تعداد تکرار بهنگام‌سازی تا رسیدن به همگرایی	تعداد دفعات همگرایی به جواب مطلوب
۹	۴	۲۱۷	۱۰۰
۱۰		۲۱۳	۱۰۰
۱۱		۲۰۹	۱۰۰
۱۲	۵	۲۱۶	۴۳
۱۳		۲۱۸	۹۹
۱۴	۶	۲۱۷	۳۰
۱۵	۷	۲۱۵	۲۴

۶- جمع‌بندی و پیشنهادها

در این تحقیق برای یافتن مشخصه تفاضلی با حداقل احتمال در الگوریتم رمز قطعه‌ای، گراف نمایش عملکرد تفاضلی الگوریتم رمز قطعه‌ای به‌کار رفت. با این نمایش، یافتن مشخصه تفاضلی با حداقل احتمال، معادل با یافتن کم‌وزن‌ترین مسیر چند-شعبه بین دو گره آغازی و پایانی در گراف حاصل است. همانطور که ملاحظه شد در طی این مقاله به دو سؤال مطرح شده در ابتدای مقاله پاسخ داده شد. اولاً نحوه به‌کارگیری شبکه‌های عصبی هاپفیلد و

۳- می‌توان شیوه‌های مختلف بهینه‌سازی هوشمند مانند الگوریتم‌های ژنتیک، اجتماع مورچگان، شبکه‌های عصبی و مانند آن را در یافتن مسیر چند-شعبه مناسب در گراف نمایش عملکرد تفاضلی الگوریتم رمز قطعه‌ای به کار برد و عملکرد آنها را از نظر کارایی و کارامدی مقایسه کرد.

۷- منابع

[۱] ع.قائمی بافقی، ب.صادقیان، "یک مدل بازنمایی عملکرد تفاضلی الگوریتم‌های رمز قطعه‌ای با ساختار جانشینی- جایگشتی"، نشریه علمی امیرکبیر، شماره آ-۵۸، ۱۳۸۳.

[۲] ع.قائمی بافقی، "تحلیل تفاضلی الگوریتم رمز قطعه‌ای سرپنت"، هفتمین کنفرانس سالانه انجمن کامپیوتر ایران، ۱۳۸۰.

[3] E.Biham and A.Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", *Advances in Cryptology-CRYPTO '90*, pp. 2-21, 1990

[4] A.Ghaemi Bafghi, B.Sadeghiyan, "Differential Model of Block Ciphers with Ant Colony Technique", *IST2003-2nd Biannual International Symposium on Telecommunication*, Iran, 2003.

[5] A.Ghaemi Bafghi, B. Sadeghiyan, "Finding Suitable Differential Characteristics for Block Ciphers with Ant Colony Technique", *9th IEEE Symposium on Computers and Communications*, 2004.

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

[7] K. Urahama and H. Nishiyuki, "Neural Algorithms for Placement Problems", *International Joint Conference on Neural Networks 3*, Nagoya, 2421-2424, 1993.

است. این مقایسه نشان می‌دهد که در شش مورد، نتایج ارائه شده در این مقاله بهتر از نتایج گزارش شده در سایر مقالات است و در دو مورد، احتمال مشخصه تفاضلی به دست آمده برابر با احتمال مشخصه‌های نظیر در مقالات دیگر است. همچنین با صرف نظر از مشخصه‌های بومرنگ گزارش شده از الگوریتم رمز سرپنت، مشخصه تفاضلی ۷ دوری با احتمال 2^{-125} به دست آمده در این مقاله، اولین مشخصه تفاضلی برای بیش از ۶ دور از این الگوریتم رمز است. نتایج به دست آمده در این مقاله در مقایسه با مشخصه‌های منتشر شده در مقالات دیگر، نشان دهنده کارایی شیوه پیشنهادی در این مقاله برای یافتن مشخصه تفاضلی مناسب است.

جدول ۱۸ مقایسه مشخصه‌های تفاضلی به دست آمده از الگوریتم رمز

سرپنت در این مقاله و دیگر مقالات منتشر شده

تعداد دور مشخصه	احتمال مشخصه به دست آمده در مقاله‌های دیگر	احتمال مشخصه به دست آمده در این مقاله
۴	2^{-31} [۴۳]	2^{-29}
	2^{-24} [۴۴]	2^{-22}
	2^{-29} [۴۲]	2^{-29}
۵	2^{-80} [۴۳], 2^{-67} [۴۴]	2^{-65}
	2^{-61} [۴۴], 2^{-60} [۴۲]	2^{-60}
۶	2^{-97} [۴۴]	2^{-94}
۷	---	2^{-125}

پژوهش گزارش شده در این مقاله را از جنبه‌های مختلفی می‌توان ادامه داد که در زیر چند نمونه ذکر می‌شود:

- ۱- در این تحقیق مقادیر مناسب برای پارامترهای شبکه عصبی با انجام آزمایش‌های مختلف تعیین شده است. با توسعه شبکه عصبی می‌توان بهترین مقادیر این پارامترها را در طی روند بهینه‌سازی به دست آورد.
- ۲- شیوه این تحقیق را برای یافتن مشخصه‌های مطلوب برای الگوریتم‌های رمز قطعه‌ای دیگر به کار برد.

- Convergence to Valid Solutions”, *Proceedings International Conference on Neural Networks 7*, 1994.
- [17] N. Fynabiki and Y. Takefuji, “A Neural Network Parallel Algorithm for Channel Assignment Problems in Cellular Radio Networks”, *IEEE Transactions on Vehicular Technology 41*, 430-437, 1992.
- [18] Y. Takifuji and K. C. Lee, “Artificial Neural Networks for Four-Coloring Map Problems and K-Colorability Problems”, *IEEE Transactions on Circuits and Systems 38*, 326–333, 1991.
- [19] K. Smith and M. Palaniswami, “Static and Dynamic Channel Assignment Using Neural Networks”, *IEEE Journal on Selected Areas in Communications 15*, 238–249, 1997.
- [20] D. D. Caviglia, G. M. Bisio, F. Curatelli, L. Giovannacci and L. Raffo, “Neural Algorithms for Cell Placement inVLSI Design”, *IEEE International Joint Conference on Neural Networks 1*, 573–580, 1989.
- [21] F. Arajo, B. Ribeiro, L. Rodrigues, “A Neural Network for Shortest Path Computation”, *IEEE Transactions on Neural Networks*, 12(5) ,2001.
- [22] S. G. Hong, S. W. Kim, and J. J. Lee, “The Minimum Cost Path Finding Algorithm Using a Hopfield Type Neural Network”, *Proceedings IEEE International Conference on Fuzzy Systems 4*, 1719–1726, 1995.
- [23] T. Haines, H. V. Medanic, “A neural Network Shortest Path Algorithm”, *IEEE International Symposium on Intelligent Control*, 1994.
- [24] J. Wang, “A Recurrent Neural Network for Solving the Shortest Path Problem”, *IEEE International Symposium Circuits and Systems 6*, 319–322, 1994.
- [8] H. Date, M. Seki, and T. Hayashi, “LSI Module Placement Using Neural Computation Networks”, *International Joint Conference on Neural Networks 3*, San Diego, 831–836, 1990.
- [9] G. A. Tagllaribi and E. W. Page, “Solving Constraint Satisfaction Problems with Neural Networks”, *IEEE International Conference on Neural Networks 3*, 741–747, 1987.
- [10] B. Kamgar-Parsi, J. A. Gualtieri, and J. E. Devaney, “Clustering with Neural Networks”, *Biological Cybernetics 63*, 201–208, 1990.
- [11] G. P. Babu and M. N. Murty, “Connectionist Approach for Clustering”, *International Conference on Neural Networks 7*, 4661–4666, 1994.
- [12] S. K. Chen, P. Mangimeli, and D. West, “The Comparative Ability of Self-Organizing Neural Networks to Define Cluster Structure”, *Omega 23*, 271–279, 1995.
- [13] A. Barami and C. Dagli, “Hybrid Intelligent Packing System (HIPS) Through Integration of Artificial Neural Networks”, *Artificial Intelligence and Mathematical Programming, Applied Intelligence 4*, 321–336.
- [14] Dai, J. Cha, W. Guo, and F. Wang, “A Heuristic-Based Neural Network for Packing Problems”, *International Conference on Data and Knowledge Systems for Manufacturing and Engineering 2*, 698–703, 1994.
- [15] T. Hameenanttila and J. D. Carothers, “A Hopfield Neural Network Solution to the TCM Partitioning Problem”, *IEEE International Conference on Neural Networks 7*, 4676–4680, 1994.
- [16] M. O. Berger, “k-Coloring Vertices Using a Neural Network with

- [33] J.Hopfield and D.W.Tank, "Neural: Computation of Decisions in Optimization Problems", *Biological Cybernetics* 52, 141–152, 1985.
- [34] Y. B. Cho, T. Kurokawa, Y. Takefuji, and H. S. Kim, "An O(1) Approximate Parallel Algorithm for the n-Task n-Person Assignment Problem", *International Joint Conference on Neural Networks* 2, Nagoya, 1503–1506, 1993.
- [35] D. Gong, M. Gen, G. Yamazaki, and W. Xu, "Neural Network Approach for General Assignment Problem", *International Conference on Neural Networks* 4, Perth, 1861–1866, 1995.
- [36] T. Kurokawa and S. Kozuka, "Use of Neural Networks for the Optimum Frequency Assignment Problem", *Electronics and Communications in Japan*, Part 1, 77, 106–116, 1994.
- [37] Y. Lin, L. M. Austin, and J. R. Burns, "An Intelligent Algorithm for Mixed-Integer Programming Models", *Computers and Operations Research* 19, 461–468, 1992.
- [38] C. Pornavalai, G. Chakraborty, and N. Shiratori, "Neural Networks for Solving Constrained Steiner Tree Problem", *IEEE International Conference on Neural Networks* 4, 1867–1870, 1995.
- [39] J. Ramanujam and P. Sadayappan, "Mapping Combinatorial Optimization Problems onto Neural Networks", *Information Sciences* 82, 239–255, 1995.
- [40] E. Wacholder, J. Han, and R. C. Mann, "An Extension of the Hopfield-Tank Model for Solution of the Multiple TSP", *IEEE International Conference on Neural Networks* 2, 305–325, 1991.
- [41] A. Yamamoto, M. Ohta, H. Ueda, A. Ogihara, and K. Fukunaga, "Asymmetric Neural Network and its Application to
- [25] Y. Xia, J. Wang, "A Discrete-Time Recurrent Neural Network for Shortest-Path Routing", *IEEE Transactions on Automatic Control*, 45(11), 2000.
- [26] F. Zhang, X. Yin, "A Simulated Annealing Neural Network and Lanczos Inverse Approach for Impedance Inversion", University of Petroleum, China, 1998 SEG Expanded Abstracts
- [27] L.I. Burke, "Adaptive Neural Networks for the Traveling Salesman Problem: Insights from Operations Research", *Neural Networks* 7, 681–690, 1994.
- [28] R. D. Brandt, Y. Wang, A. J. Laub, and S. K. Mitra, "Alternative Networks for Solving the Travelling Salesman Problem and the List-Matching Problem", *International Conference on Neural Networks* 2, 333–340, 1988.
- [29] A.H.Gee and R. W. Prager, "Limitations of Neural Networks for Solving Traveling Salesman Problems", *IEEE Transactions on Neural Networks* 6, 280–282, 1995.
- [30] W. Lin, J. G. Delgado-Frias, G. G. Pechanek, and S. Vassilladis, "Impact of Energy Function on a Neural Network Model for Optimization Problems", *Proceedings IEEE International Conference on Neural Networks* 7, 4518–4523, 1994.
- [31] R. Van Vliet and H. Cardon, "Combining a Graph Partitioning and a TSP Neural Network to Solve the MTSP", in *Artificial Neural Networks* 2, T. Kohonen, K. Makisara, O. Simula, and J. Kangas (eds.), North Holland, Amsterdam, 157–162, 1991.
- [32] J.Hopfield, "Neural Networks and Physical Systems with Emergent Collective Computational Abilities", *Proceedings of National Academy of Sciences* 79, 2554–2558, 1982.

- Optimization with Gaussian Machines”, *IEEE International Joint Conference on Neural Networks 1*, 533–540, 1989.
- [49] T. Bultan and C. Aykanat, “Circuit Partitioning Using Parallel Mean Field Annealing Algorithms”, *3rd IEEE Symposium on Parallel and Distributed Processing*, 534–541, 1991.
- [50] M. K. Unaltuna and V. Pitchumani, “Unsupervised Competitive Learning Neural Network Algorithms for Circuit Bipartitioning”, *World Congress on Neural Networks 1*, San Diego, 302–307, 1994.
- [51] S. Vaithyanathan, H. Ogmen, and J. Ignizio, “Generalized Boltzmann Machines for Multidimensional Knapsack Problems”, *Intelligent Engineering Systems Through Artificial Neural Networks 4*, ASME Press, New York, 1079–1084, 1994.
- [52] V. Zissimopoulos, V. Paschos, and F. Pekergin, “On the Approximation of NP-Complete Problems by Using the Boltzmann Machine Method: The Case of Some Covering and Packing Problems”, *IEEE Transactions on Computers 40*, 1413–1418, 1991.
- Knapsack Problem”, *IEICE Transactions Fundamentals E78-A*, 300–305, 1995.
- [42] E. Biham, O. Dunkelman, and N. Keller, “The Rectangle Attack-Rectangling the Serpent”, *Lecture Notes in Computer Science*, 2001.
- [43] T. Kohono, J. Kelsey, and B. Schneier, “Preliminary Cryptanalysis of Reduced-Round Serpent”, *Third AES Candidate Conference*, 2000.
- [44] X. Y. Wang, and et.al. “The Differential Cryptanalysis of an AES Finalist-Serpent”, Technical Report TR-2000-04, 2000.
- [45] D. H. Ackley, G. E. Hinton, and T. J. Sejnowski, “A Learning Algorithm for Boltzmann Machines”, *Cognitive Science 9*, 147–169, 1985.
- [46] H. Jeong and J. H. Park, “Lower Bounds of Annealing Schedule for Boltzmann and Cauchy Machines”, *IEEE International Joint Conference on Neural Networks 1*, 581–586, 1989.
- [47] Y. Takefuji and H. Szu, “Design of Parallel Distributed Cauchy Machines”, *IEEE International Joint Conference on Neural Networks 1*, 529–532, 1989.
- [48] Y. Akiyama, A. Yamashita, M. Kajiura, and H. Aiso, “Combinatorial