

تحلیل تفاضلی کارآمد الگوریتم رمزقطعه‌ای فجر ۲، 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 فجر ۱ 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 فجر ۲) پرداخته و نشان می‌دهیم که اعمال اصلاحات پیشنهاد شده در لایه-های 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 به دست آوردن مشخصه دو دوری تکرارپذیر برای الگوریتم فجر ۲ وجود ندارد، در صورتیکه در تحلیل تفاضلی الگوریتم فجر ۱ مشخصه دو دوری تکرارپذیر با احتمال مناسبی به دست آمده است.

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

۱- مقدمه

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 رمزکننده-های 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 می‌شود. لازم به ذکر است که الگوریتم‌های فجر ۱ و ۲ با 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 نیز ارزیابی شد که نتایج حاصل از ارزیابی‌های آماری رضایت بخش بود [۲]. در مجموع می‌توان ادعا کرد الگوریتم فجر ۱، می‌تواند 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

الگوریتم فجر ۱ اولین بار در [۱] معرفی گردید و بسیار شبیه یکی از ۱۵ الگوریتم منتخب دور اول AES یعنی E2 و الگوریتم طارق ۲ (یکی از ۴ الگوریتم شرکت کننده در مسابقه انجمن رمز ایران) می‌باشد. از جمله نکات مثبت الگوریتم فجر ۱ سادگی عملگرها، S-boxهای خوب مشابه الگوریتم راینال و تبدیلات ابتدائی و انتهائی قوی و وابسته به کلید می‌باشد. می‌توان گفت تبدیلات ابتدائی و انتهائی به تنهایی مشابه یک الگوریتم رمز عمل می‌کنند زیرا در این دو بخش زیرکلیدها به عنوان یکی از ورودی‌ها وظیفه بالا بردن پیچیدگی الگوریتم را به عهده دارند. همین عوامل باعث می‌شوند الگوریتم فجر ۱ با تبدیلات ابتدائی و انتهائی و تنها با یک دور از هسته اصلی بتواند از تمام آزمون‌های آماری NIST عبور کند. یکی از شاخص‌هایی که برای ارزیابی الگوریتم‌های رمز قطعه‌ای در

هر دور با 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 S₁ تا S₈ 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 جانشینی ۱۶×۱۶ بیتی با استفاده از سه جعبه جانشینی ۸×۸ بیتی بنام‌های S-box1 تا S-box3 را نشان می‌دهد.

معادلات جعبه‌های جانشینی مورد استفاده به شرح زیر می‌باشند:

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

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

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

این جعبه‌های جانشینی با استفاده از توابع تقریباً غیر خطی کامل^۲ (APN) طراحی و ساخته شده‌اند. تمام پیمانه‌ها در روابط فوق،

معرف چند جمله‌ایهای ابتدائی^۳ جهت ساخت میدان GF(2^۸) بوده و تمام عملیات در این میدان انجام می‌گیرد [۱]. برای تولید

کلیدهای فرعی از ساختار فیستل سه دوری مشابه الگوریتم اصلی استفاده شده است که در مراجع [۱ و ۲] آمده است. شکل ۴

یک دور از ۴ دور لایه 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:

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

$$\gg \gg \gg 1 : \text{ چرخش دوری به سمت راست یک قطعه ۱۶ بیتی}$$

به اندازه یک بیت

G: مبدل کد دودوئی^۴ به کدگری^۵ برای اعداد دودوئی

$$G(x) = x \oplus (x \gg \gg 1) \quad : \text{ یعنی ۱۶ بیتی.}$$

۳- اصلاح الگوریتم رمز قطعه‌ای فجر ۱

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

که مقاومت این الگوریتم در برابر حمله تفاضلی از روش اول یعنی امنیت قابل اثبات برای ۱۶ دور هسته اصلی برابر با $DP_{\max}^{F16\text{round}} = 2^{-99.6}$ می‌باشد و در روش دوم با بکارگیری ابزار تحلیل تفاضلی^۱ CL^۱ مشخصه تفاضلی دودوئی 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 فجر ۱ به مشخصه تفاضلی ۱۵ دوری با احتمال $2^{-173.6}$ رسیدیم که این مشخصه باهفت بار تکرار یک مشخصه 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 فجر ۱ می‌پردازیم و در بخش ۳ اصلاحات انجام شده در فجر ۱ که منجر به ایجاد فجر ۲ شد، آورده شده است. در بخش ۴ به بررسی پارامتر امنیت تفاضلی ۱۶ دور از الگوریتم اصلاح شده فجر ۲ پرداخته و در بخش ۵ یک مشخصه تفاضلی ۳ دوری فجر ۲ معرفی می‌شود و در بخش ۶ با عنوان نتیجه‌گیری به مقایسه پارامترهای مهم دو الگوریتم فجر ۱ و فجر ۲ می‌پردازیم.

۲- ساختار الگوریتم رمز قطعه‌ای فجر ۱

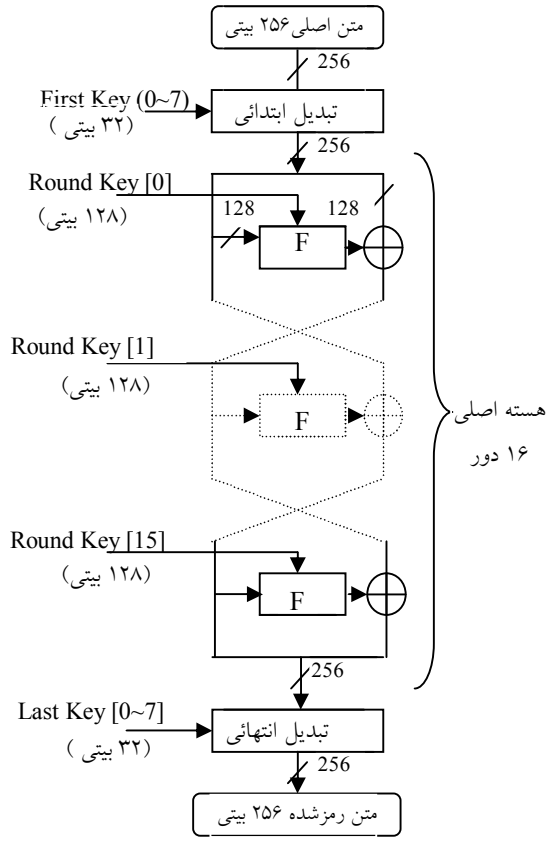
شکل ۱ فرآیند کلی الگوریتم فجر ۱ را نشان می‌دهد. تبدیل ابتدائی، هسته اصلی و تبدیل انتهائی بخشهای مختلف الگوریتم راتشکیل می‌دهند. تبدیلات ابتدائی و انتهائی هر کدام شامل هشت دور می‌باشند. هسته اصلی الگوریتم، مبتنی بر ساختار فیستل بوده و از ۱۶ دور تشکیل می‌شود. در هر دور یک کلید فرعی ۱۲۸ بیتی به تابع دور اعمال می‌شود که کلیدهای فرعی

² Almost Perfect Nonlinear

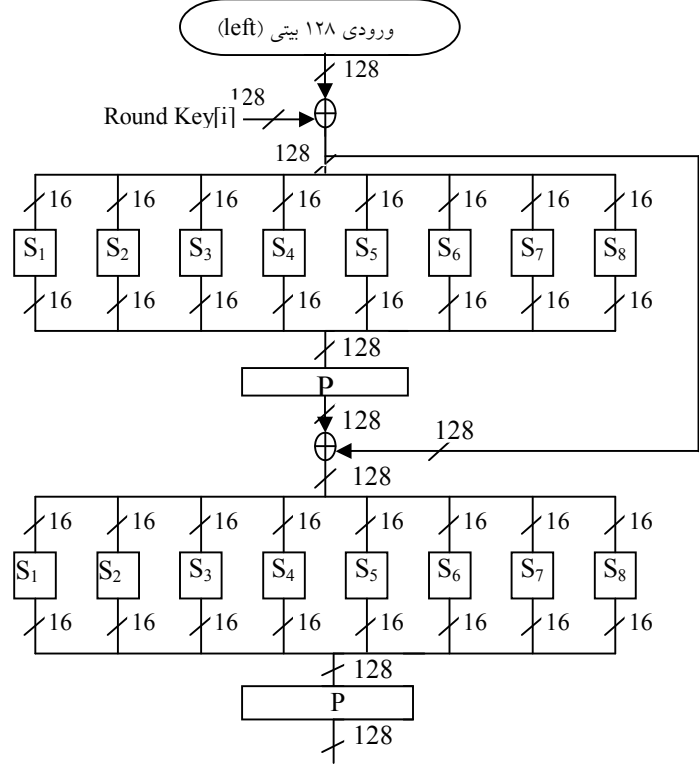
³ Primitive

⁴ Binary Code

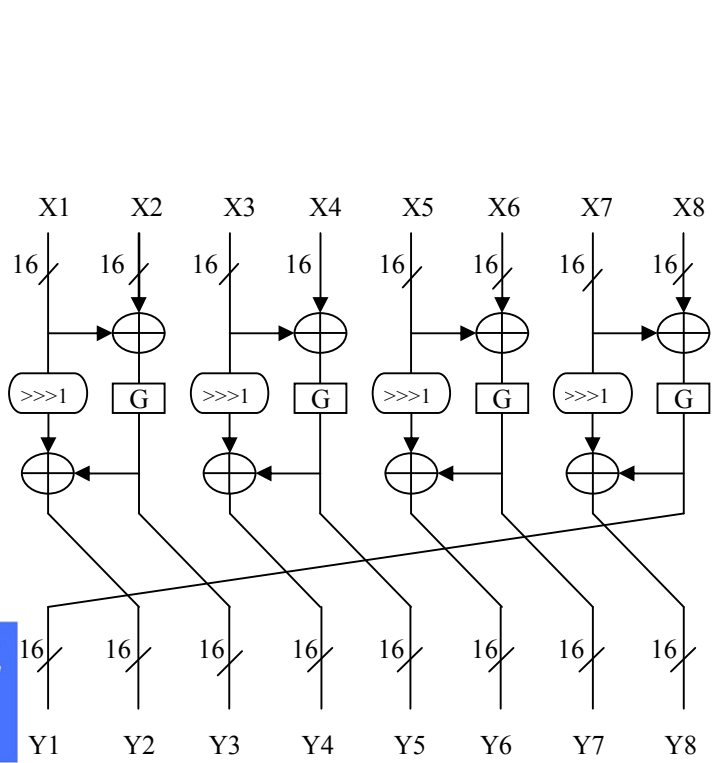
⁵ Gray Code



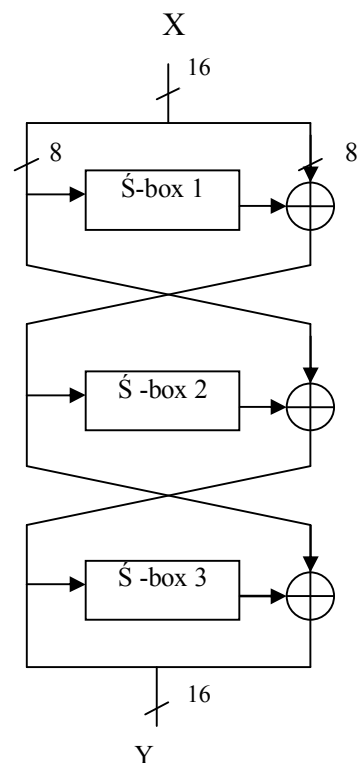
شکل ۱: نمودار کلی فرآیند الگوریتم



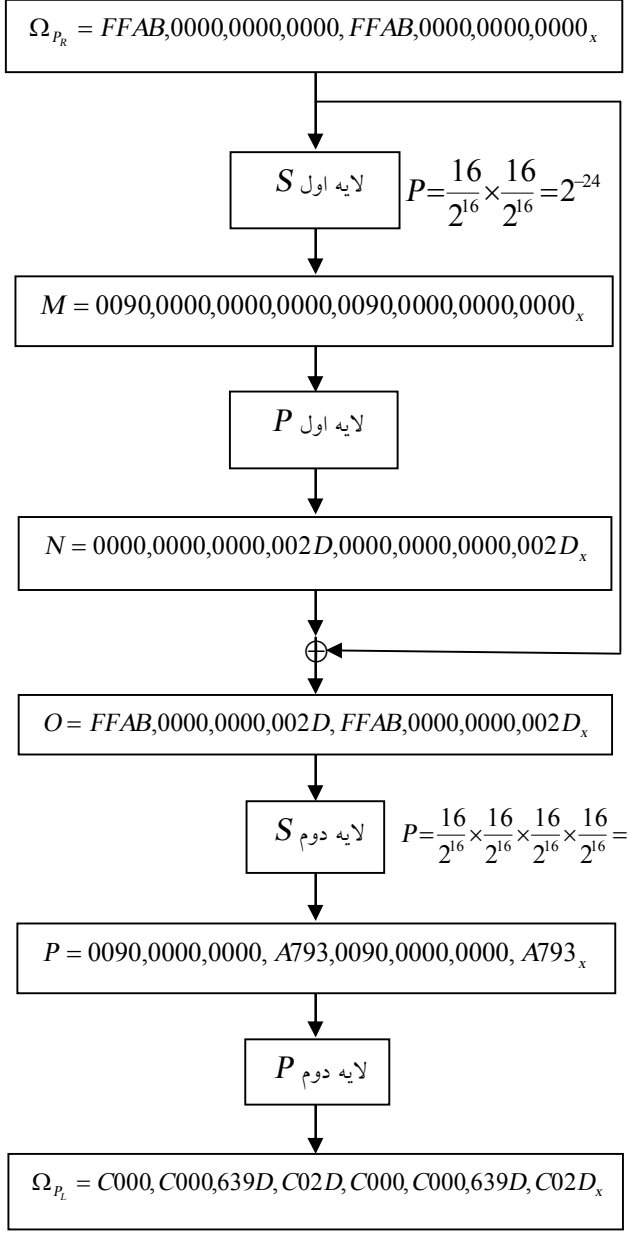
شکل ۲: تابع دور F در هسته اصلی فرآیند الگوریتم



شکل ۴: یک دور از لایه بهم ریختگی P

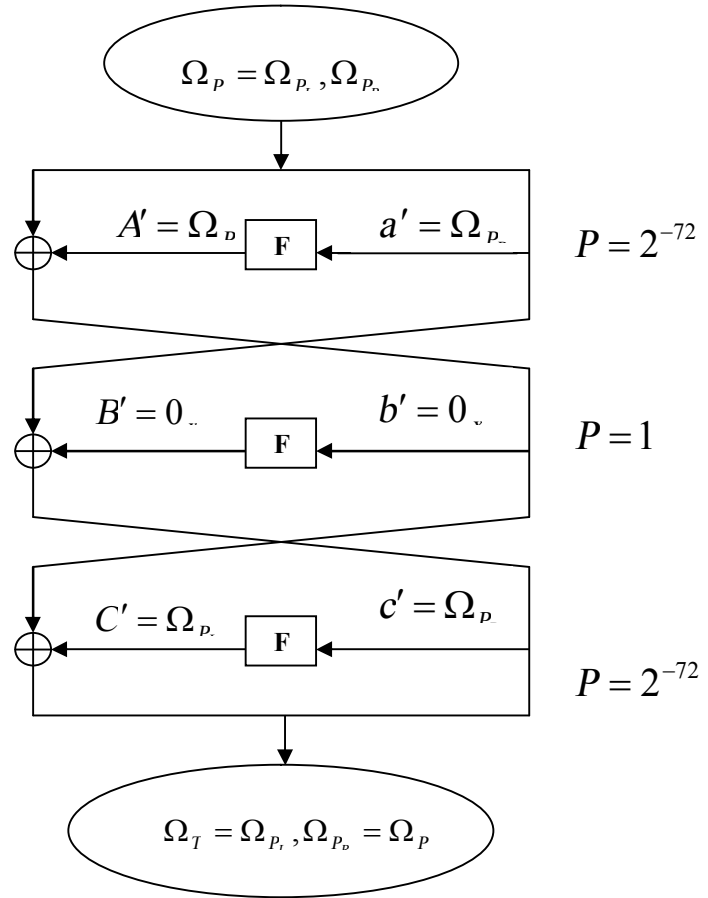


شکل ۳: ساختار جعبه‌های جانشینی بکاررفته در تابع دور F (S₈ تا S₁)



شکل ۶: نحوه به دست آمدن احتمال دورهای اول و سوم مشخصه سه دوری الگوریتم فجر ۲

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



شکل ۵: مشخصه سه دوری الگوریتم فجر ۲

جدول ۳: مقایسه پارامترهای مهم دو الگوریتم فجر ۱ و فجر ۲

ردیف	پارامتر	الگوریتم فجر ۱	الگوریتم فجر ۲	میزان بهبودی
۱	امنیت تفاضلی جعبه های 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	$2^{-99.6}$	$2^{-418.2}$	$2^{-318.6}$
۴	عدد انشعاب لایه P	1	4	4
۵	احتمال مشخصه تفاضلی سه دوری	$2^{-24.8}$	2^{-144}	$2^{-119.2}$

شده یک جایگشت می‌باشد. با روش پیاده‌سازی، عدد انشعاب لایه P در الگوریتم فجر ۲ برابر $\beta(p) = 4$ به دست آمد. از طریق روش امنیت قابل اثبات، پارامتر امنیت تفاضلی الگوریتم ۱۶ دوری فجر ۲ به میزان $\frac{2^{-418.2}}{2^{-99.6}} = 2^{-318.6}$ 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 فجر ۱ به میزان $2^{-119.2}$ بهتر شده است. نتایج ارزیابی آماری الگوریتم فجر ۲ 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، شبیه‌سازی و ارزیابی یک الگوریتم رمز قالبی جدید؛ مسعود فرهنگی؛ پایان‌نامه کارشناسی ارشد رمز، دانشگاه امام حسین علیه السلام، پائیز ۱۳۸۲.
- [۲] ارزیابی و تحلیل تفاضلی الگوریتم رمز قطعه‌ای فجر ۱؛ محسن رمضان یارندی؛ پایان‌نامه کارشناسی ارشد رمز؛ دانشگاه امام حسین علیه السلام؛ پائیز ۱۳۸۳.
- [۳] حمله تفاضلی کارآمد به الگوریتم رمز قطعه‌ای فجر ۱؛ 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 I. 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

فعالی وجود ندارد. این مشخصه تکرار پذیر نمی‌باشد و با احتمال 2^{-144} حاصل می‌شود. امکان به دست آوردن مشخصه دو دوری تکرار پذیر وجود ندارد. زیرا در مشخصه‌های دو دوری تکرار پذیر، به ازای XOR ورودی به تابع F باید XOR خروجی صفر داشته باشیم و این در مورد الگوریتم فجر ۲ که فقط به ازای XOR ورودی تمام صفر به لایه S و P، XOR خروجی نیز تمام صفر می‌شود، دست یافتنی نمی‌باشد. به دست آوردن مشخصه‌های تفاضلی برای دوره‌های بالاتر امکان پذیر است اما به دست آوردن این مشخصه‌ها با احتمال مناسب اهمیت زیادی دارد. شکل‌های ۵ و ۶ مشخصه سه دوری ونحوه به دست آمدن احتمال آنرا نشان می‌دهند. در هر دور، تفاضلات ورودی از دو لایه SP عبور می‌کنند. همان طور که در شکل ۶ مشاهده می‌شود، در دوره‌های اول و سوم برای لایه اول S فقط ورودی S-box های ۱ و ۵ 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 نیز فقط ورودی S-box های ۱، ۴، ۵ و ۸ ناصفر بوده و با احتمال $p = \frac{16}{2^{16}} = 2^{-12}$ خروجی مورد نظر هر S-box ساخته می‌شوند. در لایه P هر تفاضل ورودی فقط یک تفاضل خروجی دارد و در نتیجه احتمال مشخصه دور اول و سوم هر کدام برابر $2^{-72} = 2^{-48} \times 2^{-24}$ به دست می‌آید. در نتیجه مشخصه تفاضلی سه دوری الگوریتم اصلاح شده فجر ۲ برابر با $2^{-144} = 2^{-72} \times 2^{-72} = P_T$ می‌شود. این در حالی است که مشخصه تفاضلی سه دوری الگوریتم فجر ۱ همانطور که در مرجع [۳] آمده مشابه مشخصه دو دوری تکرار پذیر آن و برابر با $P = 2^{-24.8}$ است و این اعداد نشان دهنده بهبود چشمگیری در الگوریتم اصلاح شده فجر ۲ می‌باشد.

۶- نتیجه گیری

در این مقاله نشان داده شد که با اصلاح جعبه جانشینی S'_1 و تبدیل $G(x)$ در الگوریتم فجر ۱ می‌توان به مشخصه‌های تفاضلی بسیار مناسب‌تری رسید. همچنین ثابت شد تابع اصلاح شده $G^*(x)$ یک به یک و پوشا است و در نتیجه لایه P اصلاح