مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"
سال چهارم، شماره ۲، تابستان ۱۳۹۵، ص ۸۴- ۷۷

یک رمز قالبی جدید با استفاده از AES چهار دوری و لایه‌های انتشار بازگشتی

عبدالرسول میرقدری*[۱]، محمود یوسفی‌پور[۲]

۱- دانشیار، ۲- دانشجوی دکتری ریاضی رمز، دانشگاه جامع امام حسین(ع)

(دریافت: ۹۴/۰۸/۲۸، پذیرش: ۹۵/۰۳/۱۷)

چکیده

امنیت رمز قالبی AES باعث شده است تا بسیاری از طراحان، هنوز هم از مولفه‌های AES در طراحی‌های جدید خود استفاده کنند. لایه‌های انتشار یکی از مولفه‌های مهم رمزهای قالبی هستند که روی امنیت و کارآیی رمز تاثیر دارند. سجادیه و همکارانش در FSE 2012 یک دسته خاص از لایه‌های انتشار، تحت عنوان لایه‌های انتشار بازگشتی را معرفی کردند که در آنها برخی کلمات خروجی به‌صورت بازگشتی به‌عنوان ورودی نیز استفاده می‌شوند. در این مقاله یک روش جدید برای به‌دست آوردن یک الگوریتم رمز قالبی ۲۵۶ بیتی مبتنی بر ترکیب چهار دور رمز قالبی AES و یک لایه انتشار بازگشتی معرفی شده است. الگوریتم رمز پیشنهادی در مقایسه با رایندال در برابر تحلیل‌های خطی و تفاضلی مقاوم‌تر است. هزینه این افزایش مقاومت، کاهش یک درصدی سرعت آن در مقایسه با رایندال است. علاوه بر این، روش پیشنهادی برای طراحی رمزهای قالبی با طول قالب ۳۸۴ و ۵۱۲ بیتی نیز تعمیم داده شده است.

واژه‌های کلیدی: رمز قالبی، لایه انتشار بازگشتی، تحلیل تفاضلی و خطی، جعبه جانشینی

۱- مقدمه

محرمانگی[۱]، جامعیت[۲] و دسترس‌پذیری[۳] سه ویژگی مهم در برقراری امنیت اطلاعات و ارتباطات هستند. الگوریتم‌های رمزنگاری، اولیه‌هایی هستند که با استفاده از پارامتری به نام کلید نقش اساسی را در تامین محرمانگی اطلاعات و ارتباطات ایفا می‌کنند. با توجه به اینکه کلید میان فرستنده و گیرنده یکسان باشد یا یکسان نباشد، الگوریتم‌های رمزنگاری را می‌توان به ترتیب به دو دسته متقارن و نامتقارن دسته‌بندی کرد. الگوریتم‌های رمز متقارن را می‌توان به دو دسته عمده رمزهای دنباله‌ای[۴] و رمزهای قالبی[۵] تقسیم کرد. در طول دهه گذشته شاهد استقبال روزافزون جامعه رمزنگاری از رمزهای قالبی و جایگزینی بیشتر رمزهای دنباله‌ای با رمزهای قالبی در پروتکل‌های رمزنگاری بوده‌ایم. به عنوان مثال در نسل جدید تلفن همراه، رمزهای دنباله‌ای [۱]، A5/2 و [۲]، A5/1 با الگوریتم رمز قالبی [۳]، Kasumi جایگزین شده است. امر مسلم، این است که امروزه رمزهای قالبی جای خود را به صورت گسترده باز کرده‌اند و اکثر پروتکل‌های رمزنگاری از رمزهای قالبی استفاده می‌کنند. رمز قالبی، یک جایگشت مبتنی بر کلید است که متن آشکار را پذیرفته و آن را با استفاده از یک کلید محرمانه و یک الگوریتم رمزنگاری به متن رمزی تبدیل می‌کند. متن رمز نیز با استفاده از همان کلید محرمانه و الگوریتم رمزگشایی، کشف رمز شده و متن آشکار به‌دست می‌آید. کلید محرمانه باید از طریق یک کانال امن بین فرستنده و گیرنده به اشتراک گذاشته شود. یک تعریف برای یک رمز قالبی را می‌توان به صورت زیر در نظر گرفت.

تعریف- رمز قالبی: یک رمز قالبی تابعی است به شکل $E:\{0,1\}^K\times\{0,1\}^N\to\{0,1\}^N$، که یک ورودی K بیتی را به عنوان کلید (k) و یک ورودی N بیتی دیگر را به عنوان متن آشکار (P) می‌گیرد و در مقابل متن رمز C=E(k,P) را بر می‌گرداند. برای هر رمز قالبی و هر کلید k، تابع E_k یک جایگشت روی $\{0,1\}^N$، یعنی تابعی یک به یک از $\{0,1\}^N$ به $\{0,1\}^N$ است و بنابراین دارای یک معکوس، مثل E^{-1} می‌باشد. هم تابع رمز و هم معکوس آن باید به سادگی قابل محاسبه باشند؛ به این معنی که با داشتن P و k بتوان C=E(k,P) را محاسبه کرد و همچنین با داشتن C و k بتوان $P=E^{-1}(k,C)$ را به‌دست آورد.

رمزهای قالبی دو خانواده اصلی دارند که عبارتند از

* رایانامه نویسنده مسئول: amrghdri@ihu.ac.ir

1 -Confidentiality
2- Integrity
3 -Availability
4 -Stream Cipher
5 -Block Cipher

ساختارهای SPN[1] [۴] و فیستلی [۵] از نمونه‌های استاندارد شده الگوریتم رمز قالبی می‌توان به ساختار فیستلی الگوریتم DES و ساختار SPN الگوریتم رمز AES اشاره کرد. اکثر الگوریتم‌های رمز به‌گونه‌ای طراحی می‌شوند که بتوانند طول قالب‌های متغیر مثل ۱۲۸ بیتی و ۲۵۶ بیتی را پشتیبانی کنند. در این میان طول قالب‌های بزرگتر مانند ۲۵۶ بیت جایگاه خاص خودشان را دارند و لازم است تا ساختار رمز به‌گونه‌ای باشد که امنیت و کارآیی لازم را تامین کند. برخی از دلایل اهمیت رمزهای قالبی با طول قالب بزرگ، برای مثال ۲۵۶ بیت را می‌توان به‌صورت زیر خلاصه کرد:

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

۲- رمزهای قالبی ۲۵۶ بیتی در برابر برخی حملات خاص مانند حملات نوع جبری، نسبت به رمزهای ۱۲۸ بیتی مقاوم‌ترند، دلیل این امر این است که تعداد معادلات جبری آنها بیشتر است.

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[2] هر دو سال تکنولوژی ۱,۵ برابر رشد پیدا می کند و در نتیجه حملات عام هر سال بهبود می‌یابند (همانند حمله به **DES** به صورت جستجوی کامل در سال ۱۹۹۳) و در نتیجه برای افزایش امنیت اطلاعات نیاز به افزایش طول قالب می‌باشد.

در این مقاله ابتدا یک رمز قالبی ۲۵۶ بیتی جدید پیشنهاد می‌شود. این الگوریتم چهار دور دارد و در هر دور آن از چهار دور AES ۱۲۸ بیتی و یک تابع خطی با ورودی و خروجی‌های ۱۲۸ بیتی استفاده شده است. امنیت الگوریتم پیشنهادی در برابر حملات خطی و تفاضلی مورد بررسی قرار گرفته است که نشان می‌دهد در مقایسه با رمز قالبی AES ۲۵۶ بیتی، الگوریتم پیشنهادی دارای تعداد جعبه‌های جانشینی فعال بیشتری بوده و از این جهت امنیت آن در برابر تحلیل‌هایی مانند تحلیل خطی و تحلیل تفاضلی بهبود یافته است. هزینه این افزایش امنیت، کاهش یک درصدی سرعت الگوریتم پیشنهادی در مقایسه با AES ۲۵۶ بیتی است. در بخش دیگر مقاله، الگوریتم پیشنهادی برای به‌دست آوردن رمزهای قالبی ۳۸۴ و ۵۱۲ بیتی تعمیم داده شده است.

ساختار مقاله: این مقاله به صورت زیر سازماندهی شده است. در بخش ۲، الگوریتم رمز قالبی ۲۵۶ بیتی پیشنهادی توصیف می‌شود. در بخش ۳، منطق طراحی الگوریتم پیشنهادی ارایه می‌شود. در بخش ۴، تحلیل و ارزیابی الگوریتم پیشنهادی ارایه شده و نتایج این تحلیل و ارزیابی با نتایج مربوط به تحلیل و ارزیابی رمز قالبی AES مقایسه می‌شود. در بخش ۵، نحوه تعمیم الگوریتم پیشنهادی برای به دست آوردن رمزهای قالبی ۳۸۴ بیتی و ۵۱۲ بیتی توضیح داده می‌شود و در نهایت نتیجه‌گیری مقاله در بخش ۶ و منابع در بخش ۷ ارایه می‌شود.

۲- توصیف الگوریتم پیشنهادی

۲-۱- نماد گذاری

در این مقاله برای معرفی الگوریتم رمز قالبی، از نمادهای زیر استفاده می شود:

$\oplus$: عملگر XOR بیتی

$\&$: عملگر AND بیتی

$|$: عملگر OR بیتی

$\gg$ ($\ll$) : عملگر شیفت به چپ (راست)

$\lll$ ($\lll$) : عملگر شیفت چرخشی به چپ (راست)

$X_{(n)}$: نشان دهنده یک عدد n بیتی

$a|b$: الحاق دو رشته بیت a و b

$$LL(x) = L^2(x)$$

$$LLL(x) = L^3(x)$$

از آنجا که در الگوریتم پیشنهادی از چهار دور رمز قالبی AES و لایه انتشار بازگشتی[3] استفاده شده است، ابتدا رمز AES و لایه‌های انتشار بازگشتی به طور مختصر معرفی می‌شوند.

۲-۲- رمز قالبی AES

الگوریتم رمز رایندال[4]، در مسابقه AES ارایه شد که دارای طول قالب متفاوت ۱۲۸، ۱۹۲ و ۲۵۶ با طول کلید متفاوت ۱۲۸، ۱۹۲ و ۲۵۶ بود. نسخه با طول قالب ۱۲۸ بیتی این الگوریتم، به عنوان برنده مسابقه انتخاب و به‌عنوان یکی از استانداردهای NIST، با نام AES منتشر شد [۶]. در حال حاضر این الگوریتم در کاربردهای غیرنظامی به صورت گسترده استفاده می‌شود. از همان شروع مسابقه AES (سال ۱۹۹۷) تاکنون رمز قالبی AES مورد تحلیل و ارزیابی تحلیلگران زیادی قرار گرفته است که در این مدت ضعف خاصی از این الگوریتم منتشر نشده است. در این بخش به معرفی این الگوریتم پرداخته می‌شود.

برحسب طول کلید AES، تعداد دورهای الگوریتم به ترتیب برابر ۱۰، ۱۲ و ۱۴ دوراست. به منظور فهم بهتر AES، ۱۶ بایت

1-Substitution and Permutation Networks (SPN)

2- Mour

3 -Recursive Diffusion Layer

4- Rijndael-256

هر متن به صورت یک ماتریس ۴×۴ نمایش داده داده می‌شود (جدول (۱)).

جدول (۱). نمایش حالت AES به شکل یک ماتریس ۴×۴

۰	۴	۸	۱۲
۱	۵	۹	۱۳
۲	۶	۱۰	۱۴
۳	۷	۱۱	۱۵

هر دور الگوریتم AES به ترتیب شامل چهار تابع است:

۱) جانشینی بایتی
۲) شیفت سطری
۳) ترکیب ستونی
۴) جمع با زیرکلید دور مربوطه

توجه شود که دور آخر AES تا حدی با دورهای دیگر آن متفاوت است. در این دور از تابع ترکیب ستونی استفاده نمی‌شود. علاوه بر این قبل از اینکه حالت وارد دور اول AES شود، با یک زیرکلید (کلید سفیدساز) xor می‌شود.

چهار دور متوالی از AES ویژگی‌های امنیتی مطلوبی دارد که آن را می‌توان با توجه به تعداد جعبه‌های جانشینی فعال این چهار دور بررسی کرد. در [۶] اثبات شده است که چهار دور AES حداقل دارای ۲۵ جعبه جانشینی فعال است. با توجه به ویژگی‌های تفاضلی و خطی جعبه جانشینی به کار رفته در AES، این تعداد جعبه جانشینی کافی است تا الگوریتم چهار دوری مورد نظر در برابر حملات خطی و تفاضلی مقاوم باشد. با توجه به این امر و نیز سادگی تابع دور AES، هنوز هم برخی طراحان در طراحی‌های جدید خود از مولفه‌های این رمز قالبی استفاده می‌کنند. به عنوان مثال در این مورد می‌توان به برخی نامزدهای ارایه شده در مسابقه CAESAR [۷]، مانند AEGIS [۸]، YAES [۹] و Marble [۱۰] اشاره کرد.

۳-۲- لایه‌های انتشار بازگشتی

یک معیار مهم در طراحی لایه انتشار رمزهای قالبی این است که لایه انتشار طوری باشد که بتواند تغییرات ایجاد شده در یک دور را در دورهای بعدی به تغییرات بیشتری منتشر نماید. به عبارت دیگر باعث درگیر شدن جعبه‌های جانشینی بیشتری شود. بنابراین لایه انتشاری مطلوب است که تا حد امکان منجر به جعبه‌های جانشینی فعال بیشتری شود. یک معیار مهم برای ارزیابی یک لایه انتشار، مفهومی تحت عنوان عدد انشعاب برای این لایه انتشار می‌باشد که در ادامه تعریف می‌شود. برای این منظور لازم است تا ابتدا مفهوم وزن همینگ تعریف شود

تعریف وزن همینگ. برای یک بردار w به طول n با درایه‌های صحیح، $Hm(w)$ وزن همینگ آن تعریف می‌شود که برابر با تعداد درایه‌های غیرصفر بردار w است.

تعریف عدد انشعاب. تبدیل خطی D را که به عنوان لایه انتشارِ یک سیستم رمزی استفاده شده است، در نظر بگیرید که $\boldsymbol{s}$ کلمه را به عنوان ورودی گرفته و بردار $\boldsymbol{D(w)}$ شامل $\boldsymbol{s}$ کلمه را به عنوان خروجی تولید می‌کند. در این صورت عدد انشعاب $\boldsymbol{D}$ برابر با حداقل مقدار برای مجموع وزن همینگ بردارهای ورودی و خروجی تعریف می‌شود:

$$B_D = \min_{w\neq 0}\{Hm(w) + Hm(D(w))\}.$$

به طوری که این حداقل مقدار، روی مجموعهٔ تمام مقادیر غیرصفر ورودی محاسبه شده است.

عدد انشعاب یک تبدیل خطی، معیاری برای سنجش قدرت انتشار آن می باشد. برای یک لایه انتشار با ورودی و خروجی $\boldsymbol{s}$ کلمه، حداکثر عدد انشعاب برابر $\boldsymbol{s}+1$ است [۱۱].

لایه انتشار کامل. لایه انتشار $\boldsymbol{s}\times\boldsymbol{s}$ که عدد انشعاب آن، حداکثر مقدار ممکن یعنی برابر $\boldsymbol{s}+1$ باشد، لایه انتشار کامل نامیده می‌شود و لایه انتشار با عدد انشعاب $\boldsymbol{s}$ لایه انتشار تقریباً کامل نامیده می‌شود. یک نوع از لایه‌های انتشار که اخیراً مورد توجه قرار گرفته و دارای ویژگی‌های مناسبی جهت پیاده‌سازی هستند، لایه‌های انتشار بازگشتی هستند که در ادامه معرفی می‌شوند.

تعریف لایه 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 زیر باشد:

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

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

که در آن F_iها توابع خطی دلخواه هستند [۱۲]. همان‌طور که مشاهده می‌شود برای محاسبه معکوس لایه انتشار D یعنی D^{-1} نیازی به معکوس توابع F_iها نیست.

توجه شود که توابع F_i به کار رفته در لایه انتشار می‌توانند ساختاری ساده و سبک داشته باشند. این امر منجر به حاصل شدن لایه‌های انتشار ساده و سبک خواهد شد که از آن نیز می‌توان برای طراحی رمزهای قالبی سبک وزن استفاده کرد.

به عنوان یک مثال از این لایه‌های انتشار، می‌توان یکی از لایه‌های انتشار بازگشتی معرفی شده در [۱۲] با چهار ورودی و چهار خروجی را به صورت زیر در نظر گرفت:

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

که در آن، منظور از L، یک تبدیل خطی است.

در [۱۲]، ثابت شده است که شرط کافی برای اینکه لایه انتشار بالا کامل بوده و حداکثر عدد انشعاب یعنی برابر ۵ را داشته باشد، لازم است توابع $L(x), x \oplus L(x), x \oplus L^3(x), x \oplus L^7(x)$ معکوس‌پذیر باشند. منظور از $L^3(x)$ و $L^7(x)$، به‌ترتیب توان‌های سوم و هفتم تابع L می‌باشد.

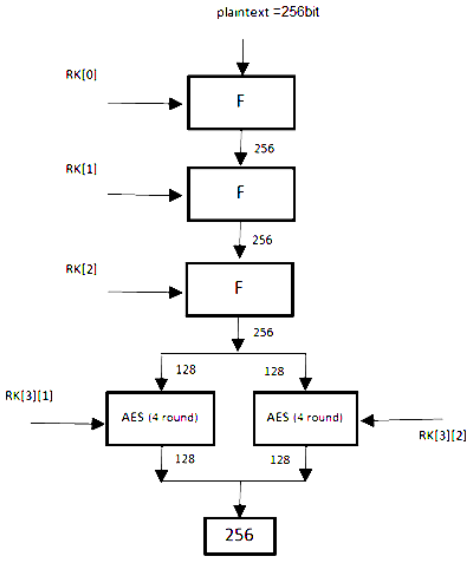
در این مقاله برای طراحی رمز قالبی جدید با طول قالب ۲۵۶ بیتی از یک لایه انتشار بازگشتی که دو زیرقالب ۱۲۸ بیتی را به عنوان ورودی گرفته و دو زیرقالب ۱۲۸ بیتی را به عنوان خروجی نتیجه می‌دهد استفاده شده است. این لایه انتشار شکل کلی زیر را دارد :

$$D:\begin{cases} y_0 = x_0 \oplus L(x_1) \\ y_1 = x_1 \oplus L(y_0) \end{cases}$$

که در ادامه تبدیل خطی L به کار رفته در آن معرفی خواهد شد.

۴-۲- معرفی الگوریتم ۲۵۶ بیتی پیشنهادی

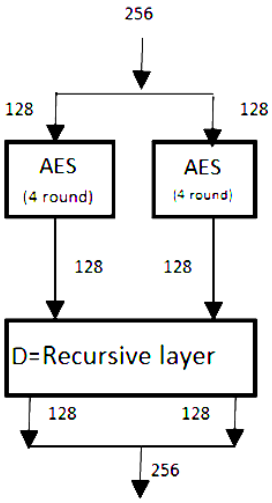
همان‌طور که ذکر شد، برای طراحی الگوریتم پیشنهادی از چهار دور AES همراه با یک لایه انتشار بازگشتی دو در دو استفاده شده است. شکل کلی این الگوریتم را می‌توان مطابق شکل (۱) در نظر گرفت.



شکل (۱). شمای کلی الگوریتم پیشنهادی

مطابق شکل (۱) این الگوریتم ۴ دور دارد که در هر دور آن از تابع دور F استفاده می‌شود. توجه شود که دور آخر الگوریتم تا حدی با سایر دورهای آن متفاوت است. در این دور، از لایه انتشار بازگشتی استفاده نمی‌شود.

تابع F . مطابق شکل (۲) تابع دور F شامل اجرای موازی دو بار الگوریتم AES چهار دوری و همچین ترکیب خروجی حاصل از آنها با استفاده از یک لایه انتشار بازگشتی به نام D است.



شکل (۲). ساختار تابع F

همانطور که قبلا اشاره شد، این لایه انتشار، دارای دو ورودی ۱۲۸ بیتی X_1 و X_2 و دو خروجی Y_1 و Y_2 است. لایه انتشار D به صورت ذیل تعریف شده است:

$$D:\begin{cases} Y_1 = X_1 \oplus X_2 \\ Y_2 = X_2 \oplus L(Y_1) \end{cases}$$

در رابطه فوق از یک تبدیل خطی Lنیز استفاده می‌شود. و تبدیل L مورد استفاده در آن به صورت زیر می‌باشد:

$$L(X) = X \lll 64 \oplus (X \,\&\, 0xFFFFFFFFFFFFFFFF)$$

اگر ورودی تبدیل L به صورت ۴ کلمه ۳۲ بیتی درنظر گرفته شود (یعنی $X=[x_1\ x_2\ x_3\ x_4]$) در این صورت تابع $Y=L(X)$ به صورت زیر نمایش داده می‌شود(روابط ذیل تشریح تابع L است):

$$y_1 = x_3$$
$$y_2 = x_4$$
$$y_3 = x_1 \oplus x_3$$
$$y_4 = x_2 \oplus x_4$$

توجه به اثبات‌های ارایه شده در [۱۲]، شرایط لازم روی تبدیل خطی L، معکوس‌پذیری توابع L و $x \oplus L(x)$ می‌باشد. لایه انتشار D مورد استفاده در اینجا، یک لایه انتشار کامل بوده و عدد انشعاب برابر سه دارد. توجه شود که تولید زیرکلیدهای رمز پیشنهادی همانند تولید زیرکلیدهای رایندال ۲۵۶ بیتی می‌باشد و الگوریتم رمزگشایی آن با توجه به الگوریتم رمزگشایی AES چهار دوری و D^{-1} به سادگی به‌دست می‌آید.

با توجه به عدد انشعاب ۳ در این الگوریتم در هر دو دور الگوریتم پیشنهادی، حداقل ۳ تابع AES چهاردوری فعال است و از آنجا که اگر ورودی AES چهار دوری غیر صفر باشد حداقل ۲۵ جعبه جانشینی فعال در آن وجود دارد. در نتیجه در هر دو دور الگوریتم پیشنهادی حداقل۷۵ و در ۴ دور بیان شده ۱۵۰جعبه جانشینی فعال وجود دارد. با توجه به آنکه با استفاده از روش‌های شمارش نظیر برنامه ریزی خطی تعداد جعبه‌های جانشینی فعال ۱۶ دور رایندال برابر ۱۴۰ جعبه جانشینی فعال است [۶]، در نتیجه تعداد جعبه‌های جانشینی فعال در الگوریتم پیشنهادی در مقایسه با رایندال افزایش یافته است.

در تابع L معرفی شده، به ازای هر L، تنها ۱۰ XOR ۳۲ بیتی اضافه در رمز پیشنهادی در مقایسه با رایندال وجود خواهد داشت که با توجه به سه بار استفاده ازتابع L، ۳۰ عمل XOR ۳۲ بیتی اضافه نسبت به رایندال ۲۵۶ وجود دارد، همچنین با شبیه‌سازی صورت گرفته، در محیط متلب با رایانه پنتیوم 4 با کلاک 3.2 گیگا هرتز، سرعت الگوریتم پیشنهادی در مقایسه با الگوریتم ۱۶ دوری رایندال تنها یک درصد کاهش پیدا می‌کند که این امر با توجه به افزایش تعداد جعبه جانشینی‌های فعال در مقایسه با رایندال و نیز بده بستان میان کارآیی و امنیت یک الگوریتم، قابل قبول می‌باشد. موضوع مهم دیگر در کارایی الگوریتم پیشنهادی این است که این الگوریتم قابلیت پیاده‌سازی موازی دارد و می‌تواند برای محیط‌هایی که مناسب پیاده سازی موازی هستند مثل محیط‌های FPGA مفید باشد و در نتیجه می‌توان در چنین محیط‌هایی با پیاده سازی مناسب سرعت بهتری نسبت به رایندال ۲۵۶ بیتی به‌دست آورد.

با پیاده‌سازی انجام‌شده مشخص گردید که سرعت رمزگشایی با سرعت رمزگذاری یکسان است. در رمز رایندال به لحاظ تئوری تعداد عملیات رمزگذاری و رمزگشایی یکسان است، اما در پیاده‌سازی عملی سرعت رمز گشایی یک درصد کمتر از رمزگذاری است. بنابراین سرعت رمزگشایی ساختار پیشنهادی با سرعت رمزگشایی رایندال برابر است.

۳- منطق طراحی

رمز قالبی معرفی‌شده در این مقاله دو مولفه اصلی دارد که عبارتنداز: تابع AES چهار دوری و لایه انتشار بازگشتی رمز قالبی AES کاهش یافته به چهار دور، در برابر حملاتی مانند حملات خطی و تفاضلی دارای امنیت اثبات‌پذیر است. بنابراین در طراحی بسیاری از الگوریتم‌های رمز جدید از AES چهار دوری استفاده شده است. برای مثال طرح رمزگذاری احراز اصالت شده ALE[13] جزو این دسته از الگوریتم‌های رمز می باشد که در FSE 2013 ارایه شده است.

لایه انتشار بازگشتی با توجه به لایه‌های انتشار معرفی شده در [۱۲]، حاصل شده است و یک ساختار ساده و کارآ دارد. علاوه بر این [۱۲]، نشان داده شده است که این لایه انتشار کامل بوده و حداکثر عدد انشعاب را دارد.

با توجه به توضیحات فوق، منطق طراحی الگوریتم پیشنهادی را می‌توان در سادگی، استفاده از توابع و مولفه‌های امن شناخته شده و امنیت خلاصه کرد.

۴- تحلیل و ارزیابی الگوریتم پیشنهادی

۴-۱- تحلیل خطی و تفاضلی

حمله تفاضلی[1] یک حمله از نوع متن اصلی منتخب است که برای اولین بار در سال ۱۹۹۱ توسط بیهام[2] و شامیر[3] منتشر شد [۱۴]. در عمل با توجه به غیرخطی بودن توابع دور در الگوریتم‌های رمز قالبی، رابطه‌ای که مقدار تفاضل خروجی یک دور را از روی مقدار تفاضل ورودی آن دور به دست می‌آورد، احتمالاتی است. با در کنار هم قرار دادن این روابط برای چند دور متوالی، عبارتی احتمالاتی به دست می‌آید که رابطه بین تفاضل ورودی و خروجی چند دور از الگوریتم را بیان می‌کند. به چنین عبارتی مشخصه تفاضلی[4] گفته می‌شود. حمله خطی[5] یک حمله از نوع متن اصلی معلوم است که برای اولین بار جهت بررسی مقاومت سیستم‌های رمزنگاری قالبی، از جمله DES توسط ماتسویی[6] در سال ۱۹۹۳ معرفی شد [۱۵] در این حمله تحلیلگر در صدد یافتن روابطی احتمالاتی درون ساختار الگوریتم، بین زیرمجموعه‌ای از بیت‌های زیرکلیدها، زیرمجموعه‌ای از بیت‌های متن اصلی و زیرمجموعه‌ای از بیت‌های متن رمز شده، به صورت زیر می‌باشد:

$$P[i_1, \dots, i_a] \oplus C[j_1, \dots, j_b] = K[k_1, \dots, k_c]$$

در رابطه بالا منظور از P، C و K به ترتیب نمایش متن اصلی، متن رمزشده و کلید است. حمله در صورتی موفقیت‌آمیز خواهد بود که احتمال برقراری رابطه خطی بالا مخالف ۰/۵ باشد. با توجه به توضیحاتی که در بخش مربوط به توصیف الگوریتم پیشنهادی ارایه شد، می‌توان نتیجه گرفته که این الگوریتم در مقایسه با رایندال تعداد جعبه های جانشینی فعال بیشتری دارد. حداقل تعداد جعبه های جانشینی متوالی در دورهای متوالی از این الگوریتم را می‌توان مطابق جدول (۲) در نظر گرفت.

1- Differential cryptanalysis
2- Biham
3- Shamir
4-Differential characteristic
5-Linear cyptanalysis
6-Matsui

نکته: در توضیح جدول (۲) ذکر این نکته ضروری است که هر دور الگوریتم پیشنهادی معادل ۴ دور رایندال است. با توجه به این جدول و ویژگی تفاضلی و خطی جعبه جانشینی رمز قالبی AES، می‌توان گفت که بهترین مشخصه تفاضلی و خطی برای دو دور الگوریتم پیشنهادی پیچیدگی داده بیشتر از جستجوی جامع خواهند داشت و در نتیجه دو دور الگوریتم پیشنهادی در برابر حمله تفاضلی و خطی مقاوم خواهد بود.

جدول(۲). حداقل تعداد *S-box*های فعال در دورهای متوالی الگوریتم پیشنهادی و مقایسه آن با رایندال

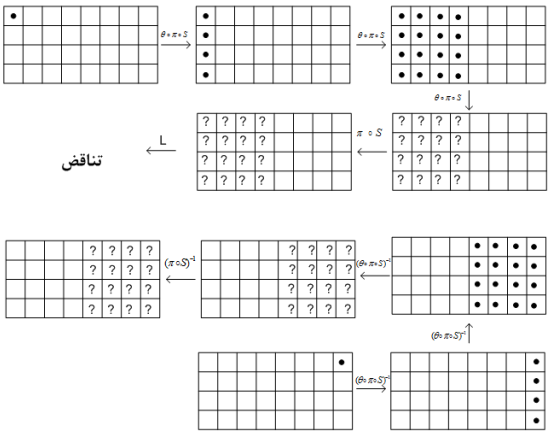
الگوریتم رایندال		الگوریتم پیشنهادی	
تعداد جعبه جانشینی	تعداد دور	تعداد جعبه جانشینی	تعداد دور
۲۵	۴	۲۵	۱
۶۵	۸	۷۵	۲
۱۰۵	۱۲	۱۰۰	۳
۱۴۰	۱۶	۱۵۰	۴

۴-۲- تحلیل تفاضلی ناممکن

روش تحلیل با استفاده از تفاضل‌های ناممکن برای اولین بار در [۱۶]، ارایه گردید. فلسفهٔ حملات تفاضلی و خطی معمولی بر مبنای یافتن رویدادهای احتمالاتی با احتمال وقوع بالا در یک الگوریتم قالبی متقارن استوار است.

در تحلیل تفاضل ناممکن، فلسفه تحلیل دقیقاً برخلاف فلسفهٔ حملهٔ تفاضلی معمولی است. به عبارت دیگر در تحلیل تفاضل ناممکن ما به دنبال رویدادی با احتمال صفر می‌گردیم، یعنی رویدادی که قطعاً نمی‌تواند در الگوریتم رخ دهد.

مطابق شکل (۳) مهمترین متمایز کننده تفاضل ناممکنی که می‌توان برای این الگوریتم به دست آورد یک تفاضل ناممکن دو دوری است و زمانی اتفاق می‌افتد که در حالت رمزگذاری تنها یکی از دو قسمت 128 بیتی و در حالت رمزگشایی نیز تنها یکی از دو قسمت غیرصفر باشند در شکل (۳) حمله تفاضلی ناممکن از طرف رمزگذار و رمزگشا مرحله به مرحله نمایش داده شده است. در این شکل عبور از یک دور تابع F که شامل عبور از ۴ دور AES و سپس عبور از لایه انتشار بازگشتی D می‌باشد، نشان داده شده است. در شکل (۳) از نماد $S\circ\pi\circ\theta$ استفاده شده است که این نماد نشان دهنده عبور از یک دور AES است که در آن S عبور از لایه غیرخطی (جعبه جانشینی)، π عبور از لایه خطی شیفت سطری و θ عبور از لایه خطی ترکیب ستونی را نشان می‌دهد. فرض کنید * تفاضلی باشد که مقدار ثابت معلوم دارد، و معادل یک بایت است. پس از اعمال * به الگوریتم بعد از اجرای دور اول به واسطه θ یک تفاضل تبدیل به ۴ تفاضل می‌شود. بعد از اجرای دور دوم به واسطه π و θ، ۴ تفاضل تبدیل به ۱۶ تفاضل می‌شود. بعد از اجرای دور سوم به واسطه S تفاضلات مقدار ثابت ولی نامعلوم (؟) دارند. بعد از اجرای دور چهارم به واسطه π و θ مقادیر ثابت نامعلوم جابجا می‌شوند. در دور چهارم یک لایه انتشار بازگشتی اضافه نیز وجود دارد که به‌واسطه عبور از این لایه بخش دوم که معادل ۱۲۸ بیت است مقدار می‌گیرد (ورودی و خروجی‌های لایه انتشار ۱۲۸ بیتی می‌باشند) از طرف رمز گشا نیز به همین روش حمله قابل اعمال است. که در شکل (۳) نشان داده شده است. لازم به ذکر است که هر چند مقادیر نامعلوم (؟) می توانند صفر باشند ولی به دلیل یک به یک بودن تابع L، همه مقادیر نامعلوم (؟) همزمان نمی‌توانند صفر باشند و این یک تناقض حساب می‌شود. با توجه به این‌که این الگوریتم معادل ۱۶ دور رایندال است. حمله تفاضلی ناممکن با این تعداد دور به این الگوریتم بعد از ۸ دور غیر قابل اعمال است.



شکل (۳). مسیر تفاضل ناممکن

اصلی که کلمات متناظر آنها دارای ارتباط خاصی با یکدیگر هستند، در نظر گرفته و سعی می‌کند ارتباط حالت‌های متناظر آنها در دورهای الگوریتم را دنبال کرده و پس از چند دور مجموع مقادیر یک کلمه خاص از حالت را پیش‌بینی کند. ارتباط متن‌های روشن معمولاً به این صورت است که مقادیر برخی کلمات ثابت هستند و برخی دیگر همه مقادیر ممکن را اتخاذ می‌کنند. "مجموع" غالباً به مفهوم جمع در گروه جمعی $GF(2^n)$ یعنی xor یا جمع در گروه جمعی Z_2^n یعنی جمع به پیمانه 2^n است.

۴-۳- تحلیل مربعی

حمله مربعی [۱۷]، حالت خاصی از حمله انتگرالی [۱۸] است؛ بنابراین حمله مربعی را با ادبیات حمله انتگرالی مورد بررسی قرار می‌دهیم.

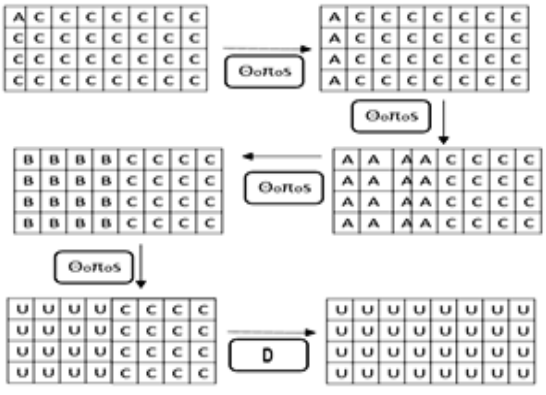
در حمله انتگرالی حالت[1] الگوریتم مجموعه‌ای از k کلمه n بیتی در نظر گرفته شده و حمله‌کننده مجموعه‌ای از متن‌های

1- State

اگر پس از i دور مجموع مقادیر یک کلمه خاص از حالت قابل پیش‌بینی باشد، معمولاً می‌توان به‌ازای یک j کوچک روی نسخه (i+j) دوری الگوریتم یک حمله استخراج کلید انجام داده و همه یا بخشی از کلیدهای j دور را به‌دست آورد.

یک حمله انتگرالی مرتبه d، حمله‌ای است که (k-d) کلمه از متن‌های روشن انتخابی ثابت هستند و d کلمه همه عناصر $(Z_2^n)^d$ را اختیار می‌کند. نماد C برای یک کلمه از حالت به مفهوم آن است که این کلمه ثابت است؛ نماد A که غالباً در حمله انتگرالی مرتبه ۱ (حمله مربعی یا Square) به‌کار می‌رود، به مفهوم آن است که این کلمه همه مقادیر ممکن را هر کدام یک بار اتخاذ می‌کند. در یک حمله مرتبه d نماد A^d برای یک کلمه به این معنی است که این کلمه هر مقدار ممکن را دقیقاً به تعداد m^{d-1} بار اتخاذ خواهد کرد. همچنین استفاده از نماد A_i^d برای d کلمه از حالت الگوریتم به این مفهوم است که چندتایی مرتب متشکل از این کلمات که دارای اندیس i هستند، همه عناصر $(Z_2^n)^d$ را اتخاذ می‌کند. بدیهی است هر کلمه دارای نماد A_i^d نیز هر مقدار ممکن را دقیقاً به تعداد m^{d-1} بار اتخاذ خواهد کرد.

در الگوریتم پیشنهادی، مطابق شکل (۴) با توجه به یکسان بودن همه ورودی‌ها، از لحاظ حمله مربعی با دنبال کردن یک حالت به این نتیجه می‌رسیم که بعد از طی ۱ دور از تابع F (که شامل ۴ مرحله عبور از AES و یک مرحله عبور از D است) همه خروجی‌ها به حالت خنثی می‌رسند و حمله به این رمز با توجه به ساختار مورد استفاده بیش از ۲ دور عملی نخواهد بود. ۲ دور این رمز معادل ۸ دور رایندال است (فرآیند تشریح حمله و نمادهای استفاده شده در شکل (۴) مانند تحلیل تفاضلی است).



شکل (۴). تمایزگر حمله مربعی

۵- تعمیم الگوریتم پیشنهادی برای به‌دست آوردن رمزهای قالبی ۳۸۴ بیتی و ۵۱۲ بیتی

با افزایش تعداد شاخه‌ها طول قالب را به ۳۸۴ و ۵۱۲ بیت می توان افزایش داد. اگر تعداد شاخه‌ها به ۳ افزایش یابد و در هر شاخه یک AES ۴ دوری وجود داشته باشد در این صورت در هر دو دور حداقل ۴ تا شاخه فعال است و ۱۰۰ جعبه جانشینی فعال وجود دارد و نیز در ۴ دور، ۲۰۰ جعبه جانشینی فعال وجود دارد. ماتریس MDS بازگشتی با ۳ ورودی/ خروجی همانند مرجع [۱۵] به صورت زیر پیشنهاد می‌شود:

$$\begin{cases} Y_{1(128)} = X_{1(128)} \oplus X_{2(128)} \oplus X_{3(128)} \\ Y_{2(128)} = X_{2(128)} \oplus X_{3(128)} \oplus L(Y_{1(128)} \oplus X_{3(128)}) \\ Y_{3(128)} = Y_{1(128)} \oplus Y_{2(128)} \oplus X_{3(128)} \end{cases}$$

برای این لایه انتشار بازگشتی نیز تابع L ارایه شده در بخش قبل مناسب است زیرا کافی است تنها L و $L \oplus I$ معکوس‌پذیر باشند. اگر تعداد شاخه‌ها به ۴ افزایش یابد و در هر شاخه یک AES ۴ دوری وجود داشته باشد در این صورت در هر دو دور حداقل ۵ تا شاخه فعال است و ۱۲۵ جعبه جانشینی فعال در هر دو دور وجود دارد. ماتریس MDS بازگشتی با ۴ورودی/ خروجی به صورت زیر پیشنهاد می‌شود:

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

تنها تفاوتی که در این بخش وجود دارد آن است که شرایط لازم برای تابع L، معکوس‌پذیری توابع $L(x), L(x) \oplus x, L^3(x) \oplus x, L^7(x) \oplus x$ است. به همین دلیل باید تابع خطی ۱۲۸ بیتی به دست آوریم که شرایط فوق را داشته باشد و علاوه بر این قابلیت پیاده‌سازی کارآ داشته باشد. یک نمونه از این توابع را می‌توان به صورت زیر در نظر گرفت:

$$L(X_{(128)}) = (X_{(128)} \ggg 32) \oplus (X_{(128)} \gg 96)$$

۶- نتیجه‌گیری

در این مقاله یک الگوریتم رمز قالبی ۲۵۶ بیتی معرفی شد که در آن از AES چهار دوری و یک لایه انتشار بازگشتی ۲×۲ استفاده می‌شود. با توجه به امنیت و کارآیی تابع AES و نیز لایه انتشار معرفی شده، الگوریتم پیشنهادی از امنیت و کارآیی خوبی برخوردار است. به طوری که این الگوریتم در مقایسه با رایندال از تعداد جعبه های جانشینی فعال بیشتری برخوردار می‌باشد. نتایج شبیه‌سازی نیز نشان می‌دهد که این افزایش امنیت، هزینه‌ای برابر با کاهش یک درصدی سرعت در مقایسه با رایندال دارد. همچنین روش ارایه شده برای طراحی الگوریتم‌های ۳۸۴ و ۵۱۲ بیتی نیز تعمیم داده شد.

۷- مراجع

[1] M. Briceno, I. Goldverg, and D. Wagner, "A Pedagogical Implementation of the GSM A5/2, voice privacy," encryption algorithms, 1999.

[2] M. Briceno, I. Goldverg, and D. Wagner, "A Pedagogical Implementation of the GSM A5/1, voice privacy," encryption algorithms, 1999.

[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] Announcing the Advanced Encryption Standard (AES), "Federal Information Processing Standards Publication 197," United States National Institute of Standards and Technology (NIST), November 26, 2001.

[5] T. Suzaki and K. Minematsu, "Improving the Generalized Feistel. FSE 10," LNCS 6147, pp. 19–39, Springer, Verlag, 2010.

[6] J. Daemen and V. Rijmen, "The design of Rijndael: AES-the advanced encryption tandard," Springer 2002.

[7] D. J. Bernstein, "CAESAR call for submissions, final," January 27, 2014.

[8] W. Hongjun and P. Bart AEGIS, "A Fast Authenticated Encryption Algorithm," http://competitions:cr:yp:to/caesar-submissions:html, 2014.

[9] A. Bosselaers and F. Vercauteren, YAES, http://competitions:cr:yp:to/caesar-submissions:html, 2014.

[10] J. Guo, Marble, http://competitions:cr:yp:to/caesar- J. J. Guo, Marble, http://competitions:cr:yp:to/caesar-submissions:html, 2014.

[11] N. T. Courtois and J. Pieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations," in Advances in Cryptology , Asiacrypt, 2002 .

[12] M. Sajadieh and M. Dakhilalian, H. Mala, P. Sepehrdad, "Recursive Diffusion Layers for Block Ciphers and Hash Functions," FSE, 2012.

[13] A. Bogdanov, F. Mendel, F. Regazzoni, V. Rijmen, and E. Tischhauser, "ALE: AES-based light weight authenticated encryption," In FSE'13, to appear, 2013.

[14] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," Journal of Cryptology, vol. 4, no. 1, pp. 3–72, 1991.

[15] M. Matsui, "Linear Cryptanalysis Method for DES Cipher," In T. Helleseth, editor, Advances in Cryptology, Eurocrypt'93, LNCS 765, pp. 386–397, Springer-Verlag, 1994.

[16] M. Nicky et al., "Differential trancatted cryp [tanalysis using mixed-integer linear programming," Information Security and Cryptology, Springer Berlin Heidelberg, 2011.

[17] J. Daemen, L. R. Knudsen, and V. Rijmen, "The Block Cipher Square," In Eli Biham, editor, Fast Software Encryption, 4th International Workshop, FSE '97, Haifa, Israel, January 20-22, 1997, vol. 1267 of Lecture Notes in Computer Science, pp. 149-165, Springer-Verlag, 1997.

[18] L. Knudsen and D. Wagner, "Integral cryptanalysis," In J. Daemen and V. Rijmen, editors, Fast Software Encryption: 9th International Workshop, FSE 2002, Leuven, Belgium, February 4-6, 2002. Revised Papers, vol. 2365 of Lecture Notes in Computer Science, pp. 112-127, Springer-Verlag, 2002.

Journal Of Electronical & Cyber Defence
Vol. 4, No. 2, 2016, Serial No.14

One Secure Block Cipher Based on Recursive Diffusion Layers and Four Rounds of AES

A. Mirghdri*, M. Yosefipour

*Imam Hossein University

(Received: 19/11/2015, Accepted: 06/06/2016)

ABSTRACT

Security of the Advanced Encryption Standard (AES) block cipher is the main reason for using its components in the new designs. The diffusion layer is one of the main block ciphers components that effect the performance and security of them. Recursive diffusion layers that was defined formally in FSE 2012 by Sajadiyeh et al. are a class of the diffusion layers which using some words of output as inputs. In this paper, a new approach for designing a block cipher is defined. Using it, one can obtain a 256-block cipher based on the four rounds of AES and a recursive diffusion layer. The suggested algorithm is compared with Rijndael-256 and it is shown that it is more resistant against linear and differential cryptanalysis. Increasing this resistance, decreases the speed by one percent when compared by Rijndael-256, i.e. there is a tradeoff between the resistance and speed. Moreover, the suggested method has been generalized for designing the block ciphers with block sizes of 384 and 512 bit.

Keywords: Block Cipher, recursive diffusion layers, Linear and differential analysis, Substitution box.

* Corresponding Author Email: amrghdri@ihu.ac.ir