مجله علمی پژوهشی «علوم و فناوری‌های پدافند نوین»
سال هشتم، شماره ۳، پاییز ۱۳۹۶؛ ص ۱۸۹-۱۸۱

تعمیم سازوکار سوییچینگ لایه انتشار برای طراحی رمزهای قالبی ۲۵۶ بیتی

عبدالرسول میرقدری[1*]، محمود یوسفی‌پور[2]، بهروز خادم[3]
۱- دانشیار، ۲- دانشجوی دکتری، ۳- استادیار، دانشگاه جامع امام حسین (ع)
(دریافت: ۹۵/۰۵/۱۶، پذیرش: ۹۵/۰۹/۳۰)

چکیده

یکی از روش‌های مهم برای بررسی مقاومت یک رمز قالبی در برابر تحلیل‌های اساسی مانند تحلیل تفاضلی و تحلیل خطی، تعیین حداقل تعداد جعبه‌های جانشینی فعال در طول روند تحلیل است. با توجه به این شاخص، می‌توان نسبت حداقل جعبه‌های جانشینی فعال به کل جعبه‌های جانشینی به‌کار رفته در رمز قالبی را به‌دست آورد. بیشتر بودن این نسبت بیانگر طراحی بهتر الگوریتم رمز قالبی است. در ساختارهای فیستلی به دلیل XOR کردن نیمه راست و چپ حالت، عمل حذف تفاضل‌ها رخ می‌دهد که این امر باعث کاهش نسبت ذکر شده می‌شود. پیش از این روشی برای کاهش حذف تفاضل‌ها در ساختارهای فیستلی و بهبود نسبت جعبه‌های جانشینی فعال به کل جعبه‌های جانشینی ارائه شده که در آن از ماتریس‌های MDS چندگانه استفاده شده است. اگرچه این روش برای طراحی رمزهای قالبی با طول قالب ۱۲۸ بیت مناسب است، ولی برای طراحی رمزهای قالبی با طول قالب بزرگ‌تر، مانند قالب ۲۵۶ بیتی، به طور نسبی پیچیده و دشوار است. در این مقاله، ابتدا مسئله پیدا کردن لایه‌های انتشار چندگانه مناسب برای ساختار سوییچینگ، با ابعاد بزرگ و روی میدان‌های بزرگ مورد مطالعه و بررسی قرار می‌گیرد. سپس یک الگوریتم جستجو ارائه شده است و با استفاده از آن چند دسته از لایه‌های انتشار بازگشتی چندگانه معرفی می‌شوند. در بخش دیگر این مقاله، از لایه‌های انتشار بازگشتی چندگانه استفاده شده است و یک ساختار برای طراحی رمزهای قالبی ۲۵۶ بیتی مبتنی بر ساختار سوییچینگ ارائه خواهد شد. با توجه به بررسی امنیت و کارایی ساختار پیشنهادی، می‌توان گفت که طرح‌های مبتنی بر این ساختار در برابر حمله‌های مهمی مانند حمله تفاضلی، حمله خطی و حمله تفاضلی ناممکن مقاوم بوده و در مقایسه با الگوریتم‌های ۲۵۶ بیتی موجود کارایی مناسبی دارند.

کلیدواژه‌ها: لایه‌های انتشار، تحلیل تفاضلی، تحلیل تفاضلی ناممکن، تحلیل خطی، سازوکار سوییچینگ

Extending the Switching Mechanism for 256 bit Block Ciphers Designing

A. Mirghadri*, M. YosefiPour, B. Khadem
Imam Hossein University
(Received: 06/08/2016; Accepted: 20/12/2016)

Abstract

One of the most important methods for checking the resistant of a block cipher against linear and differential analysis is counting of minimum active s-boxes. According to this number, proportion of minimum active s-boxes to all used s-boxes can be obtained. In Feistel structure, left and right half XORing cause difference cancelation reducing this proportion. One method for reducing difference cancelation and improving this proportion is presented previously using multiple MDS matrix. However, this method is suitable for design of 128 bit block ciphers and hasn't good efficiency in 256 bit block ciphers. In this paper, the problem of finding proper multiple diffusion layers for Switching Structure on big dimension and big field is firstly surveyed. Then, a search algorithm is presented, used for making several categories of Recursive Diffusion Layers. In the next section, by using this Recursive Diffusion Layers, a 256 bit block cipher is designed base on Switching Structure. We verify security and efficiency of this scheme is verified and it is concluded that this scheme is resistant to linear and differential attack showing impossible differential attack and also has a good efficiency compare to other 256 bit block cipher algorithm.

Keywords: Diffusion Layers, Linear Cryptanalysis, Differential Cryptanalysis, Impossible Differential Cryptanalysis, Switching Mechanism.

*Corresponding Author E-mail: amrghdri@ihu.ac.ir

۱. مقدمه

در طول دهه اخیر شاهد استقبال روزافزون جامعه رمزنگاری از رمزهای قالبی بوده‌اید. این امر در حدی است که در بسیاری از موارد رمزهای دنباله‌ای با رمزهای قالبی جایگزین شده‌اند. به عنوان مثال در نسل جدید تلفن همراه، رمزهای دنباله‌ای A5/1 [۱] و A5/2 [۲] با الگوریتم رمز قالبی Kasumi [۳] جایگزین شده‌اند. اگرچه الگوریتم‌های استاندارد رمزهای قالبی مانند AES، بسیاری از نیازها در حوزه کاربرد رمزهای قالبی را رفع می‌کنند ولی با این وجود هر سال شاهد ارائه الگوریتم‌های رمز قالبی جدید هستید. برای مثال الگوریتم‌هایی مانند LBlock [۴]، Prince [۵]، Midori [۶ و ۷] برخی رمزهای قالبی جدید هستند که در یک یا دو سال اخیر معرفی شده‌اند.

یک الگوریتم رمز قالبی، یک جایگشت مبتنی بر کلید است که متن آشکار را با استفاده از یک کلید محرمانه به متن رمزی تبدیل می‌کند. رمزهای قالبی به SPN[1]ها، ساختارهای فیستلی و ساختارهای ترکیبی تقسیم‌بندی می‌شوند [۸]. هر الگوریتم رمزنگاری، از جمله رمزهای قالبی از دو لحاظ امنیت و کارایی قابل بررسی است. منظور از کارایی یک الگوریتم رمز، سرعت محاسباتی و الزامات حافظه و منابع برای پیاده‌سازی آن است. همچنین امنیت یک الگوریتم رمز قالبی، به عنوان مقاومت آن در برابر حملات شناخته شده تعریف می‌شود. از حملات شناخته شده مهم روی رمزهای قالبی، می‌توان تحلیل‌های تفاضلی و خطی را نام برد.

تحلیل تفاضلی: تحلیل تفاضلی یک روش برای به‌دست آوردن بیت‌های کلید با استفاده از تفاضل‌های میان متن‌های آشکار و متن‌های رمزی حاصل از یک رمز قالبی است[۹]. در این تحلیل مهم‌ترین کار این است که بتوان تفاضل‌های ورودی را که با احتمال بالایی به تفاضل‌های خروجی خاص منجر می‌شوند، پیدا کرد.

تحلیل خطی: در تحلیل خطی از روابط خطی میان بیت‌های متن آشکار، بیت‌های متن رمزی و بیت‌های کلید استفاده می‌شود تا بتوان بیت‌هایی از کلید یا اطلاعاتی در مورد آن‌ها به‌دست آورد [۱۰].

مقاومت در برابر تحلیل تفاضلی و خطی: از آنجا که ویژگی‌های تفاضلی و خطی برای متن‌های آشکار در طول تبدیل‌های خطی یک الگوریتم رمز با احتمال برابر ۱ منتقل می‌شود، بنابراین این تبدیل‌ها نقشی در مقاومت این الگوریتم در برابر حملات ذکر شده ندارند و عملگرهای غیرخطی هستند که باعث سختی این حملات روی یک الگوریتم رمز می‌شوند. مهم‌ترین مؤلفه غیرخطی به‌کار رفته در طراحی اکثر رمزهای قالبی، جعبه‌های جانشینی هستند که ویژگی‌های تفاضلی و خطی آن‌ها و نیز تعداد جعبه‌هایی که در یک حمله تفاضلی یا خطی درگیر می‌شوند، به طور مستقیم روی مقاومت الگوریتم در برابر حملات مورد نظر تأثیر می‌گذارد [۱۱].

در ساختار فیستلی به دلیل XOR شدن نیمه راست حالت با نیمه سمت چپ حالت، تفاضل‌هایی که در یک دور خاص ایجاد شده‌اند، می‌توانند بعد از چند دور حذف شوند. این امر، فرآیند حذف تفاضل‌ها[2] در ساختار فیستلی نامیده می‌شود. با توجه به مزیت ساختارهای فیستلی در برابر ساختارهای SPN (مانند عدم نیاز به معکوس الگوریتم برای رمزگشایی و سرعت بالای این ساختار)، فعالیت‌هایی برای افزایش تعداد جعبه‌های جانشینی فعال برای این ساختارها صورت گرفته است که یکی از مهم‌ترین کارها در این مورد توسط شیرایی و شیبوتانی [۱۲] ارائه شده است. آن‌ها روش استفاده از ماتریس‌های MDS چندگانه در ساختارهای فیستلی را پیشنهاد داده و روش جدید خود را سازوکار سوییچینگ[3] نام‌گذاری کردند. اگرچه این روش باعث کاهش حذف تفاضل‌ها در ساختارهای فیستلی و افزایش حداقل تعداد جعبه‌های جانشینی فعال می‌شود، ولی معایبی نیز دارد که از جمله آن‌ها می‌توان به موارد زیر اشاره کرد:

فرض کنید بعد ماتریس MDS به‌کار رفته در ساختار سوییچینگ برابر m و طول قالب رمز قالبی مبتنی بر این ساختار برابر n باشد. پیدا کردن ماتریس‌های MDS چندگانه، با شرایط لازم و متناسب با ساختار سوییچینگ، برای حالتی که m و n کوچک باشد، امکان‌پذیر است. اما برای وقتی که m و n بزرگ باشند این کار سخت خواهد بود [۱۲].

۱- با توجه به بند ۱، برای طراحی رمزهای قالبی با طول قالب کوچک، مانند ۱۲۸ بیت روش مناسب ارائه شده است [۱۲] ولی برای طراحی رمزهای قالبی با طول قالب بزرگ‌تر مانند ۲۵۶ بیت، استفاده از آن ساختار سخت خواهد بود.

در این مقاله ابتدا روش به‌دست آوردن لایه‌های انتشار چندگانه با ابعاد بزرگ و شرایط لازم متناسب با سازوکار سوییچینگ مورد مطالعه و بررسی قرار گرفته و با ارائه یک الگوریتم جستجو، لایه‌های انتشار چندگانه از نوع بازگشتی به‌دست می‌آید. در ادامه با استفاده از لایه‌های انتشار بازگشتی حاصل، یک ساختار برای طراحی رمزهای قالبی با طول قالب

[1] Substation Permutation Network

[2] Difference Cancelation

[3] Switching Structure

۲۵۶ بیت پیشنهاد شده است و ضمن بررسی کارایی آن، امنیت این ساختار طراحی در برابر تحلیل‌هایی مانند حمله تفاضلی، حمله خطی و تفاضلی ناممکن مورد مطالعه و بررسی قرار می‌گیرد. نتایج نشان می‌دهد که ساختار پیشنهادی در مقایسه با دیگر ساختارهای رمز قالبی با طول قالب ۲۵۶ بیت از کارایی مناسبی برخوردار بوده و علاوه بر این در برابر حملات ذکر شده امنیت اثبات‌پذیر دارد. برای روشن شدن اهمیت طراحی رمزهای قالبی ۲۵۶ بیتی نیز، دلایل زیر را می‌توان بیان کرد:

۱-در مقایسه با رمزهای قالبی ۱۲۸ بیتی یا کمتر، توجه کمی به رمزهای قالبی با طول ۲۵۶ بیت شده است.

۲-به این دلیل که تعداد معادلات جبری رمزهای ۲۵۶ بیتی نسبت به تعداد معادلات رمزهای ۱۲۸ بیتی بیشتر است، بنابراین می‌توان گفت رمزهای قالبی ۲۵۶ بیتی در برابر حملات نوع جبری، نسبت به رمزهای ۱۲۸ بیتی مقاوم‌تر هستند.

۳-رمزهای قالبی ۲۵۶ بیتی در برابر برخی حملات عام مانند حملات لغت‌نامه‌ای، حملات مصالحه زمان حافظه و حمله روز تولد، نسبت به رمزهای ۱۲۸ بیتی مقاوم‌ترند.

۴-طبق قانون مور[1] هر دو سال فناوری ۱/۵ برابر رشد پیدا می‌کند و در نتیجه حملات عام هر سال بهبود می‌یابند (همانند حمله جستجوی کامل روی DES) و در نتیجه برای افزایش امنیت اطلاعات نیاز به افزایش طول قالب و طول کلید است.

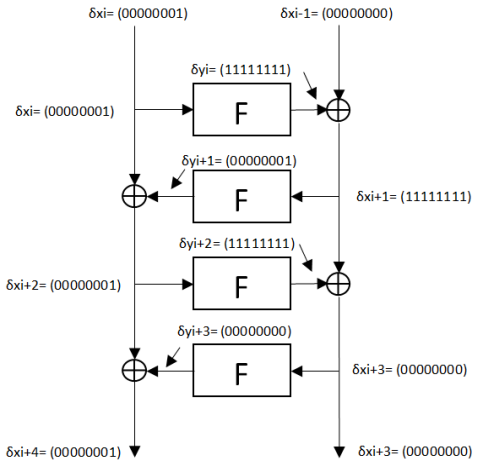
مابقی این مقاله به صورت زیر سازمان‌دهی شده است:

در بخش ۲، ساختار مبتنی بر سوییچینگ لایه‌های انتشار مورد بررسی قرار گرفته و مسائل مرتبط با این ساختار بیان شده است. در بخش ۳، ساختار پیشنهادی مبتنی بر استفاده از لایه‌های انتشار بازگشتی توضیح داده شده است و مزیت‌های این روش در مقابل روش قبلی بیان می‌شود. در این بخش یک الگوریتم جستجو برای پیدا کردن لایه‌های انتشار بازگشتی چندگانه معرفی و با استفاده از آن چند دسته لایه انتشار بازگشتی چندگانه به‌دست می‌آید. در بخش ۴، یک رمز قالبی ۲۵۶ بیتی جدید مبتنی بر روش توضیح داده شده در بخش ۳ ارائه و در بخش ۵، امنیت و کارایی آن بررسی و با الگوریتم رایندال مقایسه می‌شود.

۲. توصیف ساختار مبتنی بر سوییچینگ لایه‌های انتشار

در ساختار رمزهای فیستلی دو شاخه‌ای که از ساختار SP به عنوان تابع دور خود استفاده می‌کنند، در صورتی که تبدیل انتشار آن ماتریس *MDS* باشد. حداقل تعداد جعبه‌های جانشینی فعال برابر $\lfloor r/4 \rfloor(\beta+1)+(r \bmod 4)-1$ است (β عدد انشعاب تبدیل انتشار P است) [۱۲].

همان‌طور که در بخش ۱ بیان شد، در ساختار فیستلی به دلیل XOR شدن نیمه راست و چپ قالب، ممکن است عمل حذف تفاضل‌ها رخ دهد، بنابراین این ساختار در مقایسه با ساختار SPN، تعداد جعبه‌های جانشینی فعال کمتری خواهد داشت [۱۳]. برای توضیح بیشتر فرآیند حذف تفاضل در یک ساختار فیستلی با در نظر گرفتن حالت منقطع، می‌توان شکل (۱) را در نظر گرفت. همان‌طور که در شکل (۱) مشخص است بعد از ۴ دور عمل حذف تفاضل‌ها رخ داده است.



شکل ۱. چگونگی حذف تفاضل‌ها در ساختار فیستلی

شیرایی و شیبوتانی در FSE 2004 ساختار فیستلی را طوری تغییر دادند که بتوانند از حذف تفاضل در طول چند دور متوالی جلوگیری کنند [۱۳]. ایده کلی آن‌ها به این صورت است که به جای استفاده از یک نوع لایه انتشار در طراحی یک رمز قالبی فیستلی، از چندین لایه انتشار متفاوت در دورهای متوالی رمز استفاده شود. در ادامه کار شیرایی و شیبوتانی، شیرایی و پرنیل [۱۳] نشان دادند که اگر به جای یک ماتریس MDS در تابع دور از دو ماتریس MDS با ابعاد m×m مانند D_1 و D_2 استفاده شود، به طوری که هم عدد انشعاب هر یک از این ماتریس‌ها (برابر β=m+1 و هم عدد انشعاب الحاق شده دو ماتریس D_1 و D_2 یعنی [D_2 D_1] برابر β=m+1 باشد، تعداد جعبه‌های جانشینی فعال تفاضلی در ۶ دور برابر β= 2(m+1) 2 خواهد بود. اثبات شده که اگر عدد انشعاب الحاق دو ماتریس $(D_1^t)^{-1}$ و $(D_2^t)^{-1}$ یعنی [$(D_2^t)^{-1}$ $(D_1^t)^{-1}$] نیز برابر m+1 باشد، تعداد جعبه‌های جانشینی فعال خطی نیز در ۶ دور برابر β= 2(m+1) 2 خواهد بود [۱۴].

از آنجا که می‌بایست عدد انشعاب حاصل از الحاق دو ماتریس (یا چند ماتریس) MDS استفاده شده در ساختار مبتنی بر

[1] Mour

سوییچینگ لایه انتشار مورد بررسی قرار بگیرد و شرایط لازم را برآورده کند، بنابراین پیدا کردن ماتریس‌های با ابعاد بزرگ‌تر از ۴×۴ (در حالتی که بیشتر از دو ماتریس MDS استفاده شود) و ماتریس‌های با ابعاد بزرگ‌تر از ۸×۸ سخت خواهد بود. این امر باعث می‌شود تا استفاده از سازوکار سوییچینگ لایه‌های انتشار در ساختار فیستلی معمولی برای طراحی رمزهای قالبی ۱۲۸ بیتی کارایی داشته باشد و استفاده از این روش برای طراحی رمزهای قالبی با طول قالب بزرگ‌تر، به عنوان مثال ۲۵۶ بیت، پیچیده و دشوار خواهد بود. در ادامه این مقاله روشی پیشنهاد می‌شود که با استفاده از آن می‌توان ساختار مبتنی بر سوییچینگ لایه‌های انتشار را برای طراحی رمزهای قالبی با طول قالب بزرگ‌تر نیز استفاده کرد. برای این منظور نشان داده می‌شود که پیدا کردن لایه‌های انتشار بازگشتی چندگانه بزرگ، با شرایط متناسب با ساختار سوییچینگ، امکان پذیر است.

۳. استفاده از لایه‌های انتشار بازگشتی چندگانه در ساختار سوییچینگ

در این بخش توضیح داده می‌شود که چگونه می‌توان لایه‌های انتشار بازگشتی چندگانه با ابعاد بزرگ به‌دست آورد، به طوری که شرایط لازم مطابق با سازوکار سوییچینگ لایه‌های انتشار را داشته باشند. برای این منظور ابتدا لایه‌های انتشار بازگشتی به صورت مختصر معرفی می‌شوند.

۳-۱. لایه‌های انتشار بازگشتی

یک لایه انتشار مانند D با s کلمه x_i به عنوان ورودی و s کلمه y_i به عنوان خروجی، یک لایه انتشار بازگشتی نامیده می‌شود، اگر نمایش آن به صورت رابطه (۱) باشد [۱۵]:

$$D: \begin{cases} y_0 = x_0 \oplus F_0(x_1, x_2, \dots, x_{s-1}) \\ y_1 = x_1 \oplus F_1(x_2, x_3, \dots, x_{s-1}, y_0) \\ \vdots \\ y_{s-1} = x_{s-1} \oplus F_{s-1}(y_0, y_1, \dots, y_{s-2}) \end{cases}$$
$$D^{-1}: \begin{cases} x_{s-1} = y_{s-1} \oplus F_{s-1}(y_0, y_1, \dots, y_{s-2}) \\ x_{s-2} = y_{s-2} \oplus F_{s-2}(x_{s-1}, y_0, \dots, y_{s-3}) \\ \vdots \\ x_0 = y_0 \oplus F_0(x_1, x_2, \dots, x_{s-1}) \end{cases} \quad (۱)$$

در رابطه (۱) F_iها توابع دلخواه هستند و همان‌طور که مشاهده می‌شود برای محاسبه معکوس لایه‌های انتشار بازگشتی، نیازی به معکوس این توابع نیست. لازم به ذکر است این نوع لایه‌های انتشار خود معکوس نیستند اما معکوس آن‌ها مشابه با خودشان است. از آنجا که در رابطه (۱) تنها از XOR و توابع F_i استفاده شده است که می‌توان این توابع را نیز با تعداد عملیات کم و سبک طراحی نمود، بنابراین لایه‌های انتشار بازگشتی، برای طراحی رمزهای قالبی سبک‌وزن مناسب می‌باشند.

به عنوان یک مثال از این نوع لایه‌های انتشار می‌توان لایه انتشار ۴×۴ رابطه (۲) را در نظر گرفت:

$$D: \begin{cases} y_0 = x_0 \oplus x_2 \oplus x_3 \oplus L(x_1 \oplus x_3) \\ y_1 = x_1 \oplus x_3 \oplus y_0 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus y_0 \oplus y_1 \oplus L(x_3 \oplus y_1) \\ y_3 = x_3 \oplus y_1 \oplus y_2 \oplus L(y_0 \oplus y_2) \end{cases} \quad (۲)$$

شرایطی که برای کامل بودن این لایه انتشار برای تابع L مورد استفاده در آن لازم است، معکوس پذیری توابع

$$L(x),\ x \oplus L(x),\ x \oplus L^3(x), x \oplus L^7(x)$$

است که در آن منظور از $L^i(x)$ اعمال تابع L به تعداد i مرتبه متوالی است [۱۶].

۳-۲. مزایای لایه‌های انتشار بازگشتی و استفاده از آن‌ها در ساختار سوییچینگ

بر خلاف ماتریس‌های MDS که انجام عملیات در آن‌ها در میدان‌های گالوا و با عملگرهای جمع و ضرب است و پیاده‌سازی ماتریس‌ها با ابعاد بزرگ هزینه‌بر است، لایه‌های انتشار بازگشتی از عملگرهایی مانند چرخش، شیفت و XOR استفاده می‌کند که دارای محاسبات آسان و هزینه سبک هستند. در ادامه، روشی برای بهبود ساختار مبتنی بر سوییچینگ لایه‌های انتشار ارائه می‌شود که با استفاده از آن می‌توان شرایط لازم برای ساختار ذکر شده را برای حالتی که m و n بزرگ باشند نیز برآورد و از آن برای طراحی رمزهای قالبی با طول قالب بزرگ‌تر استفاده کرد. روش پیشنهادی استفاده از جعبه‌های جانشینی بزرگ و لایه‌های انتشار بازگشتی است.

اگر بخواهید با استفاده از ساختار سوییچینگ، یک رمز با طول قالب ۲۵۶ بیتی طراحی کنید دو روش در پیش دارید. روش اول استفاده از ساختار فیستل با تعداد شاخه‌های بیشتر (مشابه رمز قالبی Clefia [۱۷]) است که در عمل ویژگی امنیتی مبتنی بر سازوکار سوییچینگ را کم اثرتر می‌کند. روش دوم ساخت جعبه‌های جانشینی بزرگ ۳۲ بیتی (مشابه جعبه‌های جانشینی Hierocrypt) [۱۸] و سپس استفاده از لایه‌های انتشار بازگشتی با ورودی‌های ۳۲ و ۶۴ بیتی است. هر چند روش‌های گوناگونی برای طراحی ماتریس‌های MDS با طول ورودی‌های بزرگ وجود دارد ولی پیدا کردن ماتریس‌های MDS چندگانه با شرایط لازم متناسب با ساختار سوییچینگ کار ساده‌ای نیست. در این مقاله به جای جستجوی ماتریس‌های MDS چندگانه، روی موضوع پیدا کردن لایه‌های انتشار بازگشتی چندگانه تمرکز می‌شود و چند دسته لایه انتشار بازگشتی چندگانه معرفی می‌شود.

۳-۳. جستجوی لایه‌های انتشار بازگشتی D_1 و D_2 با شرایط لازم

برای به‌دست آوردن لایه‌های انتشار بازگشتی ۴×۴ مناسب برای رمز قالبی ۲۵۶ بیتی ابتدا جستجویی برای تبدیل‌های انتشار منظم تنها با یک تابع و حداقل تعداد دور به شکل کلی مطابق رابطه (۳) انجام شد. با جستجو مشاهده شد که به ازای همه حالات برای iα و β iها (که عناصری از GF(2) می‌باشند، یعنی یا صفر هستند و یا اینکه یک می‌باشند) چنین لایه انتشاری وجود ندارد. بنابراین از روش دیگری برای جستجو استفاده شد. برای جستجوی گسترده‌تر مکان عناصر به‌روز شده تغییر داده شدند. به این معنا که در رابطه (۲) ابتدا y_0 به‌روز می‌شود سپس y_1 بعد y_2 و در انتها y_3 ولی در روش فعلی ترتیب به صورت تصادفی است و ممکن است ابتدا y_3 به‌روز شود سپس y_1 بعد y_0 و در نهایت y_2 به‌روز می‌شود.

ابتدا فرض می‌شود که چهار لایه انتشار بازگشتی منظم ۴ ورودی/خروجی مطابق جدول (۱) موجود است. سپس برای اینکه روند طراحی ماتریس‌ها بیان شود الگوریتم زیر اجرا می شود:

$$Y:\begin{cases} y_0 = x_0 \oplus \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus \alpha_3 x_3 \oplus L(\beta_1 x_1 \oplus \beta_2 x_2 \oplus \beta_3 x_3) \\ y_1 = x_1 \oplus \alpha_1 x_2 \oplus \alpha_2 x_3 \oplus \alpha_3 y_0 \oplus L(\beta_1 x_2 \oplus \beta_2 x_3 \oplus \beta_3 y_0) \\ y_2 = x_2 \oplus \alpha_1 x_3 \oplus \alpha_2 y_0 \oplus \alpha_3 y_1 \oplus L(\beta_1 x_3 \oplus \beta_2 y_0 \oplus \beta_3 y_1) \\ y_3 = x_3 \oplus \alpha_1 y_0 \oplus \alpha_2 y_1 \oplus \alpha_3 y_2 \oplus L(\beta_1 y_0 \oplus \beta_2 y_1 \oplus \beta_3 y_2) \end{cases} \quad (۳)$$

جدول ۱. لایه‌های انتشار بازگشتی منظم ۴ ورودی/خروجی [۱۶]

شرایط لازم: معکوس پذیری توابع زیر	شکل کلی لایه انتشار
$I \oplus L^7$ ، $I \oplus L^3$ ، $I \oplus L$ ، L	$D:\begin{cases} y_0 = x_0 \oplus x_2 \oplus x_3 \oplus L(x_1 \oplus x_3) \\ y_1 = x_1 \oplus x_3 \oplus y_0 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus y_0 \oplus y_1 \oplus L(x_3 \oplus y_1) \\ y_3 = x_3 \oplus y_1 \oplus y_2 \oplus L(y_0 \oplus y_2) \end{cases}$
$I \oplus L^7$ ، $I \oplus L^3$ ، $I \oplus L$ ، L	$D:\begin{cases} y_0 = x_0 \oplus x_1 \oplus x_2 \oplus L(x_1 \oplus x_3) \\ y_1 = x_1 \oplus x_2 \oplus x_3 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus x_3 \oplus y_0 \oplus L(x_3 \oplus y_1) \\ y_3 = x_3 \oplus y_0 \oplus y_1 \oplus L(y_0 \oplus y_2) \end{cases}$
$I \oplus L^{15}$ ، $I \oplus L^7$ ، $I \oplus L^3$ ، $I \oplus L$ ، L	$D:\begin{cases} y_0 = x_0 \oplus x_2 \oplus L(x_1 \oplus x_2 \oplus x_3) \\ y_1 = x_1 \oplus x_3 \oplus L(x_2 \oplus x_3 \oplus y_0) \\ y_2 = x_2 \oplus y_0 \oplus L(x_3 \oplus y_0 \oplus y_1) \\ y_3 = x_3 \oplus y_1 \oplus L(y_0 \oplus y_1 \oplus y_2) \end{cases}$
$I \oplus L^{15}$ ، $I \oplus L^7$ ، $I \oplus L^3$ ، $I \oplus L$ ، L	$D:\begin{cases} y_0 = x_0 \oplus x_1 \oplus x_3 \oplus L(x_1 \oplus x_2 \oplus x_3) \\ y_1 = x_1 \oplus x_2 \oplus y_0 \oplus L(x_2 \oplus x_3 \oplus y_0) \\ y_2 = x_2 \oplus x_3 \oplus y_1 \oplus L(x_3 \oplus y_0 \oplus y_1) \\ y_3 = x_3 \oplus y_0 \oplus y_2 \oplus L(y_0 \oplus y_1 \oplus y_2) \end{cases}$

۳-۴. الگوریتم جستجو برای یافتن لایه‌های انتشار

۱) انتخاب دو لایه انتشار DD1 و DD2 از چهار لایه انتشار فوق (دقت کنید DD1 و DD2 می‌توانند یکسان باشند).

۲) انتخاب یک جایگشت برای اعداد {0,1,2,3} و انتساب آن به متغیرهای DD1. مثال: فرض کنید لایه انتشار انتخابی DD1 به صورت رابطه (۵) انتخاب شده باشد و جایگشت هم {2,3,1,0} باشد در این صورت رابطه (۶) را دارید.

۳) انتخاب یک جایگشت برای اعداد {0,1,2,3} و انتساب آن به متغیرهای DD2.

۴) محاسبه عدد انشعاب تفاضلی دو لایه DD1 و DD2. اگر عدد انشعاب تفاضلی برابر ۵ بود به مرحله ۵ برو. در غیر این صورت به مرحله ۱ برو.

۵) محاسبه عدد انشعاب خطی دو لایه DD1 و DD2. اگر عدد انشعاب خطی برابر ۵ بود DD1 و DD2 را چاپ کن. در صورت عدم اتمام به مرحله ۱ برو.

$$DD1:\begin{cases} y_0 = x_0 \oplus x_2 \oplus x_3 \oplus L(x_1 \oplus x_3) \\ y_1 = x_1 \oplus x_3 \oplus y_0 \oplus L(x_2 \oplus y_0) \\ y_2 = x_2 \oplus y_0 \oplus y_1 \oplus L(x_3 \oplus y_1) \\ y_3 = x_3 \oplus y_1 \oplus y_2 \oplus L(y_0 \oplus y_2) \end{cases} \quad (۵)$$

$$\begin{cases} y_2 = x_2 \oplus x_1 \oplus x_0 \oplus L(x_3 \oplus x_0) \\ y_3 = x_3 \oplus x_0 \oplus y_2 \oplus L(x_1 \oplus y_2) \\ y_1 = x_1 \oplus y_2 \oplus y_3 \oplus L(x_0 \oplus y_3) \\ y_0 = x_0 \oplus y_3 \oplus y_1 \oplus L(y_2 \oplus y_1) \end{cases} \quad (۶)$$

به عبارت دیگر با این روش به جای ۴ حالت ارائه شده در [۱۴] ۹۶ = ۴!×۴ حالت وجود خواهد داشت (۴ تعداد لایه‌های انتشار ۴ ورودی/خروجی با عدد انشعاب ۵ و !۴ تعداد حالاتی جابه‌جایی

ورودی‌ها). با این روش دو ساختار کلی برای لایه‌های انتشار D_1 و D_2 که شرایط لازم ساختار سوییچینگ را داشته باشند به صورت روابط (۷ و ۸) به‌دست آمد.

$$D1:\begin{cases} Y_{0(32)} = X_{0(32)} \oplus X_{1(32)} \oplus X_{2(32)} \oplus L(X_{1(32)} \oplus X_{3(32)}) \\ Y_{1(32)} = X_{1(32)} \oplus X_{2(32)} \oplus X_{3(32)} \oplus L(X_{2(32)} \oplus X_{0(32)}) \\ Y_{2(32)} = X_{2(32)} \oplus X_{3(32)} \oplus X_{0(32)} \oplus L(X_{3(32)} \oplus X_{1(32)}) \\ Y_{3(32)} = X_{3(32)} \oplus X_{0(32)} \oplus X_{1(32)} \oplus L(X_{0(32)} \oplus X_{2(32)}) \end{cases}$$

$$D2:\begin{cases} Y_{3(32)} = X_{3(32)} \oplus X_{1(32)} \oplus X_{0(32)} \oplus L(X_{2(32)} \oplus X_{0(32)}) \\ Y_{2(32)} = X_{2(32)} \oplus X_{0(32)} \oplus X_{3(32)} \oplus L(X_{1(32)} \oplus X_{3(32)}) \\ Y_{1(32)} = X_{1(32)} \oplus X_{3(32)} \oplus X_{2(32)} \oplus L(X_{0(32)} \oplus X_{2(32)}) \\ Y_{0(32)} = X_{0(32)} \oplus X_{2(32)} \oplus X_{1(32)} \oplus L(X_{3(32)} \oplus X_{1(32)}) \end{cases} \quad (۷)$$

$$D1:\begin{cases} Y_{0(32)} = X_{0(32)} \oplus X_{2(32)} \oplus X_{3(32)} \oplus L(X_{1(32)} \oplus X_{3(32)}) \\ Y_{1(32)} = X_{1(32)} \oplus X_{3(32)} \oplus X_{0(32)} \oplus L(X_{2(32)} \oplus X_{0(32)}) \\ Y_{2(32)} = X_{2(32)} \oplus X_{0(32)} \oplus X_{1(32)} \oplus L(X_{3(32)} \oplus X_{1(32)}) \\ Y_{3(32)} = X_{3(32)} \oplus X_{1(32)} \oplus X_{2(32)} \oplus L(X_{0(32)} \oplus X_{2(32)}) \end{cases}$$

$$D2:\begin{cases} Y_{3(32)} = X_{3(32)} \oplus X_{2(32)} \oplus X_{1(32)} \oplus L(X_{2(32)} \oplus X_{0(32)}) \\ Y_{2(32)} = X_{2(32)} \oplus X_{1(32)} \oplus X_{0(32)} \oplus L(X_{1(32)} \oplus X_{3(32)}) \\ Y_{1(32)} = X_{1(32)} \oplus X_{0(32)} \oplus X_{3(32)} \oplus L(X_{0(32)} \oplus X_{2(32)}) \\ Y_{0(32)} = X_{0(32)} \oplus X_{3(32)} \oplus X_{2(32)} \oplus L(X_{3(32)} \oplus X_{1(32)}) \end{cases} \quad (۸)$$

برای آن‌که لایه‌های انتشار D_1 و D_2 معرفی شده در بالا، شرایط لازم برای استفاده در ساختار سوییچینگ را داشته باشند باید تابع L و ۹ تابع$(0 \le n \le 8)$ $I \oplus L^{2^n-1}$ معکوس‌پذیر باشند که با بررسی صورت گرفته، توابع ۳۲ بیتی متعددی این ویژگی را دارند که از جمله آن‌ها می‌توان به تابع رابطه (۹) اشاره کرد:

$$L_1(x_{(32)}) = (x_{(32)} \lll 29) \oplus (x_{(32)} \gg 31) \lll 29 \quad (۹)$$

و یا توابع زیر را می‌توان در نظر گرفت:

$$L_1(x_{(32)}) = (x_{(32)} \oplus x_{(32)} \gg 1) \ggg 3$$

$$L_1(x_{(32)}) = (x_{(32)} \oplus (x_{(32)} \& 10) \gg 1) \ggg 1$$

برای به‌دست آوردن رابطه (۸) تمام زیر ماتریس‌های ۱×۱، ۲×۲، ۳×۳ و ۴×۴ از ماتریس ۸×۴ ناشی از الحاق دو تبدیل انتشار ۴×۴ را (همانند گزارش‌های قبلی [۱۶]) محاسبه کرده و مشاهده شد، تنها دو دسته تبدیل ارائه شده دارای عدد انشعاب ۵ بوده‌اند. برای اطمینان بیشتر با قرار دادن عدد ۲ به جای L در نرم‌افزار متلب و چک کردن آن در $GF(2^{\wedge}q)$ مشاهده شد که دو تبدیل خطی ارائه شده دارای عدد انشعاب ۵ خطی و تفاضلی در الحاق دو ماتریس برای $q >= 9$ هستند. رابطه (۹) نیز با استفاده از یک ماتریس ۳۲×۳۲ باینری توصیف کننده تابع خطی طبق شرایط تابع L بررسی شد. برای توضیح بیشتر چگونگی تشکیل ماتریس باینری توصیف کننده تبدیل خطی زیر با فرض عناصر ۴ بیتی به صورت زیر است:

$$L(x) = (x \ggg 2) + x \gg 1$$

۴. یک ساختار رمز قالبی ۲۵۶ بیتی بر اساس لایه‌های انتشار D_1 و D_2 پیشنهادی

در این بخش با استفاده از لایه‌های انتشار بازگشتی D_1 و D_2 که در بخش ۳-۳ معرفی شدند، یک روش طراحی برای رمزهای قالبی ۲۵۶ بیتی مبتنی بر ساختار سوییچینگ پیشنهاد می‌شود. توجه شود روش ارائه شده در این بخش یک چارچوب برای تهیه الگوریتم‌های ۲۵۶ بیتی مشخص می‌کند که با استفاده از مؤلفه‌هایی مانند جعبه‌های جانشینی در آن می‌توان به طور عملی یک رمز قالبی ۲۵۶ بیتی به‌دست آورد. از آنجا که در عمل و بسته به شرایط مختلف، برای یک الگوریتم رمز قالبی تعداد دورهای متفاوتی را می‌توان به عنوان حاشیه امنیتی آن در نظر گرفت بنابراین تنها مشخص کردن این که چارچوب پیشنهادی در چه دوری می‌تواند به امنیت برسد کافی است و تعداد دورهای دقیق برای یک رمز قالبی مبتنی بر ساختار پیشنهادی می‌بایست از تعداد دورهای مشخص شده برای امنیت ساختار مورد نظر بیشتر باشد. همچنین به دلیل اینکه بحث اصلی چارچوب توصیفی روی بخش جایگشت رمزهای قالبی است و حملات بررسی شده روی آن کاری با بخش طرح کلید آن ندارند، بنابراین می‌توان در کنار این روش پیشنهادی از یک طرح کلید امن مانند طرح کلید رایندال ۲۵۶ بیتی استفاده کرد تا بتوان یک الگوریتم عملی به‌دست آورد. برای توصیف ساختار پیشنهادی، شکل (۲) را در نظر بگیرید که در آن به ترتیب زیر عمل می‌شود:

۱- در ساختار مورد نظر از دو تابع F_1 و F_2 با ورودی ۱۲۸ بیتی استفاده شده است.

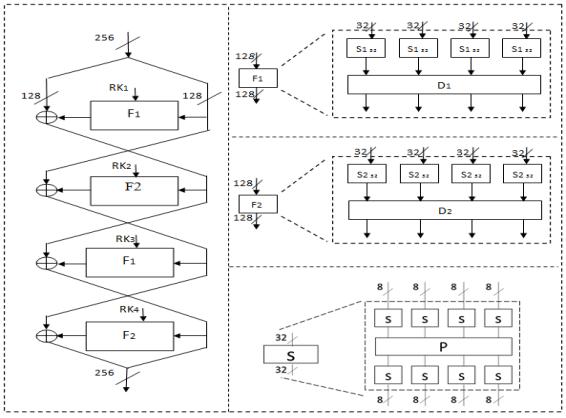
۲- تابع F_1 با استفاده از جعبه‌های جانشینی ۳۲ بیتی S_1 و تبدیل انتشار ۴ ورودی/ خروجی D_1 طراحی می‌شود.

۳- تابع F_2 با استفاده از جعبه‌های جانشینی ۳۲ بیتی S_2 و تبدیل انتشار ۴ ورودی/ خروجی D_2 طراحی می‌شود.

۴- جعبه‌های جانشینی ۳۲ بیتی S_1 و S_2 مطابق شکل (۲) با استفاده از ساختار SPS و جعبه‌های جانشینی هشت بیتی تولید می‌شوند [۱۸].

۵- D_1 و D_2 در بخش ۳-۴ طوری طراحی شده‌اند که علاوه بر اینکه عدد انشعاب D_1 و D_2 برابر ۵ است، این دو لایه انتشار، شرایط لازم برای استفاده در ساختار سوییچینگ را دارند. یعنی عدد انشعاب $[D_1\ D_2]_{4*8}$ و همچنین $[\ (D_1{}^t)^{-1}\ (D_2{}^t)^{-1}\ ]_{4*8}$ نیز برابر ۵ است.

۶- الگوریتم رمزگشایی ساختار پیشنهادی با توجه به فیستلی بودن آن نیازی به محاسبه معکوس توابع F_1 و F_2 ندارد، فقط ترتیب اعمال زیر کلیدها در رمزگذار و رمزگشا نیز بر عکس هم است.



شکل ۲. ساختار پیشنهادی رمز قالبی با طول قالب ۲۵۶ بیت

۵. امنیت و کارایی الگوریتم رمز قالبی پیشنهادی

در این بخش، امنیت و کارایی الگوریتم پیشنهادی مورد مطالعه و بررسی قرار می‌گیرد و نشان داده می‌شود که این الگوریتم در برابر حمله‌های مهمی مانند حمله خطی و تفاضلی امنیت اثبات‌پذیر دارد و در برابر حمله تفاضلی ناممکن هم مقاوم است. در پایان مقایسه‌ای بین این ساختار و رایندال ۲۵۶ بیتی هم انجام می‌گیرد.

۵-۱. امنیت الگوریتم پیشنهادی در برابر حمله‌های خطی و تفاضلی

با توجه به توضیحات ارائه شده در بخش ۲، یک رمز قالبی مبتنی بر روش طراحی پیشنهادی، در هر ۶ دور متوالی دارای ۱۰ = (۴+۱) × ۲ جعبه جانشینی فعال تفاضلی و خطی ۳۲ بیتی است. چون جعبه‌های جانشینی ۳۲ بیتی با استفاده از جعبه‌های جانشینی هشت بیتی و یک ماتریس MDS ۴×۴ روی کلمات هشت بیتی، در یک ساختار SPS، حاصل شده‌اند. بنابراین هر جعبه جانشینی ۳۲ بیتی فعال، منجر به فعال شدن حداقل ۵ جعبه جانشینی هشت بیتی خواهد شد. در نتیجه در هر شش دور متوالی ۵۰ = ۱۰ × ۵ جعبه جانشینی هشت بیتی فعال دارد. در حال حاضر جعبه‌های جانشینی هشت بیتی (به طور مثال جعبه جانشینی استفاده شده در AES) می‌توانند مشخصه‌های تفاضلی برابر ۶-۲ داشته باشند. بنابراین با استفاده از این نوع جعبه‌های جانشینی در ساختار پیشنهادی، بهترین مشخصه تفاضلی برای شش دور از طرح مبتنی بر روش طراحی فوق، حداکثر احتمال برابر با $(2^{-6})^{50} = 2^{-300}$ خواهد داشت. اریبی[1] خطی جعبه جانشینی استفاده شده در AES برابر ۴-۲ است. بنابراین با توجه به لم piling، اریبی خطی برای ۵۰ جعبه جانشینی برابر با $\epsilon = 2^{(50-1)} \prod_{i=1}^{50} 2^{-4} = 2^{-151}$ است. در نتیجه تعداد داده مورد نیاز برای انجام حمله $N = \epsilon^{-2}$ برابر با $N=(2^{-151})^{-2}=2302$ است. در جدول (۲) تعداد جعبه‌های جانشینی فعال ۸ و ۳۲ بیتی در دورهای مختلف الگوریتم مورد نظر محاسبه و نمایش داده شده است.

جدول ۲. تعداد جعبه‌های جانشینی ۸ و ۳۲ بیتی برای دورهای مختلف

تعداد جعبه‌های فعال ۸ بیتی	تعداد جعبه‌های فعال ۳۲ بیتی	تعداد دور
۵×۵=۲۵	۵	۴
۱۰×۵=۵۰	۱۰	۶
۲۰×۵=۱۰۰	۲۰	۱۲
۳۰×۵=۱۵۰	۳۰	۱۸

۵-۲. امنیت الگوریتم پیشنهادی در برابر حمله تفاضل ناممکن

الگوریتم پیشنهادی دارای ساختار فیستلی با تابع دور SP است با این ویژگی که تبدیل انتشار به‌کار رفته در دورهای زوج و فرد یکسان نیستند. قبلاً نشان داده شده که ساختار فیستلی دوشاخه‌ای با تابع دور دوسویی دارای تفاضل ناممکن ۵ دوری به صورت $(0,\alpha) \nrightarrow (0,\alpha)$ است [۱۹]. بنابراین الگوریتم پیشنهادی هم دارای همین تفاضل ناممکن ۵ دوری هست. طویل‌ترین تفاضل‌های ناممکن یافت شده برای ساختارهای مختلف خانواده رمزهای فیستلی شامل ساختارهای شبهِ *CAST*، شبه *RC6*، شبه

[1] Bias

MARS، شبکه فیستلی تعمیم یافته (*GFN*) و ساختار فیستلی دوشاخه‌ای فهرست شده است [۲۰]. در تمام تفاضل‌های ناممکن ذکر شده در این فهرست، تفاضل‌های ورودی و خروجی بر حسب صفر یا غیر صفر بودن کلمات (همان شاخه‌های ساختار) هستند. در این فهرست نیز بهترین تفاضل ناممکن یافت شده برای ساختار فیستلی دو شاخه‌ای منطبق بر مشخصه ۵ دوری کنوسن است[۱۹].

در روش قبلاً گزارش شده [۲۱]، برای ساختار فیستلی با تابع دور به فرم *SP* که تبدیل *P* به‌کار رفته از جنس ماتریس باینری باشد، تفاضل ناممکن با طول ۶ یا حتی ۷ دور به‌دست آمده است. این روش به طور مستقیم برای رمز طراحی شده قابل استفاده نیست زیرا این روش برای ساختار فیستلی با تبدیل دور *SP* با تبدیل *P* به شکل ماتریس باینری کارایی دارد اما در رمز پیشنهادی از ماتریس‌های *MDS* استفاده شده که در مقایسه با ماتریس باینری انتشار قوی‌تری را به همراه دارد. از سوی دیگر با توجه به استفاده از جعبه‌های جانشینی ۳۲ بیتی مرکب به فرم *SPS* با ماتریس *MDS* به عنوان تبدیل *P*، جستجوی تفاضل ناممکن باید با بریدن کلمات حداقل ۳۲ بیتی انجام شود و بریدن کلمات کوچک‌تر یعنی ۸ بیتی بی‌نتیجه خواهد بود. این روش را با هدف یافتن تفاضل ناممکن ۶ دوری، روی رمز طراحی شده با بریدن کلمات ۳۲ بیتی بررسی شد. تفاضل‌های ورودی و خروجی به صورت ۸ کلمه ۳۲ بیتی شامل ۷ عنصر صفر و یک عنصر غیر صفر مورد آزمایش قرار گرفتند و خوشبختانه هیچ تفاضل ناممکن ۶ دوری برای الگوریتم رمز پیشنهادی یافت نشد. بنابراین طولانی‌ترین تفاضل ناممکن برای این رمز همان تفاضل ناممکن ۵ دوری کنوسن است.

۵-۳. بررسی کارایی الگوریتم پیشنهادی

در هر دور از الگوریتم پیشنهادی، توابع F از ۴ جعبه جانشینی ۳۲ بیتی S و تبدیل انتشار با ۴ ورودی/خروجی تشکیل شده است که در آن جعبه‌های جانشینی ۳۲ بیتی پیاده‌سازی آن‌ها با استفاده از جدول‌های جستجو امکان‌پذیر است. همچنین در طراحی لایه‌های انتشار بازگشتی D_1 و D_2 فقط از عملگرهایی مانند چرخش، شیفت و XOR روی کلمات ۳۲ بیتی استفاده شده است که این کار برای پیاده‌سازی روی پردازنده‌های ۳۲ بیتی مناسب بوده و این نوع لایه‌های انتشار از سرعت مناسبی برخوردار هستند. با توجه به توضیحات ارائه شده، و همچنین با پیاده‌سازی صورت گرفته با زبان C++ با رایانه پنتیوم ۴ با کلاک ۳/۲ گیگاهرتز، سرعت الگوریتم پیشنهادی در حدود ۳۷ مگابیت در ثانیه است.

۵-۴. مقایسه امنیت و کارایی الگوریتم پیشنهادی با رمز رایندال

با توجه به اینکه ساختار پیشنهادی دارای طول قالب ۲۵۶ بیت است باید با یک الگوریتم رمز قالبی ۲۵۶ بیتی به لحاظ امنیت و کارایی مقایسه شود، به دلیل اینکه ساختار پیشنهادی از نوع فیستلی است مقایسه امنیت باید با رمز استاندارد فیستلی ۲۵۶ بیتی انجام گیرد، چون یک رمز استاندارد فیستلی ۲۵۶ بیتی به عنوان مرجع مقایسه وجود ندارد فقط به مقایسه امنیت در برابر حملات خطی، تفاضلی با شمارش حداقل تعداد جعبه‌های جانشینی در تعداد دور مساوی با رمز رایندال [۲۲] پرداخته می‌شود.

با کمی تأمل در جدول (۳)، مشخص می‌شود در ۱۲ دور جعبه‌های جانشینی فعال در دو الگوریتم نزدیک به هم است (تعداد کل جعبه‌های جانشینی در دو الگوریتم در ۱۲ دور ۳۸۴ است) بنابراین نسبت جعبه‌های جانشینی فعال به کل جعبه‌ها در رمز رایندال فقط ۲ درصد بالاتر از الگوریتم پیشنهادی است و به این معنی است که امنیت رمز پیشنهادی در برابر حملات خطی و تفاضلی نزدیک به امنیت رایندال است.

جدول ۳. حداقل تعداد S-boxهای فعال در دورهای متوالی ساختار پیشنهادی و مقایسه آن با Rijndael-256

رایندال [۲۲]	ساختار پیشنهادی	
S-box فعال	S-box فعال	دور
۲۵	۲۵	۴
۱۰۵	۱۰۰	۱۲

در مورد مقایسه کارایی دو الگوریتم می‌توان گفت با توجه به اینکه پیاده‌سازی هر دو الگوریتم با استفاده از جدول‌های مراجعه امکان‌پذیر است و این نوع پیاده‌سازی سریع اکثراً برای پیاده‌سازی آن دسته از رمزهای قالبی که از جعبه‌های جانشینی ۸ بیتی استفاده می‌کنند به‌کار می‌رود. در اینگونه موارد به جای محاسبات مستقیم، از مقادیر از قبل محاسبه شده استفاده می‌شود، همچنین در اینگونه ساختارها تبدیل انتشار نیز به این روش قابل پیاده‌سازی است. از طرفی در الگوریتم پیشنهادی از لایه‌های انتشار بازگشتی D_1 و D_2 استفاده شده است که در پیاده‌سازی لایه‌های انتشار بازگشتی D_1 و D_2 فقط از عملگرهایی مانند چرخش، شیفت و XOR روی کلمات ۳۲ بیتی استفاده شده است که این کار برای پیاده‌سازی روی پردازنده‌های ۳۲ بیتی مناسب است.

با پیاده‌سازی صورت گرفته دو رمز، با زبان C++ با رایانه پنتیوم ۴ با کلاک ۳/۲ گیگاهرتز، سرعت الگوریتم پیشنهادی در

مقایسه با الگوریتم ۱۶ دوری رایندال تنها یک درصد کاهش پیدا می‌کند. موضوع مهم دیگر در کارایی الگوریتم پیشنهادی این است که این الگوریتم قابلیت پیاده‌سازی موازی دارد و می‌تواند برای محیط‌هایی که مناسب پیاده‌سازی موازی هستند مثل محیط‌های FPGA مفید باشد و در نتیجه می‌توان در چنین محیط‌هایی با پیاده‌سازی مناسب سرعت بهتری نسبت به رایندال ۲۵۶ بیتی به‌دست آورد.

۶. نتیجه‌گیری

در این مقاله، ساختار سوییچینگ برای طراحی رمزهای قالبی مورد مطالعه و بررسی قرار گرفت و سختی‌های این روش برای طراحی یک رمز قالبی با طول قالب بزرگ‌تر (برای مثال، ۲۵۶ بیت) تشریح شد. برای حل این مشکل، استفاده از لایه‌های انتشار بازگشتی چندگانه، به جای ماتریس‌های MDS چندگانه، در ساختار سوییچینگ پیشنهاد شد و یک الگوریتم جستجو برای پیدا کردن این لایه‌های انتشار ارائه شد. با استفاده از این روش جستجو، یک شکل کلی برای لایه‌های انتشار بازگشتی چندگانه معرفی شد که از آن‌ها می‌توان برای ساخت لایه‌های انتشار بزرگ استفاده کرد. در این نوع لایه‌های انتشار از شیوه تبدیل انتشار بازگشتی با استفاده از دو تابع که معکوس هم هستند استفاده شد که می تواند از لحاظ پیاده‌سازی قابل توجه باشد. با استفاده از این لایه‌های انتشار و نیز روش طراحی جعبه‌های جانشینی ۳۲ بیتی یک رمز قالبی با طول قالب ۲۵۶ بیت ارائه شد و امنیت و کارایی آن مورد بررسی قرار گرفت. با توجه به توضیحات ارائه شده در این مقاله می‌توان گفت که الگوریتم پیشنهادی با شش دور در برابر حملات خطی و تفاضلی امنیت اثبات‌پذیر دارد. همچنین امنیت و کارایی الگوریتم پیشنهادی با رایندال مقایسه شد، امنیت آن دو درصد و کارایی آن نسبت به رایندال یک درصد کمتر است.

۷. مراجع

[1] Briceno, M.; Goldverg, I.; Wagner, D. “A Pedagogical Implementation of the GSM A5/1: Voice Privacy Encryption Algorithms”; 1999, http://cryptome.org/gsm-a512.html

[2] Briceno, M.; Goldverg, I.; Wagner, D. “A Pedagogical Implementation of the GSM A5/2 Voice Privacy Encryption Algorithms”; 1999, http://cryptome.org/gsm-a512.html

[3] 3rd Generation Partnership Project “Technical Specification Group Services and System Aspects, 3G Security, Specification of the 3GPP Confidentiality and Integrity Algorithms”; Document 2: Kasumi Specification, V3.1.1, 2001.

[4] Wu, W.; Zhang, L. “LBlock: A Lightweight Block Cipher”; Applied Cryptography and Network Security 2011, 327–344.

[5] Borghoff, J.; Canteaut, A.; Güneysu, T.; Kavun, E. B.; Knezevic, M.; Knudsen, L. R.; Leander, G.; Nikov, V.; Paar, C.; Rechberger, C.; Rombouts, P.; Thomsen, S. S.; Yalçın, T. “PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications”; Advances in Cryptology, Asiacrypt 2012, 208–225.

[6] Albrecht, M. R.; Driessen, B.; Kavun, E. B.; Leander, G.; Paar, C.; Yalçın, T. “Block Ciphers – Focus on the Linear Layer (Feat. PRIDE)”; Advances in Cryptology, Crypto 2014, 57–76.

[7] Banik, S.; Bogdanov, A.; Isobe, T.; Shibutani, K.; Hiwatari, H.; Akishita, T.; Regazzoni, F. “Midori: A Block Cipher for Low Energy”; Advances in Cryptology, Asiacrypt 2014, 411–436.

[8] Shannon, C. B. “Communication Theory of Secrecy Systems”; J. Bell. Syst. Tech. 1949, 28, 656–715.

[9] Biham, E.; Shamir, A. “Differential Cryptanalysis of DES-like Cryptosystems”; J. Cryptology 1991, 4, 3–72.

[10] Matsui, M. “Linear Cryptanalysis Method for DES Cipher”; Advances in Cryptology, Eurocrypt 1994, 765, 386–397

[11] Mouha, N.; Wang, Q.; Gu, D.; Preneel, B. “Differential and Linear Cryptanalysis using Mixed-Integer Linear Programming”; Information Security and Cryptology 2011, 7537, 57-76.

[12] Shirai, T.; Preneel, B. “On Feistel Ciphers using Optimal Diffusion Mappings across Multiple Rounds”; Asiacrypt 2004, 3329, 1-15.

[13] Shirai, T.; Shibutani, K. “Improving Immunity of Feistel Ciphers against Differential Cryptanalysis by using Multiple MDS Matrices”; Fast Software Encryption 2004, 3017, 260-278.

[14] Shirai, T.; Shibutani, K. “On Feistel Structures using a Diffusion Switching Mechanism”; Fast Software Encryption 2006, 4047, 41-56.

[15] Sajadieh, M.; Dakhilalian, M.; Mala, H.; Sepehrdad, P. “Recursive Diffusion Layers for Block Ciphers and Hash Functions”; Fast Software Encryption 2012, 7549, 385-401.

[16] Sajadieh, M.; Dakhilalian, M.; Mala, H.; Sepehrdad, P. “Efficient Recursive Diffusion Layers for Block Ciphers and Hash Functions”, J. Cryptology 2015, 28, 240-256.

[17] Shirai, T.; Shibutani, K.; Akishita, T.; Moriai, S.; Iwata, T. “The 128-bit Block Cipher CLEFIA”; Fast Software Encryption 2007, 4593, 181-195.

[18] Ohkuma, K.; Muratani, H.; Sano, F.; Kawamura, S. “The Block Cipher Hierocrypt”; Selected Areas in Cryptography 2001, 2012, 72-88.

[19] Knudsen, L. “DEAL - A 128-bit Block Cipher”; Technical Report 151, Department of Informatics, University of Bergen, Bergen, Norway, 1998.

[20] Bouillaguet, C.; Dunkelman, O.; Fouque, P. A.; Leurent, G. “New Insights on Impossible Differential Cryptanalysis”; Selected Areas in Cryptography 2011, 7118, 43–259.

[21] Wei, Y.; Li, P.; Sun, B.; Li, C. “Impossible Differential Cryptanalysis on Feistel Ciphers with SP and SPS Round Functions”; Applied Cryptography and Network Security 2010, 6123, 105–122.

[22] Daemen, J.; Rijmen, V. “The Design of Rijndael: AES-the Advanced Encryption Standard”; Springer Science & Business Media, 2013.