پنجمین کنفرانس انجمن رمز ایران
انجمن رمز ایران
Iranian Society of Cryptology
۲۴ الی ۲۶ مهر ماه ۱۳۸۶ دانشگاه علم و صنعت ایران

تحلیل تفاضلی کارآمد الگوریتم رمزقطعه‌ای فجر۲، نسخه اصلاح شده فجر ۱

محسن رمضان یارندی
پژوهشکده پردازش هوشمند علائم
yarandi@rcisp.com

جواد مهاجری
پژوهشکده الکترونیک دانشگاه صنعتی شریف
mohajer@sharif.edu

عبدالرسول میرقدری
گروه ریاضی دانشگاه امام حسین (ع)
mirghadry@yahoo.co.in

چکیده: الگوریتم رمز قطعه‌ای فجر۱ یک الگوریتم ۱۶ دوری شبه DES با طول کلید و قطعات ورودی و خروجی ۲۵۶ بیت است. در این مقاله ابتدا به معرفی اجمالی این الگوریتم و ارائه نقاط ضعف آن پرداخته و دو راه‌کار برای رفع نقاط ضعف مربوطه ارائه خواهیم داد. سپس به تحلیل الگوریتم بهبودیافته(الگوریتم فجر۲) پرداخته و نشان می‌دهیم که اعمال اصلاحات پیشنهاد شده در لایه‌های P و S موجب افزایش عدد انشعاب لایه P ، و بهبود پارامتر امنیت تفاضلی تابع دور F به میزان $2^{-35.4}$ می‌گردد. در انتها به مقایسه دو الگوریتم از نظر مقاومت در برابر حمله تفاضلی خواهیم پرداخت. امکان به‌دست آوردن مشخصه دو دوری تکرارپذیر برای الگوریتم فجر۲ وجود ندارد، درصورتیکه درتحلیل تفاضلی الگوریتم فجر۱ مشخصه دو دوری تکرارپذیر با احتمال مناسبی به دست آمده است.

کلمات کلیدی: الگوریتم‌های رمز قطعه‌ای شبه DES ، حمله تفاضلی، پارامتر امنیت تفاضلی، مشخصهٔ تفاضلی، عدد انشعاب.

۱- مقدمه

الگوریتم فجر ۱ اولین بار در[۱] معرفی گردید و بسیار شبیه یکی از۱۵ الگوریتم منتخب دور اولAES یعنی E2 و الگوریتم طارق ۲(یکی از ۴ الگوریتم شرکت کننده در مسابقه انجمن رمز ایران) می باشد. از جمله نکات مثبت الگوریتم فجر ۱ سادگی عملگرها، S-boxهای خوب مشابه الگوریتم رایندال و تبدیلات ابتدائی و انتهائی قوی و وابسته به کلید می‌باشد. می‌توان گفت تبدیلات ابتدائی و انتهائی به تنهائی مشابه یک الگوریتم رمز عمل می‌کنند زیرا در این دو بخش زیرکلیدها به عنوان یکی از ورودی‌ها وظیفه بالا بردن پیچیدگی الگوریتم را به‌عهده دارند. همین عوامل باعث می‌شوند الگوریتم فجر۱ با تبدیلات ابتدائی و انتهائی و تنها با یک دور از هسته اصلی بتواند از تمام آزمون‌های آماری NIST عبور کند. یکی از شاخص هایی که برای ارزیابی الگوریتم‌های رمز قطعه‌ای در نظر گرفته می‌شود، اثبات مناسب و مطلوب بودن آنها به عنوان یک مولد اعداد تصادفی است. بدین معنا که از نظر محاسباتی نتوان بین دنباله‌های تولید شده توسط آنها و یک منبع تولید دنباله‌های تصادفی تمایز قائل شد. این ارزیابی برای رمزکننده‌های قطعه‌ای در واقع برآوردی آماری از میزان حصول ویژگیهای درهم پیچیدگی و انتشار الگوریتم به شمار می‌رود و بعنوان یکی از مهمترین معیارهای ارزیابی این نوع رمزکننده‌ها محسوب می شود. لازم به ذکر است که الگوریتم‌های فجر۱ و ۲با یک دور هسته اصلی نیز می‌توانند به عنوان یک الگوریتم تولید کننده دنباله‌های شبه تصادفی عمل کنند. با این حال این دو الگوریتم با تعداد دورهای متفاوت نیزارزیابی شد که نتایج حاصل از ارزیابی‌های آماری رضایت بخش بود[۲].در مجموع می‌توان ادعا کرد الگوریتم فجر۱، می تواند به عنوان یک مولد خوب برای تولید دنباله‌های شبه تصادفی در نظر گرفته شود. این الگوریتم در [۳] مورد تحلیل قرار گرفت و نشان داده شد

که مقاومت این الگوریتم دربرابر حمله تفاضلی از روش اول یعنی امنیت قابل اثبات برای ۱۶ دور هسته اصلی برابر با $DP_{\max}^{F16round} = 2^{-99.6}$ می‌باشد و درروش دوم با بکارگیری ابزار تحلیل تفاضلی CL[1] مشخصهٔ تفاضلی دودوری تکرار پذیر مناسبی با احتمال $2^{-24.8}$ بدست آمد[۳]. هر چند در [۳] به مشخصه تفاضلی ۱۶ دوری با احتمال $2^{-198.4}$ رسیده ایم ولی معمولاً برای تحلیل تفاضلی یک الگوریتم ۱۶ دوری به مشخصه تفاضلی ۱۵ دوری نیاز است. پس از بررسی مجدد الگوریتم فجر۱ به مشخصه تفاضلی ۱۵ دوری با احتمال $2^{-173.6}$ رسیدیم که این مشخصه باهفت بار تکرار یک مشخصهٔ ۲ دوری تکرار پذیر همراه با یک مشخصه یک دوری بدست آمد. این به معنی آنست که با $2^{175.6}$ زوج متن اصلی می‌توان کلید دور آخر را بدست آورد، که در مقایسه با جستجوی کامل فضای کلید آن یعنی 2^{256} ، کاهش زیادی را نشان می‌داد و نتایج بررسی‌ها نشان داد که با ایجاد تغییرات در لایه‌های P و S می‌توان به رفع نقاط ضعف فوق و ایجاد مقاومت لازم در برابر حملات تفاضلی دست یافت بدون آنکه به سایر ویژگی‌های مطلوب الگوریتم آسیب وارد شود. در بخش ۲ این مقاله به معرفی ساختار الگوریتم فجر۱ می پردازیم و در بخش ۳ اصلاحات انجام شده در فجر۱ که منجر به ایجاد فجر۲ شد، آورده شده است. در بخش ۴ به بررسی پارامتر امنیت تفاضلی ۱۶ دور از الگوریتم اصلاح شده فجر۲ پرداخته ودر بخش ۵ یک مشخصه تفاضلی ۳ دوری فجر۲ معرفی می شود و در بخش ۶ با عنوان نتیجه‌گیری به مقایسه پارامترهای مهم دو الگوریتم فجر۱ و فجر۲ می‌پردازیم.

۲- ساختار الگوریتم رمز قطعه‌ای فجر۱

شکل۱ فرآیند کلی الگوریتم فجر ۱ را نشان می‌دهد. تبدیل ابتدائی، هسته اصلی و تبدیل انتهائی بخشهای مختلف الگوریتم راتشکیل می‌دهند. تبدیلات ابتدائی و انتهائی هر کدام شامل هشت دور می‌باشند. هسته اصلی الگوریتم، مبتنی بر ساختار فیستل بوده واز ۱۶ دورتشکیل می شود. در هر دور یک کلید فرعی ۱۲۸ بیتی به تابع دور اعمال می شود که کلیدهای فرعی هر دوربا استفاده از کلید اصلی و الگوریتم تولید کلید ساخته می‌شوند. همانگونه که از شکل ۲ پیداست ، تابع دور F متشکل از دو شبکه SP است[۱]. هر شبکه SP از سه لایه تشکیل شده است. در لایه ابتدائی ترکیب داده‌های ورودی با کلید فرعی انجام می‌شود. لایه دوم، لایه‌ای غیر خطی است که شامل ۸ جعبه جانشینی یکسان به نام S_1 تا S_8 است و همگی ۱۶×۱۶ بیتی می‌باشند. لایه انتهائی یا سوم، لایه خطی P بوده و از جعبه جایگشت‌دهنده بیتها تشکیل می‌یابد. شکل ۳ روش ساخت جعبه‌های جانشینی۱۶× ۱۶ بیتی با استفاده ازسه جعبه جانشینی ۸×۸ بیتی بنامهای Ś-box1 تا Ś-box3 را نشان می‌دهد. معادلات جعبه‌های جانشینی مورد استفاده به شرح زیر می‌باشند:

$$\text{Ś-box } 1(x) = [(97x + 191) \bmod 361]^{-1} \pmod{425} \quad (۱)$$

$$\text{Ś-box } 2(x) = [(161(x^{223} \bmod 355)) + 131] \pmod{57} \quad (۲)$$

$$\text{Ś-box } 3(x) = [(187x + 107) \bmod 451]^{-1} \pmod{299} \quad (۳)$$

این جعبه‌های جانشینی با استفاده ازتوابع تقریباً غیر خطی کامل[2] (APN) طراحی و ساخته شده اند. تمام پیمانه‌ها در روابط فوق، معرف چند جمله‌ایهای ابتدائی[3] جهت ساخت میدان $GF(2^8)$ بوده و تمام عملیات دراین میدان انجام می‌گیرد[۱].برای تولید کلیدهای فرعی از ساختار فیستل سه دوری مشابه الگوریتم اصلی استفاده شده است که در مراجع[۲و۱] آمده است. شکل۴ یک دور از ۴ دورلایه P را نشان می‌دهد. البته در انتهای دور چهارم عمل چرخش ۱۶ بیتی به سمت راست وجود ندارد. عملگرهای بکار رفته در لایه خطی P عبارتند از :

$\oplus$: XOR بیت به بیت دو قطعه فرعی ۱۶ بیتی.

$>>>1$: چرخش دوری به سمت راست یک قطعه ۱۶ بیتی به اندازه یک بیت

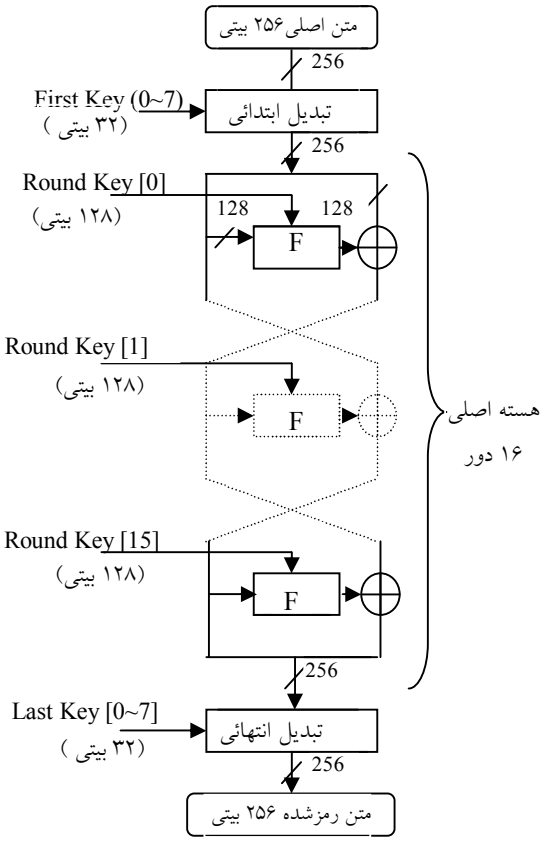
G : مبدل کد دودوئی[4] به کدگری[5] برای اعداد دودوئی ۱۶ بیتی . یعنی : $G(x) = x \oplus (x >>> 1)$

۳- اصلاح الگوریتم رمز قطعه‌ای فجر۱

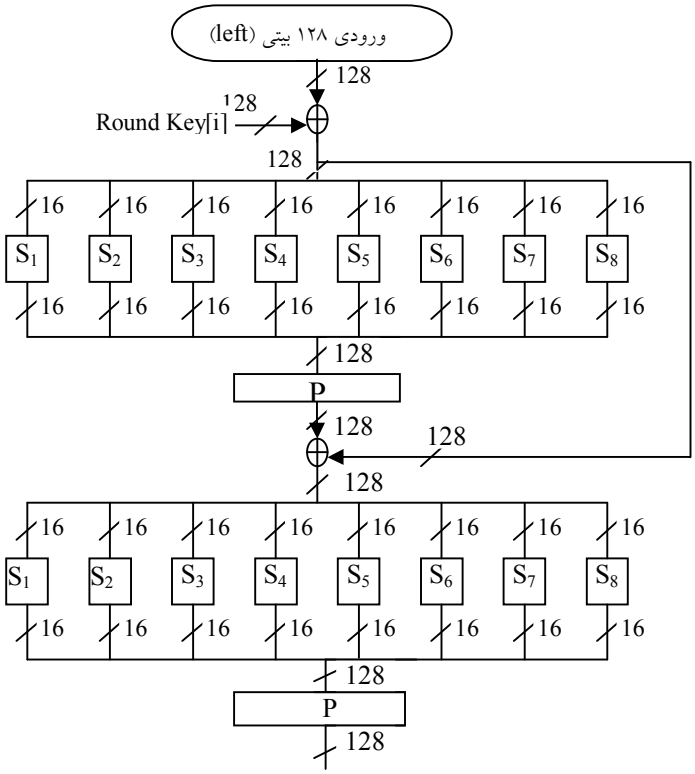
در [۳] نشان داده شد که برقراری رابطه $G(x) = G(\bar{x})$ باعث

[1] (Codec Laboratory) تهیه شده درمرجع[۲].

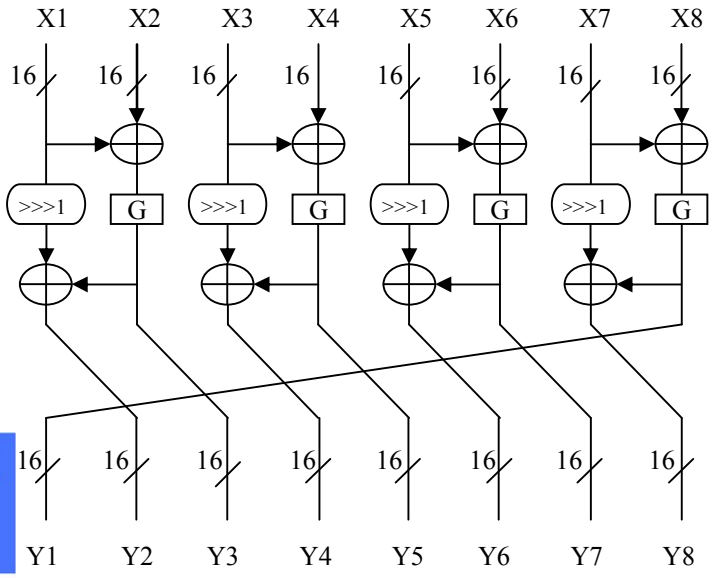
[2] Almost Perfect Nonlinear
[3] Primitive
[4] Binary Code
[5] Gray Code



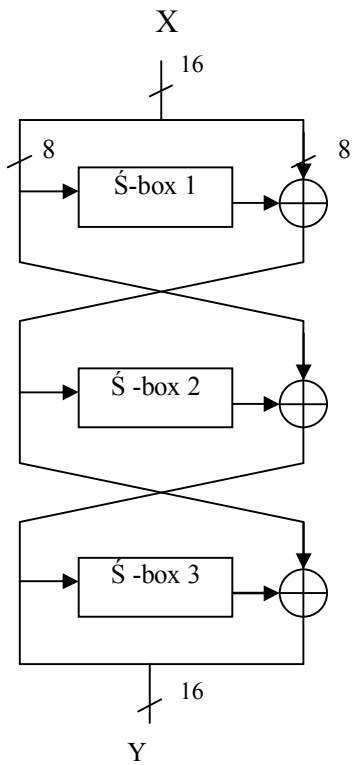
شکل۱:نمودار کلی فرآیند الگوریتم



شکل۲: تابع دور F در هسته اصلی فرآیند الگوریتم



شکل ۴ : یک دور از لایه بهم ریختگی P



شکل۳: ساختارجعبه‌های‌جانشینی‌بکاررفته‌درتابع‌دور F (S1تاS8)

می‌شود لایه P در الگوریتم فجر۱ یک به یک و پوشا نباشد. خروجی لایه مذکور با آن‌که ۱۲۸ بیتی می‌باشد اما حداکثر 2^{112} حالت ممکن را شامل می‌شود. همانطور که در [۳] نشان داده شد، این تبدیل لایه P مانند دریچه برای الگوریتم فجر۱ عمل می‌کند وعدد انشعاب لایه P در این الگوریتم برابر ۱ می‌باشد. لازم است با انجام تغییراتی درتابع G(x) شرایط مناسب برای تبدیل لایه P به یک جایگشت فراهم شود. بنابراین هدف از اصلاح $G(x)$ آنست که $G(x)$ یک تابع یک به یک و پوشا بشود تا لایه P یک جایگشت باشد.

با جایگزین ساختن تابع $G^*(x)$ به جای تابع $G(x)$ می‌توان در عین سادگی به تابع یک به یک و پوشا رسید.

$$G^*: GF\left(2^m\right) \to GF\left(2^m\right)$$
$$G^*(x) = x \oplus (x >> 1) \qquad (۴)$$

که در آن "$1 >>$ " انتقال[۱] به سمت راست یک قطعه ۱۶ بیتی به اندازه ۱ بیت است؛ و بیت وارد شده از سمت چپ، بیت صفر خواهد بود ونماد $\oplus$، XOR بیت به بیت دو قطعه ۱۶ بیتی است. با اعمال این تغییر استفاده از ساختار چهار دوری P می‌تواند منجر به عدد انشعاب مناسب شود.

می‌دانیم در لایه P سه عملگر "$1 >>$ "، "$1 <<<$"و" $\oplus$" بکار رفته است که تابع $G^*(x)$ نیز از دو عملگر "$1 >>$ " و $\oplus$ استفاده می‌کند. بنابراین $G^*(x)$ مطابق لم زیر یک تابع یک‌به‌یک و پوشا است.

لم ۱: $G^*(x)$ یک تابع یک‌به‌یک و پوشا می‌باشد.

اثبات: فرض کنید

$$x_1 = a_1, a_2, ..., a_m \quad , \quad x_2 = a_1', a_2', ..., a_m'$$

برای اثبات یک‌به‌یک بودن تابع با فرض

$$G^*(x_1) = G^*(x_2)$$

کافی است نشان دهیم: $x_1 = x_2$ داریم:

$$G^*(x_1) = (o, a_1, a_2, ..., a_{m-1}) \oplus (a_1, a_2, ..., a_m)$$
$$= a_1, a_1 \oplus a_2, a_2 \oplus a_3, ..., a_{m-1} \oplus a_m$$

به‌طور مشابه:

$$G^*(x_2) = a_1', a_1' \oplus a_2', a_2' \oplus a_3', ..., a_{m-1}' \oplus a_m'$$

اگر $G^*(x_1) = G^*(x_2)$ باشد آنگاه نظیر به نظیر باید بیت‌های آنها یکسان باشند یعنی:

$$a_1 = a_1'$$
$$a_1 \oplus a_2 = a_1' \oplus a_2'$$
$$a_2 \oplus a_3 = a_2' \oplus a_3'$$
$$\vdots$$
$$a_{m-1} \oplus a_m = a_{m-1}' \oplus a_m'$$

که از روابط $a_1 = a_1'$ و $a_1 \oplus a_2 = a_1' \oplus a_2'$ نتیجه می‌شود $a_2 = \acute{a}_2$. با ادامه روند فوق نتیجه می‌شود:

$$a_1 = a_1'$$
$$a_2 = a_2'$$
$$\dots \quad a_m = a_m' \quad \Rightarrow \quad x_1 = x_2$$

در نتیجه یک به یک بودن $G^*(x)$ اثبات می‌شود.

در مورد پوشا بودن $G^*(x)$ ؛ با توجه به‌اینکه فضای دامنه و برد تابع $G^*(x)$ یکسان و متناهی هستند و تابع $G^*(x)$ یک به یک است پس پوشا بودن $G^*(x)$ نیز نتیجه می‌شود. ■

در محاسبه مقادیر جعبه جانشینی فجر۱ در Ś-box1 نیز مشکلی وجود داشت و به ازای دو مقدار ورودی مختلف، خروجی آن ها یکسان بود که پس از اصلاح آن جدول توزیع تفاضلات S_1 تا S_8 به صورت جدول ۱ شد. همان‌طور که می‌دانیم لایه P در بدست آمدن عدد انشعاب نقش اساسی دارد و به همین دلیل اصلاح آن حائز اهمیت خاصی است. با همین تغییرات الگوریتم اصلاح شده را فجر۲ می نامیم و به تحلیل تفاضلی آن می‌پردازیم.

۴- بررسی پارامتر امنیت تفاضلی الگوریتم اصلاح شده به روش امنیت قابل اثبات

در این بخش با محاسبه پارامتر امنیت تفاضلی DP به تحلیل الگوریتم فجر ۲ می پردازیم. در نرم‌افزار CL تمام عملیات بکار رفته در این الگوریتم والگوریتم‌های مشابه بصورت بسته‌ای[۲] پیاده سازی شد معمولاً برای تحلیل یک الگوریتم، هسته اصلی آن به‌طور دقیق بررسی می‌شود و تبدیلات ابتدایی و انتهایی آن حذف می‌شوند.

۱. Shift

2 Modular

جدول ۱: قسمتی از جدول توزیع تفاضلات $S1$ تا $S8$ الگوریتم فجر۲

Δx	محل وقوع حداکثر فراوانی در Δy	مقدار فراوانی	تعداد حالات غیرصفر
0000_x	0000_x	65536	1
0001_x	$A1A3_x$	16	16129
$5A28_x$	$4E7B_x$	20	25819
$FFFF_x$	$128B_x$	10	25753

در این مقاله نیز مقاومت هسته اصلی الگوریتم در برابر حمله تفاضلی ارزیابی می‌شود. در هسته اصلی (شکل ۲) مهمترین قسمت، جعبه‌های جانشینی می‌باشند و به‌علت بزرگ بودن ابعاد جداول توزیع تفاضلات(تعداد سطر و ستون‌های جدول برابر۶۵۵۳۶=2^{16} می‌باشد) فقط بخشی ازاطلاعات در جدول ۱ آورده شده است. محل وقوع حداکثرمقادیر Δy ، در ستون دوم جدول آمده است. ستون سوم مقدار حداکثر فراوانی و ستون چهارم تعداد حالات غیر صفر در سطر ΔX ، را نشان می دهند.

(اعداد در مبنای ۱۶ با اندیس x نشان داده شده‌اند).

قدم بعدی جهت تحلیل تفاضلی، بدست آوردن پارامتر امنیت تابع دور در برابر حمله تفاضلی، $DP^{s}_{\max}$ می‌باشد. با اصلاح جدول فراخوان S'_1 مقدار پارامترهای امنیت تفاضلی S'_1 ، S'_2 و S'_3 برابر شدند.

$$DP^{S'1}_{\max} = DP^{S'2}_{\max} = DP^{S'3}_{\max} = \frac{4}{2^8} = 2^{-6} \qquad (۵)$$

با اصلاح S'_1 پارامتر امنیت تفاضلی S_1 تا S_8 نیز بهبود یافت و به مقدار زیر رسید.

$$DP^{S1\sim8}_{\max} = \frac{20}{2^{16}} = 2^{-11.7} \qquad (۶)$$

قضیه ۱: برای توابع نشان داده شده در شکل ۳ با فرض آنکه هر جعبه جانشینی S'_i دوسوئی (معکوس پذیر) باشد و $DP^{S'_i}_{\max} \le r$ در اینصورت داریم :[۶و۵]

$$DP^{S1\sim8}_{\max} \le 2r^2 \qquad (۷)$$

که در آن r مقدار ثابت مثبت می باشد.

تعریف ۱ : برای یک نگاشت خطی و معکوس‌پذیر P ، عدد انشعاب بصورت زیر تعریف می‌شود.[۱]

$$\beta(P) = \min_{a\neq 0}\left(W_h(a) + W_h(P(a))\right) \qquad (۸)$$

که در آن وزن همینگ بردار ناصفر a بصورت $W_h(a)$ نمایش داده شده است. بردار a می‌تواند متشکل از بیتها و یا یکی از عناصر میدان $GF(2^{16})$ در نظر گرفته شود. β پارامتری است که بدترین وضعیت انتشار را اندازه گیری می‌کند. ویژگی یک‌به‌یک و پوشا بودن $G^*(x)$، سبب می‌شود لایه P نیزیک‌به‌یک و پوشا باشد و چون تابع P، تابع یک به یک و پوشا است پس معکوس پذیر می‌باشد. پس با توجه به تعریف جایگشت نتیجه می‌شود لایه P یک جایگشت خواهد بود. بنابراین برای به‌دست آوردن پارامتر $DP^{F}_{\max}$ برای کل تابع دور، باید عدد انشعاب جایگشت P را به‌دست آوریم.

در ضمن به‌علت خطی بودن جایگشت P داریم:

$$P(x_1 \oplus x_2) = P(x_1) \oplus P(x_2) \qquad (۹)$$

می‌دانیم که احتمال یک مشخصه تفاضلی برابر باحاصل ضرب احتمال تفاضل جعبه‌های جانشینی فعال آن می‌باشد. از طرفی چون تعداد جعبه‌های جانشینی فعال در تابع دور توسط عدد انشعاب آن تعیین می‌گردد، باید برای بدست آوردن پارامتر امنیت تفاضلی تابع دور، به میزان عدد انشعاب، مقدار DP مربوط به جعبه‌های جانشینی فعال را در یکدیگر ضرب نمود.

تعدادی از ورودی‌ها و خروجی‌هائی که عدد انشعاب ۴ را برای لایه P اصلاح شده می‌دهند در جدول ۲ نشان داده شده است. البته تعداد بسیار زیادی ورودی لایه P با دو کلمه ۱۶ بیتی ناصفر به‌دست آمد که خروجی آنها در دوکلمه۱۶ بیتی، ناصفر بودند ولی اگر بطور مثال یک کلمه ۱۶ بیتی ورودی ناصفر باشد، در خروجی ۷ کلمه ناصفر خواهیم داشت. در نتیجه به عدد انشعاب ۴ رسیدیم.

با توجه به آن‌که عدد انشعاب به مقدار $\beta(P)=4$ بهبود یافت ، می‌توان پارامتر امنیت تفاضلی تابع F را به‌صورت زیر محاسبه کرد :

$$DP^{F}_{\max} = \left(DP^{S1\sim8}_{\max}\right)^{\beta(P)} = \left(2^{-11.7}\right)^4 = 2^{-46.8} \qquad (۱۱)$$

همچنین مشاهده می‌شود به‌علت چهار برابر شدن عدد انشعاب، پارامتر امنیت تفاضلی تابع دور F به میزان $\frac{2^{-46.8}}{2^{-11.4}} = 2^{-35.4}$

جدول ۲: مثال‌هایی از عدد انشعاب برای لایه P الگوریتم فجر۲

خروجی ۱۲۸ بیتی لایه P	$\beta(p)$	ورودی ۱۲۸ بیتی لایه P
$0000,0500,0000,0000,0000,0500,0000,0000_x$	4	$0000,0000,1000,0000,0000,0000,1000,0000_x$
$0000,0550,0000,0000,0000,0550,0000,0000_x$	4	$0000,0000,1100,0000,0000,0000,1100,0000_x$
$0000,0000,0000,0555,0000,0000,0000,0555_x$	4	$1110,0000,0000,0000,1110,0000,0000,0000_x$

بهبود یافته است. بر اساس قضیهٔ ۱، اگر تابع دور در یک ساختار فیستل سه دوری دارای پارامتر $DP^F_{\max} \le r$ باشد، آنگاه پارامتر امنیت برای کل ساختار عبارتست از :

$$DP^{F3round}_{\max} \le 2r^2 \qquad (۱۲)$$

حال با کمک نظریه امنیت قابل اثبات برای الگوریتم فجر۲ نیز عمل می‌کنیم با کمک این قضیه برای سه دور از ساختار فیستل الگوریتم فجر۲ پارامتر امنیت تفاضلی حداکثر برابر است با:

$$DP^{F3round}_{\max} = 2\left(DP^F_{\max}\right)^2 = 2^{-92.6} \qquad (۱۳)$$

ادامه کار در دو مرحله انجام می‌شود. ابتدا پارامتر امنیت را برای شش دور از هسته اصلی محاسبه نموده و سپس برای شانزده دور بسط خواهیم داد. ساختار فیستل شش دوری را می‌توان یکی از سه حالت زیر تصور نمود:[۴]

۱. اتصال سری دو شبکه فیستل سه دوری
۲. اتصال سری یک شبکه فیستل چهار دوری و یک شبکه فیستل دو دوری
۳. اتصال سری یک شبکه فیستل پنج دوری و یک شبکه فیستل یک دوری

حالت اول) پارامتر امنیت در این حالت حداکثر برابر حاصلضرب پارامتر امنیت دو شبکه فیستل سه دوری در یکدیگر می‌باشد و برابر خواهد شد با :

$$DP^{F6round}_{\max} \le \left(DP^{F3round}_{\max}\right)\left(DP^{F3round}_{\max}\right) = 2^{-185.2} \qquad (۱۴)$$

حالت دوم) می‌دانیم که یک شبکه فیستل چهاردوری از یک شبکه فیستل سه دوری ضعیف تر نیست و بطور مشابه یک شبکه فیستل دو دوری از یک شبکه فیستل یک دوری ضعیف تر نخواهد بود. لذا در بدترین شرایط پارامتر امنیت در این حالت برابر حاصلضرب پارامتر امنیت یک شبکه فیستل سه دوری در یک شبکه فیستل یک دوری خواهد بود و خواهیم داشت:

$$DP^{F6round}_{\max} \le \left(DP^{F3round}_{\max}\right)\left(DP^{F}_{\max}\right) = 2^{-92.6} \times 2^{-46.8} = 2^{-139.4} \qquad (۱۵)$$

حالت سوم) این حالت نیز مشابه حالت دوم قابل بررسی می‌باشد. به اینصورت که ساختار فیستل پنج دوری نیز از ساختار فیستل سه دوری ضعیف تر نبوده و در بدترین شرایط پارامتر امنیت مشابه حالت دوم بدست خواهد آمد.

حال برای ساختار فیستل ۱۶ دوری الگوریتم فجر۱ فقط یک حالت زیر را در نظر می‌گیریم که عبارتست از اتصال سری دو شبکه فیستل شش دوری، یک شبکه فیستل سه دوری و یک شبکه فیستل یک دوری. مشابه حالت اول پارامتر امنیت در این حالت نیز برابر حاصلضرب پارامتر امنیت این شبکه‌ها در یکدیگر می‌باشد وحداکثر برابر خواهد شد با :

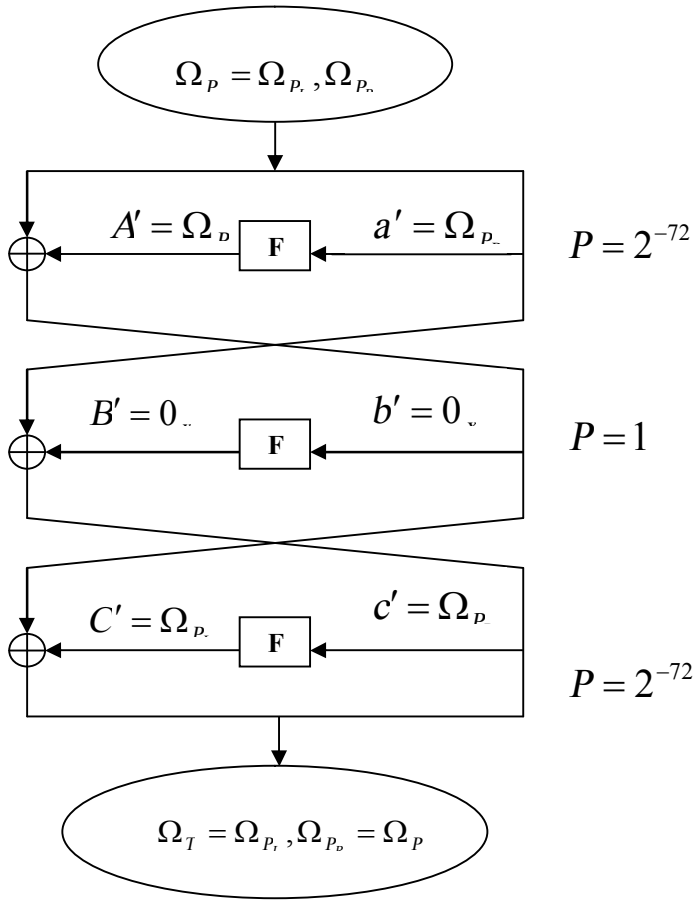
$$DP^{F16round}_{\max} \le \left(DP^{F6round}_{\max}\right)\left(DP^{F6round}_{\max}\right)\left(DP^{F3round}_{\max}\right)\left(DP^{f}_{\max}\right)$$
$$= 2^{-139.4} \times 2^{-139.4} \times 2^{-92.6} \times 2^{-46.8} = 2^{-418.2} \qquad (۱۶)$$

مشاهده می‌شود این ساختار در مقایسه با ساختار ۱۶ دوری الگوریتم فجر۱ بمراتب بهتر است و می‌تواند در مقابل حمله تفاضلی مقاوم باشد. میزان بهبود برابر با $\frac{2^{-418.2}}{2^{-99.6}} = 2^{-318.6}$ می‌باشد. باتوجه به طول قطعات که ۲۵۶ بیت می‌باشد و به‌روش جستجوی کامل نیاز به بررسی 2^{256} حالت است، می‌توان گفت الگوریتم فجر۲ با ۱۰ دور در برابر حمله تفاضلی مقاوم است و حاشیه امنیتی با شرایط موجود برابر ۶ دور است.

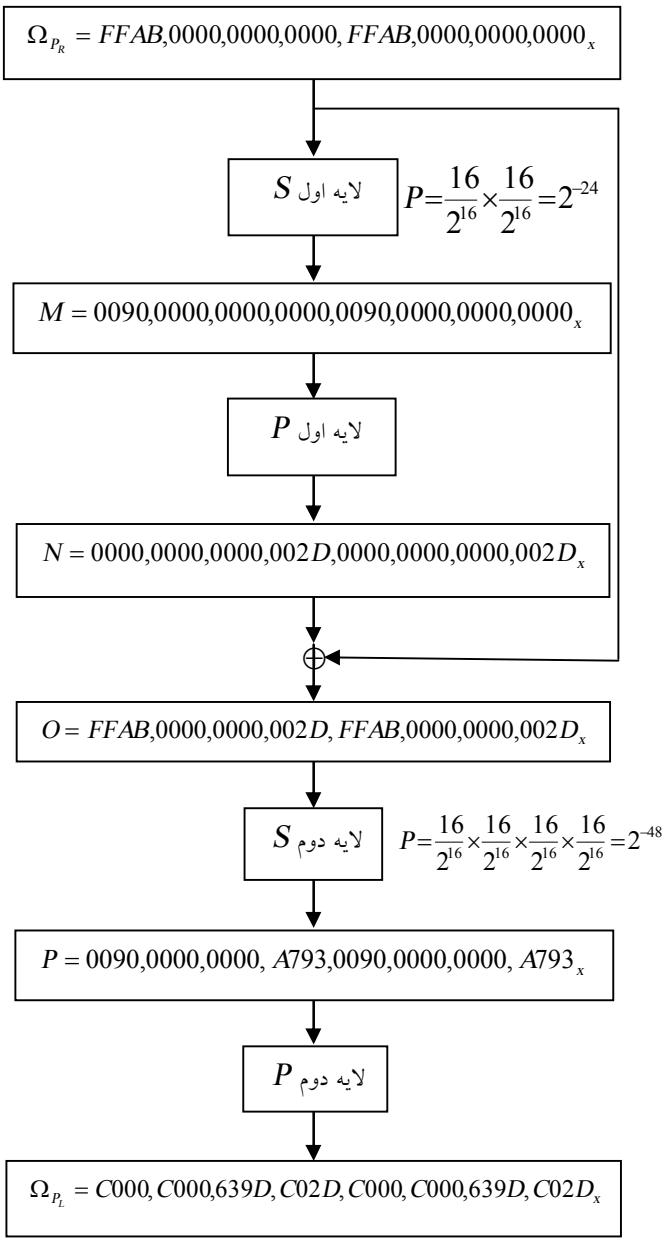
۵- بررسی امنیت الگوریتم اصلاح شده فجر۲ به روش مشخصه تفاضلی

در حمله تفاضلی به روش مشخصه تفاضلی با حذف اثر کلید، فقط با XOR ورودی و XOR خروجی های لایه S و P کار داریم. و می‌دانیم هر چه تعداد S-box های فعال بیشتر باشد، احتمال مشخصه کاهش می‌یابد. منظور از

S-box های فعال همان جعبه‌های جانشینی با ورودی تفاضلات ناصفر می‌باشند. در این قسمت به طور نمونه یک مشخصه تفاضلی ۳ دوری الگوریتم اصلاح شده را بدست می‌آوریم که در دورهای اول و سوم، شش *S-box* فعال دارند و در دور دوم هیچ *S-box*



شکل ۵ : مشخصه سه دوری الگوریتم فجر۲



شکل ۶ : نحوه بدست آمدن احتمال دورهای اول و سوم مشخصه سه دوری الگوریتم فجر۲

جدول ۳: مقایسه پارامترهای مهم دو الگوریتم فجر۱ و فجر۲

ردیف	پارامتر	الگوریتم فجر۱	الگوریتم فجر۲	میزان بهبودی
۱	امنیت تفاضلی جعبه‌های S1 تا S8	$2^{-11.4}$	$2^{-11.7}$	$2^{-0.3}$
۲	امنیت تفاضلی تابع F	$2^{-11.4}$	$2^{-46.8}$	$2^{-35.4}$
۳	امنیت تفاضلی ۱۶ دور	$2^{-99.6}$	$2^{-418.2}$	$2^{-318.6}$
٤	عدد انشعاب لایه P	1	4	4
٥	احتمال مشخصه تفاضلی سه دوری	$2^{-24.8}$	2^{-144}	$2^{-119.2}$

فعالی وجود ندارد. این مشخصه تکرار پذیر نمی‌باشد و با احتمال 2^{-144} حاصل می‌شود. امکان به‌دست آوردن مشخصه دو دوری تکرارپذیر وجود ندارد. زیرا در مشخصه‌های دو دوری تکرارپذیر، به ازای XOR ورودی به تابع F باید XOR خروجی صفر داشته باشیم و این در مورد الگوریتم فجر۲ که فقط به ازای XOR ورودی تمام صفر به لایه S و P ، XOR خروجی نیز تمام صفر می‌شود، دست یافتنی نمی‌باشد. به‌دست آوردن مشخصه‌های تفاضلی برای دورهای بالاتر امکان پذیر است اما به‌دست آوردن این مشخصه ها با احتمال مناسب اهمیت زیادی دارد. شکل‌های ۵ و٦ مشخصه سه دوری ونحوه به‌دست آمدن احتمال آن‌را نشان می‌دهند. در هر دور، تفاضلات ورودی از دو لایه SP عبور می‌کنند. همان طور که در شکل ٦ مشاهده می‌شود، در دورهای اول و سوم برای لایه اول S فقط ورودی$S\text{-}box$ های ۱ و۵ ناصفر بوده و طبق جدول ۱ با احتمال $P=\frac{16}{2^{16}}=2^{-12}$ خروجی مورد نظر هر کدام ساخته می‌شوند. برای لایه دوم S نیزفقط ورودی$S\text{-}box$ های ۱،٤، ۵ و۸ ناصفر بوده و با احتمال $P=\frac{16}{2^{16}}=2^{-12}$ خروجی مورد نظر هر $S\text{-}box$ ساخته می‌شوند. در لایه P هر تفاضل ورودی فقط یک تفاضل خروجی دارد و در نتیجه احتمال مشخصه دور اول و سوم هرکدام برابر $2^{-24}\times 2^{-48}=2^{-72}$ به‌دست می‌آید. در نتیجه مشخصه تفاضلی سه دوری الگوریتم اصلاح شده فجر۲ برابر با $P_T=2^{-72}\times 2^{-72}=2^{-144}$ می‌شود. این در حالی است که مشخصه تفاضلی سه دوری الگوریتم فجر۱ همانطور که در مرجع[۳] آمده مشابه مشخصه دو دوری تکرارپذیر آن و برابر با $P=2^{-24.8}$ است و این اعداد نشان دهنده بهبود چشمگیری در الگوریتم اصلاح شده فجر۲ می‌باشد.

۶- نتیجه گیری

در این مقاله نشان داده شد که بااصلاح جعبه جانشینی S_1' و تبدیل $G(x)$ در الگوریتم فجر۱ می‌توان به مشخصه‌های تفاضلی بسیار مناسب‌تری رسید. همچنین ثابت شد تابع اصلاح شده $G^*(x)$ یک‌به‌یک وپوشا است و در نتیجه لایه P اصلاح شده یک جایگشت می‌باشد. با روش پیاده‌سازی، عدد انشعاب لایه P در الگوریتم فجر۲ برابر $\beta(p)=4$ به‌دست آمد. از طریق روش امنیت قابل اثبات، پارامتر امنیت تفاضلی الگوریتم ۱۶ دوری فجر۲به‌میزان $\frac{2^{-418.2}}{2^{-99.6}}=2^{-318.6}$ بهبود یافت. همچنین با روش مشخصه تفاضلی بطور نمونه یک مشخصه سه دوری الگوریتم اصلاح شده با احتمال 2^{-144} بدست آمد که در مقایسه با مشخصه سه دوری الگوریتم فجر۱ به میزان $2^{-119.2}$ بهتر شده است. نتایج ارزیابی آماری الگوریتم فجر۲ نیز حاکی از شبه تصادفی بودن دنباله‌های خروجی آن بود. در انتها نتایج مقایسه پارامترهای مهم دو الگوریتم در جدول ۳ آمده است.

۷- مراجع:

[۱] طراحی ، شبیه سازی و ارزیابی یک الگوریتم رمز قالبی جدید ؛مسعودفرهنگی؛ پایان نامه کارشناسی ارشد رمز، دانشگاه امام حسین علیه السلام ، پائیز ۱۳۸۲.

[۲] ارزیابی وتحلیل تفاضلی الگوریتم رمز قطعه‌ای فجر۱ ؛ محسن رمضان یارندی؛ پایان نامه کارشناسی ارشد رمز ؛ دانشگاه امام حسین علیه السلام؛ پائیز ۱۳۸۳.

[۳] حمله تفاضلی کارآمدبه الگوریتم رمز قطعه‌ای فجر۱ ؛ محسن رمضان یارندی، عبدالرسول میر قدری، جواد مهاجری؛ مجموعه مقالات سومین کنفرانس انجمن رمز ایران ؛ شهریور ماه ۱۳۸۴؛ ص ۴۵-۵۴.

[۴] ارزیابی تحلیلی الگوریتم رمز طارق ۲، قدمعلی باقری کرم، محمد دخیل علیان ، مجموعه مقالات دومین کنفرانس انجمن رمز ایران ، ص ۲۱۸-۲۲۹.

[5] “Provable security Against a Differential Attack ", K. Nyberg and l. R. Knudsen Journal of Cryptology, Vol.8, No.1, Springer-Verlag, pp.27-37, 1995

[6] ‘"New Structure of block Cipher with Provable Security Against Differential and linear Cryptanalysis” M. Matsui, Fast Software Encryption, 3rd International Workshop Proceedings, LNCS, Springer-Verlag, pp. 208-218,1997