نشریه علمی "پدافند الکترونیکی و سایبری"
سال هفتم، شماره ۲، تابستان ۱۳۹۸، ص ۷۹-۶۹

# تحلیل تفاضل ناممکن الگوریتم رمزقالبی LowMC

هادی سلیمانی[1*]، علیرضا مهرداد[2]
۱- استادیار، گروه امنیت شبکه و رمزنگاری، پژوهشکده فضای مجازی، دانشگاه شهید بهشتی، تهران،
۲- کارشناس ارشد مخابرات امن و رمزنگاری، پژوهشکده فضای مجازی، دانشگاه شهید بهشتی، تهران
(دریافت: ۹۷/۰۳/۰۶، پذیرش: ۹۷/۰۷/۲۱)

## چکیده

تحلیل تفاضل ناممکن یک ابزار قوی برای ارزیابی امنیت رمزهای قالبی به‌شمار می‌آید. در رمزهای قالبی که بر مبنای ساختار شبکه جانشینی- جایگشتی بنا شده‌اند، تنها لایه‌ای که در برابر تفاضل از خود مقاومت نشان می‌دهد، لایه غیرخطی است. بدیهی است توجه به خصوصیات لایه غیرخطی در جلوگیری اعمال حملات آماری نظیر حمله تفاضلی از اهمیت بالایی برخوردار است. بنابراین، ویژگی‌های این لایه برای مقاومت در برابر این حمله باید به دقت مورد بررسی قرار بگیرد. وجود چنین لایه غیرخطی با توجه به ویژگی‌های مورد نیاز و اعمال آن به تمام طول قالب می‌تواند باعث مقاومت بیشتر الگوریتم در مقابل حمله تفاضلی شود. طی سالیان اخیر دسته جدیدی از رمزهای قالبی بر مبنای ساختار شبکه جانشینی ـ جایگشتی معرفی شده‌اند که در آنها لایه غیرخطی تنها به بخشی از قالب اعمال می‌شود. در این مقاله چارچوبی عمومی برای یافتن مشخصه‌های تفاضل ناممکن در این دسته از رمزهای قالبی نوین ارائه می‌شود. برخلاف روش‌های فقدان در میانه پیشین که برای یافتن مشخصه‌های تفاضل ناممکن استفاده شده است، روش ارائه‌شده در این مقاله مستقل از مشخصات لایه خطی الگوریتم رمزنگاری است و به مهاجم اجازه می‌دهد که برای الگوریتم‌های رمزنگاری با لایه خطی بسیار پیچیده به‌صورت سیستماتیک مشخصه‌های تفاضل ناممکن موثری را پیدا کند. به منظور نشان دادن کارائی روش ارائه‌شده، خانواده رمزهای قالبی LowMC که از لایه‌های خطی بیت محور استفاده می‌کنند را در این مقاله مورد بررسی قرار داده و براساس چارچوب ارائه‌شده در مقاله، مشخصه‌های تفاضل ناممکن متعددی برای نسخه‌های کاهش یافته LowMC ارائه کرده‌ایم. مشخصه‌های تفاضل ناممکن به‌دست‌آمده می‌تواند به راحتی در حملات بازیابی کلید به‌کار روند. به‌عنوان نمونه نشان می‌دهیم که براساس مشخصه تفاضل ناممکن به‌دست‌آمده برای ۶۳ دور الگوریتم LowMC(128,128,2,128)، یک حمله بازیابی کلید به ۶۴ دور الگوریتم قابل اعمال است. در حمله ارائه شده، پیچیدگی حافظه $2^{89}$، پیچیدگی زمانی برابر $2^{123.7}$ و پیچیدگی داده برابر با $2^{123.1}$ متن منتخب است.

**کلیدواژه‌ها: رمز قالبی، تحلیل رمز، تحلیل تفاضل ناممکن، الگوریتم رمز قالبی LowMC.**

## ۱- مقدمه

### ۱-۱- اولیه‌های نوین رمزنگاری

رشد سریع فناوری در حوزه فناوری اطلاعات، به‌همراه طرح مفاهیم نوینی چون اینترنت اشیاء و همچنین گستره روزافزون کاربران و تنوع سرویس‌های جدید اینترنتی (همچون شبکه‌های پیچیده اجتماعی، سرویس‌های ابری و غیره)، سبب ایجاد چالش‌ها و در نتیجه نیازهای امنیتی جدیدی شده است. با توجه به پیشرفت‌های عظیم در حوزه فناوری اطلاعات و ارتباطات، صورت مسئله‌های جدیدی در این حوزه طرح شده است که جامعه رمزنگاری جهانی تلاش کرده است با ارائه طرح‌های نوین به این نیازها پاسخ دهد. رمزنگاری مدرن راه‌کارهای نوینی را به منظور حل مسائل قدیمی در ارتباطات امن دوطرفه ارائه کرده است. پروتکل‌های محاسبات چندجانبه امن[1]، اثبات‌های هیچ‌آگاهی[2] و طرح‌های رمزنگاری هم‌ریختی کامل از برجسته‌ترین طرح‌های نوین می‌باشد. به طور خاص در سال‌های اخیر پروتکل‌های محاسبات چندجانبه امن از موضوعی صرفا نظری به موضوعی عملی تبدیل شده‌اند. در همین چارچوب مشاهده شده است که اولیه‌های رمزنگاری متقارن همچون AES برای این پروتکل‌ها مناسب نیستند [۲۱]. این مسئله سبب شده است که علم رمزنگاری به سرعت رشد کرده و براساس نیازهای جدید، اولیه‌های جدید رمزنگاری طراحی شوند. با استفاده از اولیه‌های نوین رمزنگاری که خواص ویژه‌ای دارند می‌توان به‌طور

*رایانامه نویسنده مسئول: h_soleimany@sbu.ac.ir

1- Multi party computation
2- Zero knowledge proof

قابل توجهی، کارائی طرح‌های نوینی نظیر طرح‌های MPC را افزایش داد.

در حوزه طرح‌های رمزنگاری مدرن مانند FHE[1] و MPC[2]ها، اولیه‌های رمزنگاری متقارنی باید به‌کار روند که در آنها تعداد ANDها[3] و همچنین عمق آنها[4] کم باشد. اکثر قریب به اتفاق اولیه‌های نوینی طی سالیان گذشته طراحی و ارائه شده‌اند به منظور حصول ویژگی‌های خاصی که در بالا ذکر شد، از ساختارهای نامتعارفی در مقایسه با رمزهای کلاسیک استفاده می‌کنند. در این حوزه می‌توان از رمزهای متقارن نوینی همچون LowMC [۱]، Kreyvium [۲]، Flip [۳]، MiMC [۴] و Rasta [۵] نام برد. این دسته از رمزها مشابه رمزهائی نظیر Zorro هستند که به منظور مقابله با حملات کانال جانبی طراحی شده‌اند [۶]. امنیت الگوریتم Zorro پیش از این به صورت گسترده مورد بررسی قرار گرفته است و نشان داده شده است که این الگوریتم رمز قالبی امنیت مناسبی ندارد [۱۰-۷]. این درحالی است که سایر الگوریتم‌های ذکرشده تاکنون مقاومت مناسبی در مقابل حملات ارائه‌شده از خود نشان داده‌اند.

نکته قابل توجه در الگوریتم‌های رمزنگاری نوین ذکر شده مانند LowMC این است که برخلاف کاربردهای عمومی، هزینه لایه خطی در مقابل اجزای غیرخطی قابل چشم پوشی است. برهمین اساس می‌توان اولیه‌هایی را طراحی و به کار برد که لایه خطی آنها بسیار سنگین است. هدف از این مقاله بررسی ساختارمند تحلیل تفاضل ناممکن LowMC مستقل از لایه خطی است.

## ۱-۲- کارهای پیشین

اولین نسخه از الگوریتم رمزنگاری LowMC در Eurocrypt 2015 ارائه شد [۱]. پس از مدتی در دو مقاله به‌صورت موازی نشان داده شد که برخی از نسخه‌های LowMC در مقابل تحلیل تفاضل مرتبه بالا امن نیستند [۱۲-۱۱]. برهمین اساس طراحان LowMC اقدام به تغییر نحوه محاسبه تعداد دورهای الگوریتم کرده و نسخه جدید LowMC را منتشر کردند [۱۳]. الگوریتم LowMC که برای کاربرد در طرح‌های FHE و MPC طراحی شده بود، به مرور مشخص شد که می‌تواند در بسترهای دیگر نیز مورد استفاده قرار گیرد. به‌طور مشخص طی دو سال گذشته طرح‌های پساکوانتوم جدیدی که مطرح شده‌اند از اولیه رمزنگاری LowMC استفاده می‌کنند [۱۶-۱۴]. در این طرح‌ها نسخه‌های خاصی از LowMC به‌کار رفته است که تعداد جعبه‌های جانشانی در هر دور بسیار کم است اما در مقابل تعداد دورهای آن بسیار زیاد است. به همین خاطر تحلیل تفاضل مرتبه بالا ارائه‌شده در مقالات [۱۲-۱۱] قابل اعمال به دورهای کاهش یافته این الگوریتم‌ها نیست. علاوه‌بر این، باید به این نکته اشاره کرد که علی‌رغم کاربردهای متعدد LowMC به جز تحلیل تفاضل مرتبه بالا ارائه شده در مقالات [۱۲-۱۱]، حملات دیگری به این الگوریتم نشده است. یکی از مهمترین دلائل این حقیقت این است که لایه خطی به‌کار رفته در LowMC یک ماتریس بیتی تصادفی بسیار پیچیده است. برهمین اساس بررسی امنیت LowMC در مقابل تحلیل‌های دیگر موضوعی مهم به نظر می‌رسد که مهمترین چالش در این حوزه لایه خطی به‌کار رفته است. هدف از این مقاله بررسی تحلیل تفاضل ناممکن LowMC مستقل از لایه خطی به‌کار رفته در آن است. در این حوزه می‌توان به تحقیق مشابهی بر روی الگوریتم Zorro اشاره کرد که امنیت Zorro را در مقابل تحلیل‌های تفاضلی و خطی به صورت ساختاری مورد بررسی قرار داده است [۱۷]. تفاوت اصلی مقاله حاضر با مقاله [۱۷] این است که در این مقاله ما تحلیل تفاضل ناممکن را بررسی می‌کنیم این در حالی است که مقاله [۱۷] روشی را برای یافتن تحلیل‌های تفاضلی و خطی ارائه می‌کند (که الگوریتم LowMC در مقابل آنها امنیت بالائی دارد). همچنین روش ارائه شده در مقاله ما مستقل از لایه خطی است و این در حالی است که نتائج حاصله در مقاله [۱۷] وابسته به لایه خطی است.

## ۱-۳- نوآوری مقاله

اجزای به‌کار رفته در طراحی این الگوریتم‌های نوین عموما متفاوت از اجزائی است که در رمزهای متداول گذشته استفاده شده‌اند. بدیهی است استفاده از ساختارها و اجزاهای جدید سبب به‌وجود آمدن سوالات جدیدی می‌شود. پاسخ به این سوالات معمولا به سادگی امکان‌پذیر نمی‌باشد و با چالش‌های نظری جدیدی مواجه هستیم که مستلزم بررسی‌های جدید امنیتی می‌باشند. به‌علاوه باید دقت کرد که به‌علت استفاده از ساختارها نامتعارف و یا اجزای داخلی جدید در اولیه‌های نوین رمزنگاری، ممکن است این اولیه‌ها در مقابل حملات جدیدی آسیب‌پذیر باشند که الگوریتم‌های کلاسیک دارای این ضعف‌ها نباشند. برهمین اساس تغییرات اساسی در نحوه طراحی‌ها احتیاج به بررسی‌های امنیتی گسترده و جدی‌تری دارد. امروزه با توجه به ارائه طرح‌های متعدد طی سالیان گذشته بحث تحلیل این اولیه‌ها توجه تعداد زیادی از محققین را به خود جلب کرده است.

در این مقاله، روشی کارا و متفاوت برای یافتن مشخصه‌های تفاضل ناممکن رمزهای قالبی بر مبنای ساختار SPN که در آن لایه غیرخطی تنها به بخشی از قالب اعمال می‌شود، ارائه شده است. ویژگی مشترک رمزهای قالبی مورد بحث این است که لایه غیرخطی فقط به بخشی از قالب‌های درونی اعمال می‌شود و تمام

1- Fully Homomorphic Encryption
2- Multi-Party Computation
3- Multiplicative complexity
4- Multiplicative depth

قالب را در بر نمی‌گیرد. ویژگی مهم تحلیل ارائه شده این است که این حمله مستقل از ویژگی‌های لایه خطی و غیرخطی الگوریتم و به‌طور کلی مستقل از ویژگی‌های عناصر درونی الگوریتم، می‌تواند به تمام رمزهای با ساختار مشابه، صرفا به دلیل ویژگی لایه غیرخطی جزیی[1] اعمال شود. روش ارائه‌شده بر مبنای تحلیل فقدان در میانه[2] بیان شده و مشاهده اصلی در این روش این است که تعداد تفاضل‌های ممکن که در حالت میانی الگوریتم ممکن است اتفاق بیافتد، بسیار محدود است. ما ابتدا نشان می‌دهیم که ویژگی جزیی بودن لایه غیرخطی چگونه می‌تواند برای ساخت مشخصه‌های موردنظر به کار آید سپس به وسیله تحلیل فقدان در میانه، مشخصه‌ی تفاضل ناممکن را برای الگوریتم‌های مورد نظر در حالت کلی به‌دست می‌آوریم.

سپس با استفاده از روش توصیف شده، نشان می‌دهیم که می‌توان به صورت مصداقی برای خانواده رمزهای قالبی LowMC، *مستقل از ویژگی‌های لایه خطی الگوریتم*، این حمله را بر روی این الگوریتم پیاده‌سازی کرد و مشخصات تفاضل ناممکن کارایی به دست آورد. لازم به ذکر است که به دلیل ساختار بسیار پیچیده لایه خطی در رمز قالبی LowMC امکان اعمال حملات تفاضل ناممکن پیشین به این رمز امکان‌پذیر نیست.

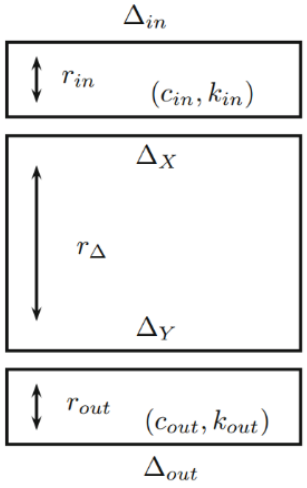
### ۱-۴- ساختار مقاله

در این مقاله ابتدا در بخش ۲، تحلیل تفاضل ناممکن و روش فقدان در میانه توضیح داده شده است. در بخش ۳، رمزهای قالبی با ساختار SPN با لایه غیر خطی جزیی بررسی شده است و در ادامه روش اعمال حمله به این رمزها توضیح داده شده است. در ادامه الگوریتم رمز قالبی LowMC به طور کلی توضیح داده می‌شود. پس از آن نحوه یافتن مشخصه تفاضل ناممکن در مدل جدید تشریح می‌شود. در ادامه چارچوبی به منظور پیدا کردن مشخصه‌های تفاضل ناممکن در LowMC ارائه می‌شود. سپس در بخش ۴، روش به‌دست آوردن مشخصه‌های تفاضل ناممکن به صورت مصداقی برای چند مورد بررسی می‌شود و نتایج اعمال حملات بر روی چند حالت مختلف LowMC را با استفاده از مدل ارائه شده در بخش ۲، شرح می‌دهیم. در نهایت در بخش ۵، به جمع‌بندی مقاله پرداخته شده است.

## ۲- تحلیل تفاضل ناممکن

### ۲-۱- ساختار کلی حملات تفاضل ناممکن

تحلیل تفاضل ناممکن به‌طور مستقل توسط نادسن[3] و بیهام[4] و همکارانش به ترتیب در [۱۸-۱۹] معرفی شده‌اند. تحلیل تفاضل ناممکن به‌طور گسترده برای حمله به الگوریتم‌های رمز قالبی مورد استفاده قرار گرفته است [۲۰]. برخلاف تحلیل تفاضلی که اساس آن یافتن مشخصه‌های تفاضلی با احتمال بالا است، تحلیل تفاضل ناممکن از تفاضل‌هایی استفاده می‌کند که احتمال وقوع آن صفر است. دو گام عمده در تحلیل تفاضل ناممکن با اهمیت است. گام اول یافتن یک مشخصه تفاضل ناممکن با طول حداکثری است به‌طوری‌که تفاضل ورودی آن $\Delta_X$ و تفاضل خروجی $\Delta_Y$ باشد. یعنی احتمال آن‌که تفاضل ورودی $\Delta_X$ بعد از $r_\Delta$ دور، به تفاضل خروجی $\Delta_Y$ منجر شود، صفر باشد یا $\Pr\left[\Delta_X \xrightarrow{r_\Delta} \Delta_Y\right] = 0$. گام دوم، استفاده از مشخصه تفاضل ناممکن به‌عنوان یک تمایزگر به‌منظور بازیابی (بخشی از) زیرکلیدهای دور است که مرحله تصفیه کردن[5] کلید نیز نامیده می‌شود. در حالت کلی، الگوریتم رمزنگاری $r_{in} + r_{out} + r_\Delta$ دوری را در نظر می‌گیریم (با اضافه کردن $r_{in}$ دور به ابتدا و $r_{out}$ دور به انتهای مشخصه تفاضل ناممکن). سپس تعدادی زوج متن اصلی و متن‌های رمزشده معادل آن‌ها در نظر گرفته می‌شوند. سپس (بخشی از) زیرکلیدهای دورهای ابتدایی و انتهایی حدس زده می‌شوند و زوج متن‌های اصلی داده شده برای $r_{in}$ دور اول رمزنگاری و زوج متن‌های رمزشده معادل آنها برای $r_{out}$ دور آخر رمزگشایی می‌شوند. در این حالت اگر به ازای یک کلید حدس زده شده، یکی از زوج متن‌های اصلی به تفاضل $\Delta_x$ در دور $r_{in}$ام و زوج متن رمزشده‌ی معادل آن به تفاضل $\Delta_y$ در انتهای دور $(r_{in} + r_\Delta)$ام منجر شود، می‌توان نتیجه گرفت که کلید حدس زده شده غلط است و باید آن را از فضای کاندیدهای احتمالی کلید حذف کرد. روند کلی حمله تفاضلی ناممکن در شکل (۱) ارائه شده است.

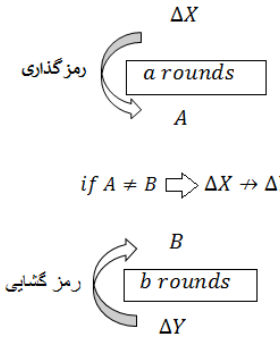



**شکل (۱):** ساختار حمله تفاضلی ناممکن.

1- Partial-nonlinear layer
2- Miss-in-the-Middle
3- Knudsen
4- Biham
5- Filtering

### ۲-۲- یافتن مشخصه تفاضل ناممکن

یافتن تفاضل ناممکن، معمولا به روش فقدان در میانه[1] انجام می‌شود. در این روش ابتدا یک مشخصه تفاضلی همچون $\Delta X \xrightarrow{a \text{ rounds}} A$ برای $a$ دور از الگوریتم با احتمال ۱ در جهت رمزگذاری پیدا می‌کنیم. سپس به صورت مشابه یک مشخصه تفاضلی همچون $B \xrightarrow{b \text{ rounds}} \Delta Y$ برای $b$ دور از الگوریتم با احتمال ۱ در جهت رمزگشائی پیدا می‌کنیم. اگر بتوان نشان داد که تفاضل‌های $A$ و $B$ هیچ‌گاه نمی‌توانند با هم برابر باشند، می‌توان نتیجه گرفت که مشخصه تفاضلی $(a+b)$ دوری $\Delta X \xrightarrow{(a+b) \text{ rounds}} \Delta Y$، یک تفاضل ناممکن خواهد بود شکل (۲).




**شکل (۲):** روش فقدان در میانه برای یافتن مشخصه تفاضل ناممکن.

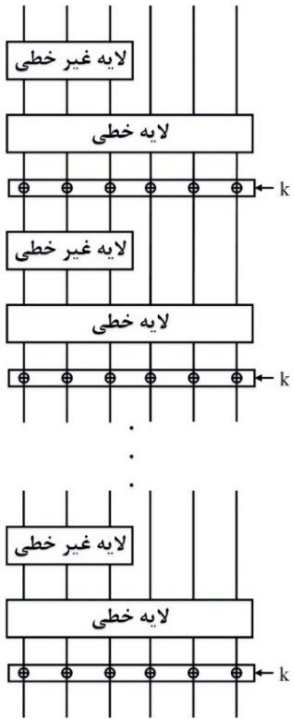
دسته گسترده‌ای از مشخصه‌های تفاضل ناممکن که با استفاده از روش فقدان در میانه به دست می‌آیند، از این ویژگی استفاده می‌کنند که در صورت انتخاب هوشمندانه تفاضل‌های ورودی و خروجی یک مشخصه تفاضلی، برخی بیت‌های تفاضل در حالت میانی الگوریتم با احتمال ۱ برابر تفاضل صفر می‌شوند. برهمین اساس اگر لایه خطی به‌گونه‌ای طراحی شود که تغییر هر کدام از بیت‌های ورودی منجر به تاثیرپذیری تمامی بیت‌های حالت میانی پس از $r$ دور شود. در این حالت اصطلاحا می‌گویند که الگوریتم پس از $r$ دور به انتشار کامل می‌رسد که در این حالت می‌توان به صورت تقریبی انتظار داشت که طول بهترین مشخصه تفاضلی ممکن حدود $2r$ دور است. به‌عنوان مثال الگوریتم رمزنگاری استاندارد AES پس از دو دور به انتشار کامل می‌رسد و بهترین مشخصه تفاضل ناممکن ارائه‌شده برای AES چهاردوری است [۲۲].

بدیهی است که روش مذکور به شدت به ساختار الگوریتم وابسته است و با افزایش پیچیدگی لایه خطی، اعمال آن ممکن نیست. ما در بخش بعد نشان می‌دهیم که چگونه می‌توان از روش فقدان در میانه در تحلیل الگوریتم‌های رمز قالبی SPN با لایه غیرخطی جزیی استفاده نمود.

## ۳- تحلیل تفاضل ناممکن رمزهای قالبی SPN با لایه غیرخطی جزیی

### ۳-۱- رمز قالبی SPN با لایه غیرخطی جزیی

رمزهای قالبی عموما از تکرار توابعی معکوس‌پذیر به نام دور تشکیل شده‌اند. هر دور، تابعی وابسته به کلید به شکل $\mathcal{R}_i(sk_i, X_i)$ است که مقدار ورودی $b$ بیتی $X_i$ را با استفاده از زیرکلید دور $sk_i \in \mathbb{F}_2^b$ به مقدار خروجی $b$ بیتی $X_{i+1}$ منتقل می‌کند. ساختار توابع دور در بسیاری از رمزهای قالبی بر پایه ساختار SPN طراحی شده‌اند. دور $i$ام از رمزهای قالبی با ساختار شبکه SPN شامل سه بخش می‌باشد: لایه غیرخطی $(\mathcal{S})$، لایه خطی $(\mathcal{L}_i)$ و عمل اضافه شدن زیرکلید دور است که عموما زیرکلید دور با استفاده از عملگرد xor اضافه می‌شود. رمزهای قالبی با ساختار شبکه SPN با لایه غیرخطی جزیی، به دسته‌ای از رمزهای قالبی اطلاق می‌شود که لایه غیرخطی در آن‌ها فقط به بخشی از قالب درونی (و نه همه‌ی قالب) اعمال می‌شود. به عنوان یک راهبرد مرسوم، لایه غیرخطی از $m$ جعبه جانشانی $n$ بیتی تشکیل می‌شود که در رمزهای با لایه غیرخطی جزیی $b > n \times m$ می‌باشد. به عبارت دیگر تنها $n \times m$ بیت از قالب از لایه غیرخطی عبور می‌کند و مابقی $b - n \times m$ بیت از لایه غیرخطی عبور نمی‌کنند. شکل ساده و شمای کلی اجرای عملیات رمزگذاری در الگوریتم‌های مذکور به صورت خلاصه در شکل (۳) قابل مشاهده است.




**شکل(۳):** رمز قالبی SPN با لایه غیرخطی جزیی.

1- Miss-in-the-middle

### ۳-۲- توصیف خانواده رمزهای قالبی LowMC

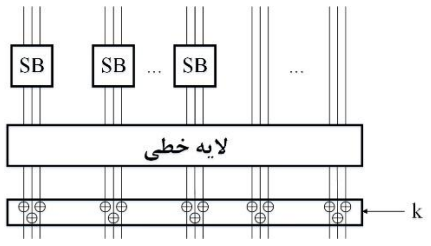
الگوریتم LowMC یک خانواده از رمزهای قالبی با طول قالب، طول کلید، داده‌های مجاز، تعداد دورها و نیز تعداد جعبه‌های جانشینی متنوع است.

**جدول (۱):** حالت‌های مختلف الگوریتم رمزنگاری LowMC.

| ردیف | طول قالب ($b$) | تعداد جعبه‌های جانشینی ($m$) | طول کلید ($k$) | داده‌های مجاز ($d$) | تعداد دور (r) |
|---|---|---|---|---|---|
| ۱ | ۲۵۶ | ۴۹ | ۸۰ | ۶۴ | ۱۲ |
| ۲ | ۱۲۸ | ۳۱ | | | ۱۲ |
| ۳ | ۶۴ | ۱ | | | ۱۶۴ |
| ۴ | ۱۰۲۴ | ۲۰ | | | ۴۵ |
| ۵ | ۱۰۲۴ | ۱۰ | | | ۸۵ |
| ۶ | ۲۵۶ | ۶۳ | ۱۲۸ | ۱۲۸ | ۱۴ |
| ۷ | ۱۹۶ | ۶۳ | | | ۱۴ |
| ۸ | ۱۲۸ | ۳ | | | ۸۸ |
| ۹ | ۱۲۸ | ۲ | | | ۱۲۸ |
| ۱۰ | ۱۲۸ | ۱ | | | ۲۵۲ |
| ۱۱ | ۱۰۲۴ | ۲۰ | | | ۴۹ |
| ۱۲ | ۱۰۲۴ | ۱۰ | | | ۹۲ |
| ۱۳ | ۵۱۲ | ۶۶ | ۲۵۶ | ۲۵۶ | ۱۸ |
| ۱۴ | ۲۵۶ | ۱۰ | | | ۵۲ |
| ۱۵ | ۲۵۶ | ۱ | | | ۴۵۸ |
| ۱۶ | ۱۰۲۴ | ۱۰ | | | ۱۰۳ |

یک دور این الگوریتم را می‌توان به صورت رابطه (۱) خلاصه کرد که در شکل (۴) قابل مشاهده است.

$$LowMCRound(i) = AK \circ AC_i \circ L_i \circ SB \qquad (۱)$$




**شکل(۴):** الگویتم رمزنگاری LowMC.

در ابتدای هر دور $m$ جعبه جانشینی یکسان ۳ بیتی به حالت[1] اعمال می‌شود (عمل SB). ساختار LowMC بدین صورت است که لایه غیرخطی SB تنها به بخشی از قالب اعمال می‌شود. به‌عبارت دیگر همیشه طول قالب بیشتر از $3m$ است (یعنی $3m < b$ است). از آنجایی‌که تحلیل‌های ارائه‌شده در این مقاله مستقل از خواص جعبه جانشینی است، از تعریف S-box استفاده‌شده در LowMC خودداری کرده و علاقمندان را به [۱] ارجاع می‌دهیم. پس از آن لایه خطی اعمال می‌شود. لایه خطی در هر دور، یک ماتریس بیتی تصادفی $b \times b$ به نام $L_i$ است که در حالت ضرب شده و محاسبات در $GF(2)$ محاسبه می‌شود. لازم به‌ذکر است مقادیر ماتریس‌های به‌کار رفته در هر دور متفاوت است. در انتهای هر دور عملیات اضافه شدن مقدار ثابت دور و مقدار کلید صورت می‌پذیرد که در فرمول ۱، به ترتیب با AK و $AC_i$ نشان داده شده‌اند. لازم به‌ذکر است که کلید تمامی دورها برابر با کلید اصلی بوده ولی مقدار ثابت دورها متفاوت بوده و به صورت تصادفی تولید می‌شوند.

در جدول (۱)، پارامترهای برخی از نمونه‌های LowMC قابل مشاهده است. در این جدول، $b$ نشان‌دهنده طول قالب، $m$ نشان‌دهنده تعداد جعبه‌های جانشانی، $k$ طول کلید و $r$ تعداد دورهای الگوریتم می‌باشند. با توجه به آن‌که LowMC برای کاربردهای خاص استفاده می‌شود، طراحان برای هر مصداق از الگوریتم LowMC در نظر گرفته‌اند که حداکثر تعداد $2^d$ متن توسط کاربر رمز می‌شود. به عبارت دیگر مقدار $d$ نشان‌دهنده این است که تحت یک کلید ثابت، کاربر می‌تواند حداکثر تعداد $2^d$ متن متفاوت را رمز کند بدون این‌که امنیت الگوریتم به خطر بیافتد. هر کدام از اعضای خانواده رمزهای قالبی LowMC را با در نظر گرفتن پارامترهای مذکور با $\text{LowMC}(b,k,m,d)$ نمایش می‌دهیم.

### ۳-۳- ویژگی‌های مشخصه‌های تفاضلی در رمزهای قالبی SPN با لایه غیرخطی جزیی

در این بخش ابتدا چند ویژگی در خصوص مشخصه‌های تفاضلی رمزهای قالبی SPN با لایه غیرخطی جزیی معرفی می‌کنیم. این ویژگی‌ها در بخش بعدی به‌منظور به‌دست آوردن مشخصه‌های تفاضل ناممکن برای یک رمز قالبی دلخواه با ساختار SPN و لایه غیرخطی جزیی به کار خواهد رفت.

**قضیه ۱.** مستقل از لایه خطی استفاده شده در یک رمز قالبی SPN با لایه غیرخطی جزیی، به طور متوسط $2^{b-n\times m\times R}$ مشخصه تفاضلی با احتمال یک برای $R$ دور از الگوریتم وجود دارد. به عبارت دیگر داریم:

$$\left|\{\Delta_{in}\in \mathbb{F}_2^{128} \mid \boldsymbol{Pr}[\Delta_{in}\rightarrow \boldsymbol{\mathcal{L}_R}\cdots\boldsymbol{\mathcal{L}_1}(\Delta_{in})]=\mathbf{1}\}\right| = \mathbf{2^{b-128\times m\times R}} \qquad (۲)$$

که در آن، $\mathcal{L}_i$ نشان‌دهنده لایه خطی (دلخواه) دور $i$ام است. رابطه مشابه‌ای نیز برای عمل رمزگشائی صادق است.

**اثبات:** اگر مقدار تفاضل ورودی تمامی جعبه‌های جانشانی در تمامی $R$ دور برابر صفر باشد (به عبارت دیگر تمام جعبه‌های

1- state

جانشانی غیرفعال باشند)، مشخصه تفاضلی با احتمال ۱ صادق است. احتمال این‌که مقدار تفاضل ورودی یک جعبه جانشانی $n$ بیتی برابر 0 باشد، به‌طور متوسط برابر $2^{-n}$ است. از طرفی تعداد جعبه‌های جانشانی در $R$ دور الگوریتم برابر $m \times R$ است چرا که در هر دور $m$ جعبه جانشانی وجود دارد. بنابراین، احتمال صفر بودن تفاضل‌های ورودی تمامی $R \times n \times m$ بیت ورودی به جعبه‌های جانشانی برابر است با $2^{-n\times m\times R}$. به‌صورت کاملا مشابه می‌توان نشان داد که رابطه مذکور در خصوص رمزگشائی نیز صادق است.

اکنون به‌منظور شمارش تعداد تفاضل‌های ممکن برای یک تفاضل، قضیه زیر را در خصوص تعداد تفاضل‌های خروجی یک جعبه جانشانی فعال بیان و آن را اثبات می‌کنیم.

**قضیه ۲**. در یک جعبه‌جانشانی $n$ بیتی یک به یک، هر تفاضل ورودی غیرصفر مانند $\Delta_{in}\in \mathbb{F}_2^n$، می‌تواند حداکثر به $2^{n-1}$ مقدار متفاوت در تفاضل خروجی تبدیل شود. به‌عبارت دیگر داریم:

$$|\{\Delta_{out}\in \mathbb{F}_2^n: \exists\, x\ \Delta_{out}= S(x)\oplus S(x\oplus \Delta_{in})\}| \le 2^{n-1} \qquad (۳)$$

**اثبات:** این قضیه از این حقیقت نشات می‌گیرد که مقادیر $S(x)\oplus S(x\oplus\Delta_{in})$ و $S(x\oplus\Delta_{in})\oplus S(x)$ به خاطر تقارن برابر هستند. در نتیجه تعداد دفعاتی که به‌ازای یک تفاضل خاص $\Delta_{in}$ در ورودی، یک مقدار در تفاضل خروجی می‌تواند رخ دهد زوج است. لازم به‌ذکر است که این قضیه پیش از این به‌منظور بهبود حملات ملاقات در میان بر روی AES استفاده شده است [۱۳].

**قضیه ۳**. اگر تفاضل ورودی (خروجی) در الگوریتم LowMC برابر $\Delta_{in}\in \mathbb{F}_2^b$ باشد، تعداد مقادیر ممکن برای تفاضل خروجی (ورودی) پس از $R$ دور، حداکثر $2^{(n-1)\times m\times R}$ خواهد بود.

**اثبات:** طبق قضیه ۲ می‌دانیم که هر تفاضل غیرصفر در ورودی جعبه‌جانشانی می‌تواند حداکثر به $2^{n-1}$ مقدار در تفاضل خروجی منجر شود. از آن‌جایی که رمز قالبی در هر دور حداکثر $m$ جعبه جانشانی فعال دارد، در نتیجه برای هر مشخصه تفاضل R دوری، حداکثر $2^{(n-1)\times m\times R}$ مشخصه تفاضلی متفاوت وجود خواهد داشت و در نتیجه تفاضل خروجی می‌تواند حداکثر $2^{(n-1)\times m\times R}$ مقدار داشته باشد.

همان‌طور که از قضیه ۳ قابل مشاهده است، زمانی که تعداد جعبه‌های فعال به اندازه کافی کم باشند، تعداد تفاضل‌های ممکن بعد از تعداد محدودی دور، بسیار کمتر از تعداد کل تفاضل‌های ممکن خواهد بود یعنی $2^b > 2^{(n-1)\times m\times R}$ خواهد بود. بر همین اساس در بخش بعد مدلی را ارائه می‌کنیم که براساس آن می‌توان از این ویژگی (یعنی محدودیت تعداد تفاضل‌های موجود در خروجی دورهای کاهش یافته الگوریتم) به‌منظور ساختن مشخصه‌های تفاضل ناممکن استفاده کرد.

## ۳-۴- یافتن مشخصه‌های تفاضل ناممکن در رمزهای قالبی SPN با لایه غیرخطی جزیی

هدف ما در این بخش بازتعریف روش فقدان در میانه به‌گونه‌ای است که بتوان از خواص ذکر شده در بخش ۳-۲ به‌منظور ساخت مشخصه‌های تفاضل ناممکن استفاده کرد. بدین منظور $r_1+r_2$ دور از یک الگوریتم رمز قالبی $n$ بیتی را در نظر می‌گیریم. در این روش ابتدا برای یک مقدار تفاضل ورودی، تمام مقادیر ممکن برای تفاضل خروجی بعد از $r_1$ دور رمزگذاری را پیدا کرده و آنها را در مجموعه‌ای نظیر $D_1$ ذخیره می‌کنیم. به‌طور مشابه، برای یک مقدار تفاضل خروجی، تمام مقادیر ممکن برای تفاضل خروجی در دور $r_1$ ام را با انجام عمل رمزگشائی برای $r_2$ دور آخر الگوریتم پیدا کرده و آنها را در مجموعه‌ای نظیر $D_2$ ذخیره می‌کنیم. در صورتی که دو مجموعه $D_1$ و $D_2$ هیچ اشتراکی با یکدیگر نداشته باشند، می‌توان نتیجه گرفت که تفاضل ورودی موردنظر هیچگاه نمی‌تواند به تفاضل خروجی مذکور منجر شود. بنابراین، با این روش تنها در صورتی می‌توان یک مشخصه تفاضل ناممکن یافت که دو مجموعه $D_1$ و $D_2$ هیچ اشتراکی نداشته باشند. به عبارت دیگر کارائی روش براساس این احتمال است که دو مجموعه $D_1$ و $D_2$ کاملا مستقل باشند و عضو مشترک نداشته باشند. ما در ادامه به‌صورت کلی احتمال آن‌که دو مجموعه $D_1$ و $D_2$ عضو مشترک نداشته باشند را محاسبه می‌کنیم.

احتمال این‌که دو مقدار n بیتی تصادفی با یکدیگر برابر باشند مساوی است با $2^{-n}$. بین دو مجموعه تعداد $|D_1|\times|D_2|$ زوج وجود دارد. بنابراین، احتمال آن‌که دو مجموعه $D_1$ و $D_2$ هیچ عضو مشترکی نداشته باشند برابر است با:

$$\max(1-2^{-n}\times|D_1|\times|D_2|,0) \qquad (۴)$$

بدیهی است که احتمال عدم وجود عضو مشترک نهایتا برابر ۱ است و دامنه معادله ۴ بین عدد ۰ و ۱ متغیر است. باید توجه کرد که احتمال محاسبه شده مربوط به احتمال وجود مشخصه تفاضل ناممکن است. بدین معنی که اگر $2^{-n}\times|D_1|\times|D_2|<1$ باشد، در این صورت مهاجم می‌تواند با احتمال $1-2^{-n}\times|D_1|\times|D_2|$ یک مشخصه تفاضل ناممکن پیدا کند.

همان‌گونه که مشاهده می‌شود، کارائی این روش به اندازه دو مجموعه $D_1$ و $D_2$ بستگی دارد. یعنی هرچقدر اندازه دو مجموعه $D_1$ و $D_2$ کوچک‌تر باشند، احتمال یافتن یک مشخصه تفاضل

ناممکن بیشتر است. به‌عبارت دیگر کارائی این روش به این بستگی دارد که تعداد مقادیر ممکن برای تفاضل میانی در نظر گرفته شده، محدود باشد. در این صورت با احتمال بالائی می‌توان انتظار داشت که پس از تشکیل دو مجموعه $D_1$ و $D_2$، اشتراکی بین دو مجموعه وجود نداشته باشد.

در بخش ۴، توضیح می‌دهیم که چگونه می‌توان تفاضل‌های ورودی و خروجی را به نحوی هوشمندانه انتخاب کرد که تعداد تفاضل‌های میانی بسیار محدود باشند.

## ۴- یافتن مشخصه تفاضل ناممکن برای خانواده رمزهای قالبی LowMC

همان‌طوری که در بخش قبل مشاهده شد خانواده رمزهای قالبی LowMC از لایه‌های خطی بسیار قوی تشکیل شده است. وجود ماتریس بیتی تصادفی سبب می‌شود که یافتن مشخصه‌های تفاضل ناممکن با روش‌های شناخته شده برای این الگوریتم بسیار دشوار باشد چراکه عموما روش‌های پیشین براساس ساختارهای بایت محور می‌باشند. با توجه به چارچوبی که در بخش ۳-۴-، ارائه شد، در این بخش نشان داده شد که چگونه می‌توان *مستقل از ویژگی‌های لایه خطی الگوریتم*، مشخصات تفاضل ناممکن کارایی به‌دست آورد.

### ۴-۱- چارچوب حمله به رمزهای SPN با ساختار توصیف شده

به‌منظور به‌دست آوردن یک مشخصه تفاضل ناممکن برای $r$ دور از الگوریتم LowMC، الگوریتم را به چهار بخش تقسیم می‌کنیم.

**آ) مسیر رفت:**

طبق قضیه ۱ می‌دانیم که مستقل از لایه خطی استفاده شده در یک رمز قالبی SPN با لایه غیرخطی جزیی، به طور متوسط $2^{\alpha}=2^{b-n\times m\times r_1}$ مشخصه تفاضلی با احتمال یک برای $r_1=\left\lfloor\frac{b-\alpha}{n\times m}\right\rfloor$ دور از الگوریتم LowMC وجود دارد. به عبارت دیگر تعداد $2^{\alpha}$ مقدار مانند $\delta_{in}^{i}\in\mathbb{F}_2^b, 1\le i\le 2^{\alpha}$ برای تفاضل ورودی الگوریتم وجود دارد به نحوی که پس از $r_1=\left\lfloor\frac{b-\alpha}{n\times m}\right\rfloor$ دور تفاضل خروجی دور با احتمال ۱ مشخص باشد.

از طرفی طبق قضیه ۳ می‌دانیم اگر تفاضل ورودی دور $(r_1+1)$ام در الگوریتم LowMC برابر $\Delta_{r_1+1}\in\mathbb{F}_2^b$ باشد، تعداد مقادیر ممکن برای تفاضل خروجی پس از دور $r_1+r_2$ام، حداکثر $2^{(n-1)\times m\times r_2}$ خواهد بود.

پس با در نظرگرفتن $2^{\alpha}$ مقدار $\delta_{in}^{i}\in\mathbb{F}_2^b, 1\le i\le 2^{\alpha}$ برای تفاضل ورودی، تفاضل خروجی دور $r_1$ حداکثر $2^{\alpha}$ مقدار می‌تواند داشته باشد (چراکه مشخصه‌های تفاضلی $r_1$ دور اول با احتمال ۱ صادق هستند). همچنین تفاضل خروجی دور $r_1+r_2$ می‌تواند حداکثر $2^{\alpha\times(n-1)\times m\times r_2}$ مقدار ممکن داشته باشد. به بیان دیگر برای $r_2=0$ تنها $2^{\alpha}$ مقدار ممکن برای تفاضل ورودی داریم و برای $r_2>0$ حداکثر $2^{\alpha\times(n-1)\times m\times r_2}$ مقدار ممکن برای تفاضل ورودی داریم. تمامی این حالات در جدولی به نام جدول $D_1$ ذخیره شد. به‌طور کلی، حداکثر مقادیر ممکن برای تفاضل ورودی ذخیره شده در جدول $D_1$ از رابطه (۵) قابل محاسبه است:

$$|\boldsymbol{D_1}|=\boldsymbol{max}(2^{\alpha,\alpha\times(n-1)\times m\times r_2}) \qquad (۵)$$

**ب) مسیر رو به عقب**

در مسیر رو به عقب نیز دقیقا همان روابط رو به جلو صادق است و می‌توان از آن‌ها استفاده کرد.

طبق قضیه ۱ می‌دانیم که مستقل از لایه خطی استفاده‌شده در یک رمز قالبی SPN با لایه غیرخطی جزیی، به‌طور متوسط $2^{\beta}=2^{b-n\times m\times r_4}$ مشخصه تفاضلی با احتمال یک برای $r_4=\left\lfloor\frac{b-\beta}{n\times m}\right\rfloor$ دور از الگوریتم LowMC وجود دارد. به عبارت دیگر تعداد $2^{\beta}$ مقدار مانند $\delta_{out}^{i}\in\mathbb{F}_2^b, 1\le i\le 2^{\beta}$ برای تفاضل خروجی الگوریتم در دور $r=r_1+r_2+r_3+r_4$ وجود دارد، به نحوی که پس از $r_4=\left\lfloor\frac{b-\beta}{n\times m}\right\rfloor$ دور عمل رمزگشائی، تفاضل دور $r=r_1+r_2+r_3$ با احتمال ۱ مشخص باشد.

از طرفی طبق قضیه ۳ می‌دانیم اگر تفاضل خروجی دور $(r_1+r_2+r_3)$ام در الگوریتم LowMC برابر $\Delta_{r_1+r_2+r_3}\in\mathbb{F}_2^b$ باشد، تعداد مقادیر ممکن برای تفاضل خروجی دور $r_1+r_2$، حداکثر $2^{(n-1)\times m\times r_3}$ خواهد بود.

پس با در نظرگرفتن $2^{\beta}$ مقدار $\delta_{out}^{j}\in\mathbb{F}_2^b, 1\le j\le 2^{\beta}$ برای تفاضل خروجی الگوریتم، تفاضل خروجی دور $r_1+r_2+r_3$ حداکثر می‌تواند $2^{\beta}$ مقدار داشته باشد (چراکه مشخصه‌های تفاضلی $r_4$ دور نهایی با احتمال ۱ صادق هستند). همچنین تفاضل خروجی دور $r_1+r_2$ می‌تواند حداکثر $2^{\beta\times(n-1)\times m\times r_3}$ مقدار ممکن داشته باشد. ما تمامی این حالات را در جدولی به نام جدول $D_2$ ذخیره می‌کنیم. دقیقا مشابه روند توضیح داده شده برای رابطه (۴)، حداکثر مقادیر ممکن برای تفاضل خروجی ذخیره شده در جدول $D_2$ از رابطه (۶) قابل محاسبه است:

$$|\boldsymbol{D_2}|=\boldsymbol{max}(2^{\beta,\beta\times(n-1)\times m\times r_3}) \qquad (۶)$$

**ج) پیدا کردن مشخصه تفاضل ناممکن**

حال طبق بخش ۳-۳-۱، اگر $2^{-b}\times|D_1|\times|D_2|\ll 1$ باشد، مهاجم می‌تواند با احتمال $1-2^{-n}\times|D_1|\times|D_2|$ یک مشخصه تفاضل ناممکن برای $r_1+r_2+r_3+r_4$ دور الگوریتم پیدا کند.

پس باید به دنبال حالتی باشیم که در آن، $2^{-b} \times |D_1| \times |D_2| \ll 1$. دلیل این امر این است که در زمان اشتراک‌گیری دو مجموعه $D_1$ و $D_2$ احتمال وجود یک عنصر مشترک بسیار پائین باشد. به‌عبارت دیگر با احتمال بسیار بالا بتوانیم یک مشخصه تفاضل ناممکن پیدا کنیم. بنابراین، برای $r_3$ و $r_2$ بزرگ‌تر از صفر، باید رابطه (۷) صدق کند:

$$\boldsymbol{2^{-b} \times |D_1| \times |D_2| \ll 1} \quad (۷)$$

$$2^{-b} \times 2^{\alpha\times(n-1)\times m\times r_2} \times 2^{\beta\times(n-1)\times m\times r_3} \ll 1$$

$$2^{(\alpha\times r_2+\beta\times r_3)\times(n-1)\times m} \ll 2^b$$

اما در حالتی که برای $r_3$ و $r_2$ برابر صفر باشد طبق روندی که برای به‌دست آوردن روابط (۵) و (۶) توضیح داده شد (برای $r_2 = 0$ تنها $2^\alpha$ مقدار ممکن برای تفاضل ورودی داریم)، تعداد اعضای $D_1$ و $D_2$ به ترتیب برابر $2^\alpha$ و $2^\beta$ خواهد بود. بنابراین، اگر مقدار $r_3$ برابر صفر باشد رابطه (۷) به شکل رابطه (۸) نوشته خواهد شد:

$$\boldsymbol{2^{\alpha\times(n-1)\times m\times r_2} \times 2^{\beta} \ll 2^{b}} \quad (۸)$$

### د) پیچیدگی یافتن مشخصه تفاضل ناممکن

پیچیدگی زمانی ساخت دو مجموعه $D_1$ و $D_2$ برابر با تعداد اعضای آن‌ها است. بنابراین، پیچیدگی زمانی کل برابر $|D_1| + |D_2|$ است که باید از پیچیدگی جست و جوی کلید کمتر باشد. زیرا در غیر این‌صورت پیچیدگی یافتن تمایزگر از پیچیدگی حمله فراگیر بیشتر می‌شود و وجود چنین تمایزگری توجیه ندارد. بنابراین، برای $r_3$ و $r_2$ بزرگ‌تر از صفر، شرط ۹ باید صدق کند:

$$\boldsymbol{\alpha \times (n-1) \times m \times r_2 + \beta \times (n-1) \times m \times r_3 < k} \quad (۹)$$

$$\alpha \times r_2 + \beta \times r_3 < \frac{k}{(n-1)\times m}$$

که برای $r_3$ برابر صفر خواهیم داشت:

$$\boldsymbol{\alpha \times (n-1) \times m \times r_2 + \beta < k} \quad (۱۰)$$

در نتیجه برای $r_3$ برابر صفر با توجه به روابط ۸ و ۱۰، رابطه کلی ۱۱ را خواهیم داشت:

$$\boldsymbol{\alpha \times (n-1) \times m \times r_2 + \beta < min(k, b)} \quad (۱۱)$$

## ۴-۲- یافتن مشخصه تفاضل ناممکن برای الگوریتم LowMC

در چارچوب ارائه شده در بخش ۴-۱، می‌توان برای دورهای کاهش یافته نسخه‌های متفاوت الگوریتم LowMC، مشخصه تفاضل ناممکن پیدا کرد. در ادامه جدولی از مشخصه‌های به‌دست‌آمده برای انواع مختلف الگوریتم LowMC تحت چارچوب کلی ارائه‌شده، آورده شده است که به‌صورت دقیق و به تفکیک پارامترهای استفاده شده ذکر شده است. حداکثر مقدار $r_1$ و $r_4$ طبق بخش ۴-۱ و پارامترهای $r_2$، $\alpha$ و $\beta$ با توجه به مقدار $r_1$ و $r_4$ و طبق رابطه کلی ۱۰ به راحتی قابل محاسبه هستند. نتایج محاسبات انجام‌شده به شرح جدول (۲) است. لازم به‌ذکر است که تمامی نتائج به‌دست‌آمده مستقل از لایه خطی است.

**جدول (۲):** تمایزگر برای حالت‌های مختلف الگویتم رمزنگاری LowMC.

| حالت | تعداد دور | $r_1 = r_4$ | $r_2$ | $r_3$ | $\alpha$ | $\beta$ |
|---|---|---|---|---|---|---|
| LowMC(128,80,31,64) | ۶۴/۱۲ | ۱ | ۱ | ۰ | ۱ | ۱۷ |
| LowMC(64,80,1,64) | ۶۴/۱۶۴ | ۲۱ | ۲۲ | ۰ | ۱ | ۱ |
| LowMC(1024,80,20,64) | ۳۴/۴۵ | ۱۷ | ۱ | ۰ | ۱ | ۴ |
| LowMC(1024,80,10,64) | ۷۱/۸۵ | ۳۴ | ۳ | ۰ | ۱ | ۴ |
| LowMC(256,128,63,128) | ۳/۱۴ | ۱ | ۱ | ۰ | ۱ | ۱ |
| LowMC(196,128,63,128) | ۳/۱۴ | ۱ | ۱ | ۰ | ۱ | ۱ |
| LowMC(128,128,3,128) | ۴۶/۸۸ | ۱۴ | ۱۸ | ۰ | ۱ | ۲ |
| LowMC(128,128,2,128) | ۶۹/۱۲۸ | ۲۱ | ۲۷ | ۰ | ۱ | ۲ |
| LowMC(128,128,1,128) | ۱۳۸/۲۵۲ | ۴۲ | ۵۴ | ۰ | ۱ | ۲ |
| LowMC(1024,128,20,128) | ۳۷/۴۹ | ۱۷ | ۳ | ۰ | ۱ | ۴ |
| LowMC(1024,128,10,128) | ۷۴/۹۲ | ۳۴ | ۶ | ۰ | ۱ | ۴ |
| LowMC(512,256,66,256) | ۳/۱۸ | ۱ | ۱ | ۰ | ۱ | ۱۲۳ |
| LowMC(256,256,10,256) | ۲۷/۵۲ | ۸ | ۱۱ | ۰ | ۱ | ۱۶ |
| LowMC(256,256,1,256) | ۲۸۸/۴۵۸ | ۸۵ | ۱۱۸ | ۰ | ۱ | ۱ |
| LowMC(1024,256,10,256) | ۸۰/۱۰۳ | ۳۴ | ۱۲ | ۰ | ۱ | ۴ |

در جدول (۲) سعی شده است با توجه به بخش ۴-۱، تا جای ممکن تعداد دورهای تمایزگر بیشینه باشد. بدین منظور از آن جا که مقدار $r_1$ و $r_4$ بیشینه و ثابت در نظر گرفته شدند، این بیشینگی را بر روی $r_2$ تحمیل کردیم و $r_3$ را برابر صفر در نظر گرفتیم. حال آن که می‌توان به‌جای $r_2$ این بیشینگی را بر روی $r_3$ اعمال کرد. همچنین برای تحقق شروط بخش ۴-۱ مجبور به محدودسازی $\alpha$ و $\beta$ بودیم که این محدود سازی با توجه به مقادیر $r_2$ و $r_3$ انجام شد.

همان‌گونه که مشخص است روش ارائه‌شده برای برخی نسخه‌های LowMC موثرتر است. به‌عنوان مثال برای ۷۱ دور از ۸۵ دور نسخه LowMC(1024,80,10,64) می‌توان یک مشخصه تفاضل ناممکن پیدا کرد (حدودا ۸۳ درصد دورها). این در حالی است که برای نسخه LowMC(64,80,1,64) می‌توان برای تنها ۶۴ دور از ۱۶۴ دور الگوریتم مشخصه تفاضل ناممکن پیدا کرد (یعنی حدود ۳۹ درصد دورها). بنابراین، مشاهده می‌شود که حاشیه امنیتی نسخه‌های مختلف LowMC در مقابل تحلیل تفاضل ناممکن متفاوت است.

### ۴-۳- اعمال حمله بازیابی کلید به ۶۴ دور الگوریتم LowMC(128,128,2,128)

ما در بخش گذشته چارچوبی کلی به منظور یافتن مشخصه‌های تفاضل ناممکن برای نسخه‌های متفاوت LowMC ارائه کرده و امنیت نسخه‌های متفاوت را براساس چارچوب ارائه شده بررسی کردیم. وجود مشخصه تفاضل ناممکن به معنای وجود یک تمایزگر است و خاصیتی غیرتصادفی و نامناسب برای الگوریتم محسوب می‌شود. از سوی دیگر مشخصه تفاضل ناممکن که برای $r$ دور از الگوریتم یافته می‌شود، ممکن است برای حمله به تعداد دور بیشتر مورد استفاده قرار گیرد (به بخش ۲-۱ مراجعه شود).

توصیف حمله بازیابی کلید به‌صورت عام بر اساس مشخصه‌های تفاضل ناممکن توصیف شده در بخش قبل امکان‌پذیر نیست چرا که پیچیدگی داده و زمان هر حمله بازیابی کلید به شدت وابسته به ویژگی‌های خاص مشخصه تفاضل ناممکن به‌کار رفته است. ما اعتقاد داریم همچون سایر حملات تفاضل ناممکن که بر روی سایر الگوریتم‌های رمزنگاری به کار رفته است، بتوان مشخصه‌های تفاضل ناممکن توصیف شده در بخش قبل به راحتی برای حمله بازیابی کلید استفاده کرد. اما از آنجائی یک حمله عام برای تمام نسخه‌ها قابلیت به صورت فرمول در آوردن ندارد، در این قسمت به عنوان یک نمونه نشان می‌دهیم که چگونه یک مشخصه تفاضل ناممکن خاص ۶۳ دوری می‌تواند برای حمله به ۶۴ دور الگوریتم به کار رود. برهمین اساس ابتدا در بخش ۰ نشان می‌دهیم که چگونه یک مشخصه تفاضل ناممکن ۶۳ دوری می‌توان برای LowMC(128,128,2,128) یافت. سپس در بخش ۰ یک حمله بازیابی کلید که براساس مشخصه به‌دست‌آمده می‌باشد را توصیف کرده و پیچیدگی حمله را به‌طور دقیق محاسبه می‌کنیم.

#### ۴-۳-۱- مشخصه تفاضل ناممکن ۶۳-دوری

روند یافتن مشخصه تفاضل ناممکن ۶۳ دوری را می‌توان به صورت گام‌های زیر بیان کرد:

در مسیر رو به جلو اگر فقط ۱ بیت فعال در ورودی به‌عنوان مقدار تفاضلی $\delta_{in}^{i}$ داشته باشیم، می‌توانیم $r_1 = \left\lfloor \frac{128-1}{3\times2} \right\rfloor = 21$ دور را با احتمال یک بگذرانیم به نحوی که هیچ یک از جعبه‌های جانشینی فعال نباشند. همچنین طبق جدول (۲) مقدار $r_2$ را برابر ۲۲ قرار می‌دهیم. در نتیجه در دور ۴۳ام $2^{\alpha\times(n-1)\times m\times r_2} = 2^{1\times2\times2\times22} = 2^{88}$ مقدار تفاضلی مختلف خواهیم داشت. هر یک از $2^{88}$ مقدار تفاضلی خروجی را با $\Delta_{in}^{i}$ نشان می‌دهیم که در آن، پارامتر $1 \le i \le 2^{88}$ است و مجموعه‌ای مانند $D_1$ را با توجه به آن تشکیل می‌دهیم.

اما در مسیر رو به عقب اگر مقدار $r_4$ را هم ۲۱ انتخاب کنیم، پیچیدگی حمله از پیچیدگی جستجوی فراگیر بالاتر رفته و حمله بی‌معنی خواهد شد. بدین منظور $\beta$ را برابر ۸ در نظر می‌گیریم. در این صورت $r_4 = \left\lfloor \frac{128-8}{3\times2} \right\rfloor = 20$ خواهد شد. و $r_3$ را برابر ۰ قرار می‌دهیم.

در نتیجه در دور ۶۳ ام $2^8$ مقدار تفاضلی خروجی مختلف $\delta_{out}^{i}$ خواهیم داشت. هر یک از $2^8$ مقدار تفاضلی خروجی به صورت یک به یک به $\Delta_{out}^{i}$ می‌رود که در آن پارامتر $1 \le i \le 2^8$ است و مجموعه‌ای مانند $D_2$ را با توجه به آن تشکیل می‌دهیم.

اگر مجموعه‌های $D_1$ و $D_2$ دارای هیچ اشتراکی نباشند در واقع یک مشخصه تفاضل ناممکن به‌دست آورده‌ایم. طبق بخش ۳-۴، مهاجم می‌تواند با احتمال $1 - 2^{-n} \times |D_1| \times |D_2| = (1 - 2^{-32})$ یک مشخصه تفاضل ناممکن پیدا کند. مشخصه تفاضل ناممکن به دست آمده به این شکل خواهد بود که یک مقدار تفاضلی $\delta_{in}^{i}$ (با شرایطی که توصیف شد) نمی‌تواند پس از ۶۳ دور به یکی از تفاضل‌های $\delta_{out}^{i}$ با مشخصات ذکرشده برود که $1 \le i \le 2^8$.

#### ۴-۳-۲- حمله بازیابی کلید به ۶۴ دور از الگوریتم

$2^n$ زوج متن $(P_j.P'_j)$ که $1 \le j \le 2^n$ را انتخاب می‌کنیم به گونه‌ای که $P_j = P'_j \oplus \delta_{in}^{i}$ است و منظور از $\delta_{in}^{i}$ همان تفاضلی است که توصیفش در بخش ۳-۴-۱ ارائه شده است. متن‌های اصلی را با استفاده از الگوریتم LowMC(128,128,2,128)، ۶۴ دوری رمز کرده و زوج متن‌های معادل آن‌ها $(C_i.C'_i)$ را به‌دست می‌آوریم.

با داشتن متون رمزشده، اگر ۶ بیت کلید مخفی را حدس بزنیم یعنی می‌توانیم به مقدار ورودی هر دو جعبه جانشینی سه بیتی دسترسی پیدا کنیم و در نتیجه به مقدار دقیق تمامی بیت‌های قالب دور ۶۳ام خواهیم رسید. ما فقط جفت‌هایی را انتخاب می‌کنیم که مقدار تفاضل به دست آمده دور ۶۳ام برابر یکی از مقادیر $\delta_{out}^{i}$ به‌ازای $1 \le i \le 2^8$ شود، در آن صورت کلید حدس زده شده غلط است و باید از لیست کاندیدهای ممکن حذف شود.

#### پیچیدگی

پیچیدگی حافظه حمله، ناشی از ذخیره‌سازی مجموعه‌های $D_1$ و $D_2$ است که به ترتیب $2^{88}$ و $2^8$ مقدار ممکن دارند که برای ذخیره‌سازی آن‌ها به حدود $2^{88} + 2^8 \cong 2^{89}$ قالب حافظه نیاز هست.

احتمال آن‌که تفاضل محاسبه‌شده در انتهای دور ۶۳ام، یکی از مقادیر $\delta_{out}^{i}$ها ($1 \le i \le 2^8$) بشود برابر است با $\frac{2^8}{2^{128}} = 2^{-120}$. بنابراین، احتمال این‌که بعد از رمزگشایی یک زوج متن رمزشده به‌ازای یک کلید حدس زده شده، کلید غلط حذف شود برابر $2^{-120}$ است. اگر تعداد کلیدهای غلط باقی‌مانده $N$ باشد، پس از امتحان کردن یک زوج، انتظار داریم که تعداد کلیدهای غلط باقی‌مانده برابر $N - N \times 2^{-120} = N(1 - 2^{-120})$ شود.

با توجه به این‌که $2^6$ کاندید برای کلید معادل وجود دارد، بنابراین، پس از تکرار رویه فوق برای $2^n$ زوج، انتظار داریم که $2^6(1 - 2^{-120})^{2^n}$ کلید در لیست باقی بماند. در این صورت اگر $n = 122.1$ انتخاب شود، تعداد کلیدهای نادرست باقی‌مانده برابر خواهد شد با:

$$2^6(1 - 2^{-120})^{2^{120} \times 2^{2.1}} \approx 2^6 \times e^{-4.2} < 1$$

بنابراین، انتظار می‌رود که هیچ کلید غلطی باقی نماند و کلید صحیح به صورت یکتا به‌دست آید.

در نتیجه با توجه به مقدار n، پیچیدگی داده حمله ارائه شده برابر است با $2^{122.1}$ زوج که معادل $2^{123.1}$ متن منتخب است.

پیچیدگی زمانی اجرای حمله برای به‌دست آوردن ۶ بیت از کلید، ناشی از $2^{122.1}$ عملیات رمزنگاری ۶۴ دوری متون منتخب و همچنین $2^{122.1} \times 2^6 = 2^{128.1}$ عمل رمزنگاری یک دوری به‌ازای $2^6$ حالت مختلف کلید است. در مجموع پیچیدگی زمانی این دو گام حدودا معادل $2^{123.1} \approx 2^{122.1} + \frac{2^{128.1}}{64}$ عمل رمزنگاری ۶۴ دوری است. همچنین ۱۲۲ بیت باقیمانده کلید را نیز می‌توان با استفاده از جستجوی جامع به‌دست آورد. در نهایت پیچیدگی زمانی کل حمله، حدودا برابر با $2^{123.1} + 2^{122} \approx 2^{123.7}$ خواهد بود.

## ۵- نتیجه‌گیری

در این مقاله چارچوبی کلی برای یافتن تمایزگر برای دسته خاصی از رمزهای قالبی ارائه شد و از روش ارائه‌شده برای یافتن تمایزگر برای رمز قالبی LowMC بهره بردیم. چارچوب ارائه‌شده فارغ از مشخصات داخلی الگوریتم و خصوصا مستقل از ویژگی‌های لایه خطی عمل می‌کند. بنابراین، وجود ایده‌آل‌ترین لایه خطی نیز، خللی در به‌دست آوردن تمایزگر ایجاد نمی‌کند. آنچه در این مقاله و تحلیل ارائه‌شده حائز اهمیت است این موضوع است که چارچوب ارائه‌شده محدود به الگوریتم خاص LowMC نیست و به تمام الگوریتم‌های رمز قالبی که از ساختار SPN استفاده می‌کنند، فقط به شرط جزیی بودن لایه غیرخطی، قابل اعمال است.

همچنین به کمک روش ارائه‌شده و روش‌های بهبودیافته دیگر که وابسته به خصوصیات داخلی هر الگوریتم است، ممکن است بتوان برای یک رمز قالبی LowMC مشخصه‌های تفاضل ناممکن را به‌نحوی به‌دست آورد تا از این تمایزگر برای حمله بازیابی کلید استفاده کرد. به دلیل پیچیدگی توضیحات از توصیف کلی حمله بازیابی کلید و استخراج یک چارچوب کلی برای این حمله پرهیز شده است. اما در قالب یک مثال این حمله به الگوریتم LowMC اعمال شده است و می‌توان از روندی مشابه برای حمله به گونه‌های دیگر این الگوریتم (با رعایت محدودیت‌های پیچیدگی)، استفاده کرد. در حمله ارائه‌شده، پیچیدگی حافظه $2^{89}$، پیچیدگی زمانی برابر $2^{123.7}$ و پیچیدگی داده برابر با $2^{123.1}$ متن منتخب است.

## ۶- منابع


[1] M. R. Albrecht, C. Rechberger, T. Schneider, T. Tiessen, and M. Zohner, "Ciphers for MPC and FHE," in EUROCRYPT 2015, 2015.

[2] A. Canteaut, S. Carpov, C. Fontaine, T. Lepoint, M. N. Plasencia, P. Paillier, and R. Sirdey, "Stream ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression," in FSE 2016, 2016.

[3] P. Meaux, A. Journault, F. X. Standaert, and C. Carlet, "Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts," in EUROCRYPT 2016, 2016.

[4] M. R. Albrecht, L. Grassi, C. Rechberger, A. Roy, and T. Tiessen, "MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity," in ASIACRYPT 2016, 2016.

[5] C. Dobraunig, M. Eichlseder, L. Grassi, V. Lallemand, G. Leander, E. List, F. Mendel, and C. Rechberger, "Rasta: A cipher with low ANDdepth and few ANDs per bit," in CRYPTO 2018, 2018.

[6] B. Gerard, V. Grosso, M. N. Plasencia, and F. X. Standaert, "Block Ciphers That Are Easier to Mask: How Far Can We Go?," in CHES 2013, 2013.

[7] H. Soleimany, "Probabilistic Slide Cryptanalysis and Its Applications to LED-64 and Zorro," in FSE 2014, 2014.

[8] S. Rasoolzadeh, Z. Ahmadian , M. Salmasizadeh, and M. R. Aref, "Total break of Zorro using linear and differential attacks," Isecure, 2014.

[9] Y. Wang, W. Wu , Z. Guo, and X. Yu, "Differential cryptanalysis and linear distinguisher of full-round Zorro," in ACNS 2014, 2013.

[10] G. Leander, B. Minaud, and S. Ronjom, "A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin, iSCREAM and Zorro," in EUROCRYPT 2015, 2015.

[11] I. Dinur, Y. Liu, W. Meier, and Q. Wang, "Optimized Interpolation Attacks on LowMC," in ASIACRYPT 2015, 2015.

[12] C. Dobraunig, M. Eichlseder, and F. Mendel, "Higher-Order Cryptanalysis of LowMC," in ICISC 2015, 2015.

[13] M. R. Albrecht, C. Rechberger, T. Schneider, T. Tiessen, and M. Zohner, "Ciphers for MPC and FHE," IACR Cryptology ePrint Archive, 2016.

[14] D. Derler, C. Orlandi, S. Ramacher, C. Rechberger, and D. Slamanig, "Digital Signatures from Symmetric-Key Primitives," IACR Cryptology ePrint Archive, 2016.

[15] D. Derler, S. Ramacher, and D. Slamanig, "Post-Quantum Zero-Knowledge Proofs for Accumulators with Applications to Ring Signatures from Symmetric-Key Primitives," in PQCrypto 2018, 2018.

[16] M. Chase , D. Derler, S. Goldfeder, C. Orlandi, S. Ramacher, C. Rechberger, D. Slamanig, and G. Zaverucha, "Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives," in CCS 2017, 2017.

[17] A. BarOn, I. Dinur, O. Dunkelman, V. Lallemand, N. Keller, and B. Tsaban, "Cryptanalysis of SP Networks with Partial Non-Linear Layers," in EUROCRYPT 2015, 2015.

[18] L. Knudsen, "DEAL - A 128-bit Block Cipher," Technical report no. 151. University of Bergen, Norway, 1998.

[19] E. Biham, A. Biryukov, and A. Shamir, "Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials," in EUROCRYPT 1999, 1999.

[20] M. R. Dastajani, M. Javad, and P. Ali, "Impossible Differential Cryptanalysis of Piccolo-80," Defence Sci. & Tech., vol. 5, no. 1, pp. 1-12, 2013. (In persian)

[21] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An ultra-lightweight block cipher," In International Workshop on Cryptographic Hardware and Embedded Systems 2007 Sep 10 (pp. 450-466). Springer, Berlin, Heidelberg, 2007.

[22] J. Daemen and V. Rijmen, "AES proposal: Rijndael," 1999.

Journal of Electronical & Cyber Defence
Vol. 7, No. 2, 2019, Serial No. 26



# Analysis of Impossible Differential on LowMC Block Cipher

**H. Soleimany*, A. Mehrdad**

*Shahid Beheshti University

(Received: 27/05/2018, Accepted: 13/10/2018)

**ABSTRACT**

Impossible differential attack is one of the strongest methods of cryptanalysis on block ciphers. In block ciphers based on SPN (substitution permutation network), the only layer that resists the difference is the nonlinear layer. Obviously, paying attention to the features of nonlinear layer is important for the sake of preventing statistical attacks, such as the differential attack. Therefore, this layers' features regarding attack tolerance should be carefully investigated. The existence of such a nonlinear layer with the required features and applying it in the entire length of the block can lead to more resistance against differential attacks. Over the past few years, a new set of block ciphers based on SPN has been introduced, in which the nonlinear layer is applied only to a particular part of the state. In this paper, a general framework for finding the characteristics of the impossible difference in this type of new block cipher is presented. Contrary to the previous miss-in-the-middle methods, which are used to find the impossible differences, the method presented in this article is independent of the feature of linear layer of the algorithm and allows the attacker to systematically find the effective impossible differential even in cryptographic algorithms with highly complex linear layer. In order to demonstrate the efficiency of the proposed method, the family of LowMC ciphers that use bitwise linear layer are examined in this paper and based on this framework some impossible differential characteristics are proposed for some versions of reduced LowMCs. This proposed impossible differential characteristics can be easily applied in key-recovery attacks based on the framework presented in this paper. As an example, we show that based on the impossible difference characteristic obtained for 63 rounds of the LowMC (128,128,2,128), a key-recovery attack is applied to the 64-round of this algorithm. In proposed attack, the complexity of memory is 289, the complexity of the time is 2123.7, and the complexity of the data is equal to 2123.1 of the chosen plain text.

**Keywords:** Block Cipher, Cryptanalysis, Impossible Differential Attack, LowMC Block Cipher

* Corresponding Author Email: h_soleimany@sbu.ac.ir