نشریه علمی "پدافند الکترونیکی و سایبری"
سال هفتم، شماره ۳، پاییز ۱۳۹۸، ص ۸-۱

تحلیل ساختاری مبتنی بر ویژگی انتگرال در یک رمز قالبی با دورهای کاهش‌یافته و ارائه یک بهبود

بهروز خادم[1*]، علی تجدد[2]، کاوه بختیاری[3]
۱- استادیار، ۲- کارشناسی ارشد، دانشگاه جامع امام حسین(ع)
۳- دانشجوی دکتری، دانشگاه دویسبورگ-اسن، آلمان
(دریافت: ۹۷/۱۰/۱۵، پذیرش: ۹۷/۱۲/۲۰)

چکیده

کدهای خطی در رمزنگاری متقارن، اهمیت رمزهای قالبی نسبت به رمزهای دنباله‌ای، کدهای احراز اصالت و طرح‌های احراز اصالت رمزگذاری شده از آن جهت بیشتر است که اغلب به‌عنوان اولیه‌های امن در ساختن انواع دیگر به‌کار می‌روند. یکی از انواع روش‌های تحلیل رمزهای قالبی، تحلیل ساختاری است که بدون نیاز به اطلاعات مربوط به مؤلفه‌های درونی این طرح‌ها مانند جایگشت‌ها و جعبه‌های جانشانی آن‌ها به امنیت آن‌ها می‌پردازد. در این مقاله با استفاده از یک تمایزگر انتگرال چهار دوری شناخته‌شده روی AES برای اولین بار، دو حمله انتگرال به یک رمز قالبی و بومی جدید با طول کلید و قالب ۲۵۶ بیتی انجام می‌شود. این دو حمله با توجه به نقاط ضعف طراحی تابع دور به یک و دو دور از این رمز قالبی بومی سه دوری انجام می‌شود. مقدار پیچیدگی حافظه، داده و زمان بهترین حمله انجام‌شده در این مقاله به‌ترتیب ۲۳۲ بایت، ۲۱۲۸ قالب متن اصلی و ۲۲۰۶ عمل رمزگذاری است. با توجه به طول کلید رمز، پیچیدگی حمله کمتر از مقدار پیچیدگی حمله جستجوی جامع فضای کلید (۲۲۵۶) است و درنتیجه یک حمله میان‌بر مؤثر محسوب می‌شود. به‌علاوه، به‌منظور بهبود این رمز بومی، در این مقاله راه‌کارهایی ارائه شده است.

کلیدواژه‌ها: رمز قالبی، تحلیل ساختاری، ویژگی انتگرال

۱- مقدمه

تحلیل ساختاری یکی از انواع روش‌های تحلیل طرح‌های رمزنگاری است که بدون نیاز به اطلاعات مربوط به مؤلفه‌های درونی این طرح‌ها به امنیت آن‌ها می‌پردازد. در تحلیل ساختاری رمزهای قالبی معمولاً به ابعاد (طول قالب، کلید و کلمه) آن توجه می‌شود و فرض می‌شود مهاجم هیچ‌گونه اطلاعات اضافی از مؤلفه‌ها و توابع درونی رمز ندارد. حمله انتگرال یکی از روش‌های جدید، قدرتمند و پرکاربردی هستند که در خانواده تحلیل‌های ساختاری قرار دارند و امروزه در تحلیل رمزهای جدید مورداستفاده بسیاری از محققان رمز و امنیت قرار می‌گیرد [۱].

۱-۱- تحقیقات مرتبط

در سال ۱۹۹۷ برای مقاومت در برابر حملات خطی و تفاضلی، رمز قالبی SQUARE توسط کنودسن[1]، ریمن[2] و دایمون[3] طراحی شد [۲]. در مرحله تحلیل نسخه اولیه این رمز قالبی، کنودسن کشف کرد که این رمز در مقابل یک نوع جدید از حمله متن اصلی انتخابی آسیب‌پذیر است که شش دور از آن را می‌شکند. به همین دلیل طراحان مجبور به افزایش تعداد دور آن شده و رمز اصلاح‌شده حاصل را همراه با این حمله جدید منتشر کردند [۲].

این حمله در سال‌های بعد به‌عنوان حمله مربع نامیده شد ولی روی رمز SQUARE نتوانست به بیش از شش دور توسعه یابد. شباهت بین رمز SQUARE با رمزهای RIJNDAEL و CRYPTON باعث شد که نسخه‌هایی از این حمله به این دو رمز ارائه شود و مجدداً شش دور از RIJNDAEL شکسته شد و به دنبال آن طراح CRYPTON هم فرضش را بر این گذاشت که این حمله نمی‌تواند به بیش از شش دور آن آسیب بزند [۴-۳].

لاکز[4] سعی کرد این حمله را به رمزهای غیرمشابه SQUARE نیز تعمیم بدهد و از این حمله برای رمز فیستلی

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

[1] Knudsen
[2] Rijmen
[3] Daemen
[4] Lucks

Twofish استفاده کرد و نام آن را به حمله اشباع تغییر داد [۵]. کنودسن و واگنر[1] فن متفاوت دیگری را به قالب اصلی این حمله افزودند و آن را حمله انتگرال نامیدند [۶].

رمز قالبی MISTY1 در سال ۱۹۹۷ طراحی شد و مورد توصیه CRYPTREC و ISO/IEC و NESSIE قرار گرفت [۷] و نسخه‌های تغییریافته آن مانند رمز Kasumi در GSM استفاده‌های گسترده‌ای یافتند [۸]. دو نوع از این رمز به نام‌های MISTY1 و MISTY2 وجود دارند. کنودسن نشان داد که می‌توان به MISTY2 حمله انتگرال چهار دوری موفق با 2^{55} عمل رمزگذاری و تنها ۹ زوج متن اصلی انجام داد [۶]. وی نشان داد که با 2^{34} متن اصلی انتخابی و پیچیدگی زمانی 2^{80} می‌توان به شش دور MISTY2 نیز حمله انتگرال انجام داد. حمله توسعه‌یافته دیگری به MISTY2 انجام شد که باهمان پیچیدگی داده، پیچیدگی زمانی را به 2^{71} کاهش داد. کنودسن همچنین حمله‌ای به پنج دور MISTY1 با 2^{34} متن اصلی انتخابی و پیچیدگی زمانی 2^{48} انجام داد که پیچیدگی داده و زمان در آن قابل‌معاوضه بود. کنودسن همچنین نشان داد که می‌توان به چهار دور MISTY1 حمله انتگرال با تنها ۲۵ متن اصلی انتخابی و 2^{72} عمل رمزگذاری انجام داد [۶]. همچنین سان[2] و لای[3] با استفاده از یک خاصیت شناخته‌شده قبلی روی شش دور از MISTY1 حمله انتگرال دیگری را با پیچیدگی داده 2^{32} و پیچیدگی محاسبات 2^{106} ارائه کردند [۹].

امروزه حمله انتگرال به‌دلیل عملی بودن روی AES به‌خصوص در شکستن نسخه کاهش‌یافته شش دوری آن از اهمیت ویژه‌ای برخوردار شده است. حمله فوق می‌تواند کلید ۱۲۸ بیتی AES را با استفاده از مجموعه‌ای از 2^{32} متن اصلی انتخابی و با پیچیدگی محاسباتی 2^{72} عمل رمزنگاری کشف کند. در این مقاله از نتایج این تحقیق برای حمله به یک رمز قالبی بومی استفاده‌شده است. گیلبرت[4] نیز حمله انتگرال پیچیده‌تری که می‌تواند به هفت دور اعمال شود را ارائه داد [۱۰].

لی[5] و همکاران یک حمله انتگرال بهبودیافته به رمز قالبی فیستلی CLEFIA انجام دادند [۱۱]. آن‌ها در این حمله یک تمایزگر انتگرال ۹ دوری مبتنی بر بایت را معرفی کردند. سپس با استفاده از فن جمع جزئی نتایج قبلی روی ۱۱ دور از همین رمز قالبی را بهبود داده و حمله انتگرال را به ترتیب روی ۱۲، ۱۳ و ۱۴ دور از این رمز (با کلید سفیدسازی) ارائه کردند.

اخیراً در یک حمله انتگرال روی رمز قالبی سبک وزن LBlock توسط ساساکی[6] و وانگ[7]، تحلیل انتگرال موفقی روی ۲۲ دور از LBlock انجام شد. حمله آن‌ها از یک تمایزگر انتگرال ۱۵ دوری استفاده می‌کرد اما به‌کار بردن ابتکاری نو باعث بهبود چشمگیر این حمله نسبت به حملات قبلی شد. به‌علاوه، انتخاب بهترین موقعیت بایت متوازن، فن ملاقات در میانه برای تشخیص نامزد کلید درست، فن جمع جزئی، ارتباط بین زیرکلیدها و ترکیب جستجوی جامع با تحلیل انتگرال ازجمله این ابتکارات می‌باشند [۱۲].

ژانگ[8] و وو[9] یک حمله انتگرال را برای نسخه اصلی رمز قالبی SIMON (که توسط آژانس امنیت ملی آمریکا معرفی‌شده بود) و نسخه‌های تعمیم‌یافته آن ارائه کردند [۱۳] و به‌وسیله آن یک خطای ذاتی در فرانمای کلید وابسته آن را پیدا کردند.

موراوسکی[10] یک حمله انتگرال موفق به هفت دور از رمز قالبی PRINCE انجام داد [۱۴]. بالاخره تودو[11] ضمن تعریف یک مفهوم جدید بنام ویژگی تقسیم، یک حمله انتگرال به نسخه کامل آن انجام داد و کلید کامل آن را با انتخاب 2^{63} قالب متن اصلی و 2^{121} عمل رمزنگاری کشف کرد [۱۵].

در ادامه ساختار این مقاله به شرح زیر است. در قسمت دوم توصیف مختصری از یک حمله انتگرال انجام‌شده قبلی به رمز قالبی AES را برای استفاده در قسمت بعدی ارائه می‌کنیم. در قسمت سوم ضمن معرفی مختصر یک رمز قالبی جدید [۱۶] که از ساختاری مشابه AES بهره می‌برد، یک نسخه از حمله انتگرال تک دوری و دو دوری به آن را ارائه می‌کنیم. در قسمت چهارم پیشنهادهایی برای بهبود رمز قالبی بومی به‌منظور مقاومت در برابر این حمله انتگرال را بیان می‌کنیم و در قسمت آخر نتایج مقاله ارائه می‌شود.

۲- حمله انتگرال به AES

ایده اصلی حمله انتگرال (در مدل متن اصلی انتخابی) تا حدودی شبیه به رویکرد حمله تفاضلی است. به‌جز این‌که در آن مهاجم به‌جای تجزیه‌وتحلیل زوج متون اصلی مرتبط و منتخب، رفتار مجموعه‌ای از متون اصلی (که با دقت انتخاب شده‌اند) را در حین انتشار به دورهای متوالی تحلیل می‌کند.

سناریوی عمومی تحلیل‌های انتگرال شامل دو گام است. در

[1] Wagner
[2] Sun
[3] Lai
[4] Gilbert
[5] Li
[6] Sasaki
[7] Wang
[8] Zhang
[9] Wu
[10] Morawiecki
[11] Todo

گام اول (یا تمایز)، مهاجم الگوریتمی (تمایزگر) را که با آن بتواند خروجی یک رمز قالبی را از یک جایگشت تصادفی تمایز دهد می‌سازد. در این نوع حملات تمایزگرهای انتگرال بر ویژگی‌های توازنی که با احتمال یک روی می‌دهند، استوار هستند. معمولاً در ابتدای حمله، برای نسخه کاهش‌یافته رمز قالبی یک تمایزگر ساخته می‌شود. سپس در گام دوم (یا کشف کلید)، در حمله کشف کلید یک رمز قالبی r دوری با یک تمایزگر $r-1$ دوری، یک دور اضافی توسط مهاجم به انتهای این تمایزگر اضافه می‌شود. سپس زوج‌های متن اصلی و متن رمزی انتخابی مورد استفاده قرار می‌گیرند. اگر k بیت از زیر کلید دور r کشف شود کلمه زیر کلید مؤثر حدس زده می‌شود. سپس برای هر مقدار حدس زده‌شده، یک دور رمزگشایی جزئی کلمه متن رمز مؤثر انجام می‌شود. این رمزگشایی برای دست‌یابی به خروجی دور $r-1$ انجام می‌شود. اگر رمزگشایی جزئی (برای خروجی دور $r-1$) با شرایط پیشگویی شده توسط تمایزگر مطابقت داشته باشد، مقدار حدس زده‌شده به‌عنوان یکی از مقادیر زیرکلید صحیح ممکن ذخیره می‌شود. محتمل‌ترین زیر کلید با تکرار متن اصلی و متن رمزهای مختلف به‌دست می‌آید.

به‌منظور تجزیه‌وتحلیل این مجموعه‌ها، نخست منطبق بر ساختار داخلی رمز، قالب‌های متن در قالب کلمات m بیتی در نظر گرفته می‌شوند و (چند)مجموعه‌هایی از مقادیر مختلف این کلمات در نظر گرفته می‌شوند. یک چندمجموعه[1]، فهرستی از مقادیر است که هر کدام می‌توانند به تعداد دلخواه تکرار شوند. در این مقاله تعدادی از انواع چندمجموعه‌های ویژه مورد بررسی قرار می‌گیرند که ابتدا تعدادی از آن‌ها معرفی می‌شوند [۵].

چندمجموعه ثابت (C)، چندمجموعه‌ای شامل یک تک مقدار است که به تعداد دلخواه تکرار می‌شود.

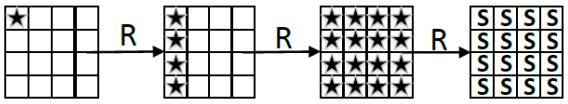
چندمجموعه اشباع (فعال A_i یا A)، چندمجموعه‌ای شامل همه مقادیر ممکن برای کلمه دقیقاً یک‌بار است.

چندمجموعه زوج (P)، چندمجموعه‌ای که هر مقدار آن، به‌دفعات زوج رخ می‌دهد.

چندمجموعه متوازن (B)، چندمجموعه‌ای که XOR همه مقادیر (با توجه به کثرت آن‌ها) صفر می‌شود.

یادآوری می‌شود که برخی از این خواص دیگر خواص را معنی می‌دهد. برای مثال، یک چندمجموعه ثابت با تعداد زوج از عناصر نیز یک چند مجموعه زوج است و یک چند مجموعه زوج یا اشباع به‌طور خودکار متوازن است.

در این قسمت یکی از بهترین حملات ساختاری انجام‌شده به AES را که منجر به پیدا شدن یک تمایزگر سه دوری برای AES شده است به‌طور مختصر توصیف می‌کنیم تا در قسمت بعدی از نتایج آن برای شکستن رمز قالبی بومی استفاده کنیم. در اینجا فرض شده خواننده با رمز AES آشنا است و فقط نکات اصلی حمله انجام‌شده به آن بیان می‌شوند. فرض کنید مهاجم در این حمله یک چندمجموعه شامل ۲۵۶ متن اصلی ۱۲۸ بیتی (در قالب ماتریس حالت ۱۶ بایتی) که بایت فعال آن‌ها شامل تمام ۲۵۶ مقدار ممکن است، در اختیار دارد. در هر حالت ۱۵ بایت باقی‌مانده از همه متون اصلی مقادیر مشابه می‌گیرند. مهاجم عملیات رمزنگاری یک دور AES را با این چندمجموعه آغاز می‌کند. خلاصه انتشار این ویژگی در ساختار سه دوری AES را می‌توان در شکل (۱) مشاهده کرد. موقعیت بایت فعال در حالت با شکل ستاره (★) نشان داده شده است و R نشان‌دهنده یک دور کامل AES و S نشان‌دهنده حاصل جمع متون در یک بایت خاص است که در این مورد برابر با صفر شد.



شکل (۱): انتشار ویژگی انتگرال در ساختار سه دوری AES [۱۷]

لازم به توضیح است که در این چند مجموعه بایتی که شامل همه ۲۵۶ مقدار ممکن را در دور اول می‌گیرد (بایت فعال) می‌تواند در هر یک از ۱۶ مکان حالت قرار بگیرد.

۲-۱- کشف کلید AES در حمله انتگرال

این ساختار می‌تواند توسط همین مهاجم برای حمله به شش دور از AES مورداستفاده قرار گیرد [۱۵] که در آن دور اول شامل RK (پیش سفیدسازی) و آخرین دور هم دور ششم (بدون MC) است. در حمله شش دوری ساختار سه دوری شکل (۱) در دورهای دوم تا چهارم استفاده می‌شود. مهاجم چهار بایت کلید در دور اول، چهار بایت کلید در آخرین استفاده از RK و یک بایت کلید در کاربرد ماقبل آخر از RK (درمجموع نه بایت کلید) را حدس می‌زند. حال او می‌تواند (پس از چهار دور رمزگذاری AES) با این بایت‌های حدس زده شده از کلید، حاصل جمع متون در یک موقعیت بایت را محاسبه کند. برای ساختاری با ۲۵۶ متن اصلی به شکل (۱)، این جمع صفر می‌شود. البته ممکن است مقادیری از این ۹ بایت کلید وجود داشته باشند که تصادفاً مقدار جمع را صفر نکنند. برای جلوگیری از چنین وضعیتی لازم است این حمله چند بار جهت تعیین منحصربه‌فرد بایت‌های کلید

[1] Multi-set

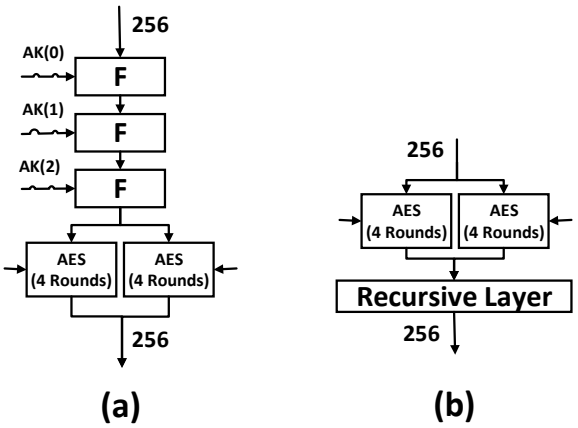
صحیح تکرار شود. هنگامی‌که ۹ بایت کلید صحیح کشف شد، کشف ۱۲ بایت کلید باقیمانده در آخرین استفاده RK به‌نسبت آسان‌تر خواهد بود (جمعاً ۲۱ بایت کلید) و پس‌ازآن کلید کامل به‌راحتی قابل‌کشف است. درمجموع این حمله با استفاده از حدود 2^{32} قالب متن اصلی انتخابی با پیچیدگی زمانی 2^{72} رمزگذاری و استفاده از 2^{32} کلمه حافظه انجام شده است [۱۱].

۳- حمله به رمز قالبی بومی جدید

در این قسمت ضمن معرفی یک رمز قالبی بومی که توسط یوسفی‌پور و میرقدری ارائه شده است [۱۶]، یک نسخه از حمله انتگرال یک دوری رمز بومی (معادل چهار دور AES و مشابه با آنچه در قسمت قبل در مورد AES انجام‌شده است) و دو دوری رمز بومی (معادل هشت دور AES) را انجام داده و پیچیدگی محاسباتی و زمانی این دو حمله را ارائه خواهیم کرد [۱۸].

۳-۱- توصیف مختصر رمز بومی

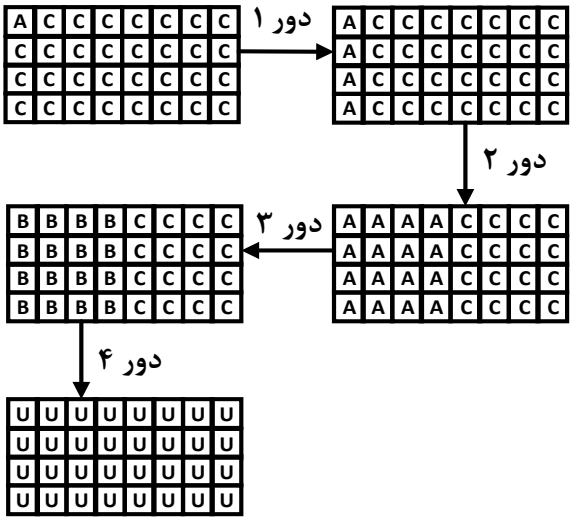
یک رمز قالبی بومی با طول کلید و قالب ۲۵۶ بیتی در شکل (۲) ارائه شده است.



شکل (۲): (a) شمای کلی و (b) تابع F در ساختار رمز بومی [۴]

ساختار این رمزبومی شامل چهار دور (سه دور کامل و یک دور ناقص) و هر دور کامل آن شامل اجرای موازی دو الگوریتم رمز AES چهار دوری به‌علاوه، یک‌لایه انتشار بازگشتی است (دور چهارم رمز بومی لایه انتشار ندارد).

مؤلفان [۱۶] به‌منظور نشان دادن مقاومت رمز خود در مقابل حمله انتگرال سناریوی مهاجم را به‌صورت شکل (۳) که مشابه قسمت ۲ است تصور کرده‌اند و نتیجه گرفته‌اند که رمز بومی تا دور چهارم در مقابل این مهاجم امن خواهد بود.



شکل (۳): سناریوی فرضی در حمله انتگرال به رمز بومی [۱۶]

در این مقاله سناریوی حمله انتگرال به رمز بومی به شکل (۴) در نظر گرفته شده و انجام شده است، در ادامه سناریوی پیشنهادی به‌طور خلاصه معرفی می‌شود. برای شروع برخی نمادهای موردنیاز را معرفی می‌کنیم،

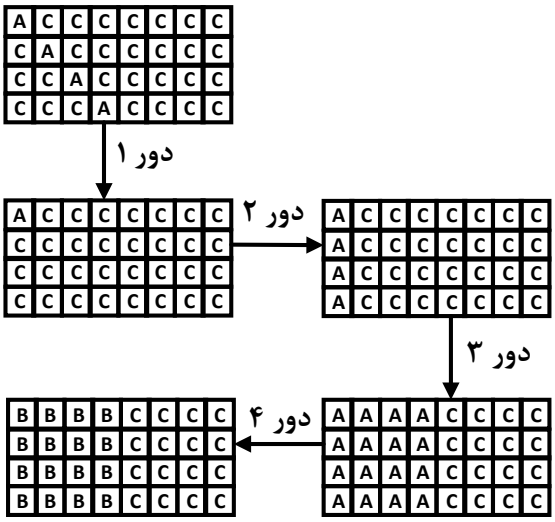
a_i (ماتریس حالت i)

m_i (بایت خروجی عملگرMC دور i)

k_i (بایت زیرکلید دور i)

k_i' (بایت زیرکلید دور i اگر عمل RK قبل از عمل MC روی دهد)

r_i (بایت بعد از عمل RK دورi)



شکل (۴): سناریوی پیشنهادی در حمله انتگرال به رمز بومی

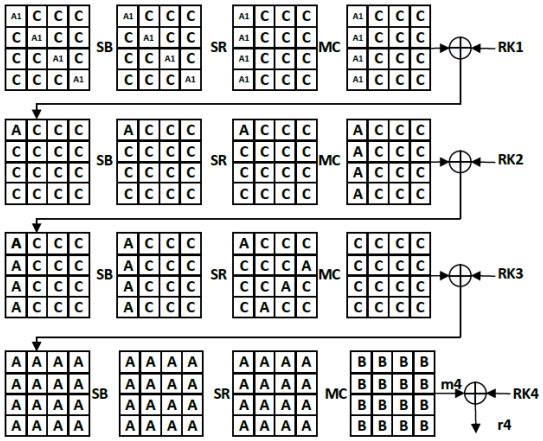
۳-۲- حمله انتگرال تک دوری به رمز بومی

شکل (۲) نشان می‌دهد که در ساختار رمز بومی، هر دور شامل

اجرای همزمان و موازی دو AES چهار دوری و یک لایه انتشار بازگشتی است. در مورد تاثیر لایه بازگشتی بر حمله ساختاری، می توان مشاهده کرد که چون از یک طرف (با توجه به نتایج حمله انتگرال انجام‌شده در قسمت ۲، معلوم شد که خروجی دور چهارم AES متوازن (B) است و از طرف دیگر در لایه انتشار بازگشتی رمز بومی فقط از عملگر XOR استفاده شده است [۱۶]، بنابراین، متوازن بودن کلیه بیت‌های ورودی به لایه انتشار بازگشتی، باعث می‌شود که هیچ تغییری در خاصیت توازن خروجی لایه بازگشتی به‌وجود نیاید و در نتیجه این لایه تاثیری بر حمله نداشته باشد. بنابراین، حمله یک دوری انجام‌شده به این رمز بومی و پیچیدگی محاسباتی آن مشابه حمله ذکرشده در قسمت ۲ است.

با انتخاب ۲۵۶ قالب متن رمزی (۲۵۶ حالت ۳۲ بایتی در نظر بگیرید) که تنها در یک بایت از حالت a_1 در شکل (۳) فعال و در بقیه بایت‌های آن ثابت‌اند آغاز می‌شود. یک بایت از حالت a_1 به ۴ بایت از متن اصلی و (با توجه به الگوریتم تولید زیر کلید AES) به ۴ بایت از k_0 (کلید اصلی) وابسته است. ابتدا 2^{32} متن اصلی را به‌طوری‌که مشابه شکل (۳) در ۴ بایت از ۳۲ بایت حالت (به‌صورت قطری) فعال باشند انتخاب می‌کنیم. علت این انتخاب به دلیل عملکرد مؤلفه‌های درونی هر دور رمزبومی و اثر آن‌ها روی ترتیب قرار گرفتن بایت‌های فعال در ساختار رمزبومی است به‌طوری‌که در ابتدای دور دوم رمز بومی فقط یک بایت از حالت فعال باشد تا بتوانیم از آن برای ساخت تمایزدهنده تک دوری مشابه شکل (۳) استفاده کرده و یک دور به آن بیافزائیم. سپس ۴ بایت از کلید را حدس می‌زنیم. برای هر بایت کلید، ما می‌توانیم 2^{24} گروه از ۲۵۶ متن اصلی را به‌گونه‌ای ایجاد کنیم که هر گروه رمزگذاری در یک بایت خاص a_1 متفاوت باشند.

مطابق با شکل (۵) با دنبال کردن این تغییر در رمز، بعد از m_4 کلیه بایت‌ها به شکل متوازن می‌رسند و بعد از لایه انتشار نیز تغییری نمی‌کنند. توجه داشته باشید که هر چهار دور AES به‌علاوه لایه انتشار یک دور رمز بومی را تشکیل می‌دهند. برای ادامه تحلیل و با توجه به عدم تأثیر زیرکلید در تغییر آرایش بایت‌های فعال، ما فرض می‌کنیم که در دور پنجم AES عملگر RK قبل از عملگر MC اتفاق بیفتد (نماد پرایم مشخص‌کننده این حالت است). در این ساختار هر بایت از m_4 به متن رمزی، ۴ بایت از k_6 و یک بایت از k'_5 (زیرکلید دور پنجم در حالتی که عمل RK قبل ازMC روی دهد) بستگی دارد. این ۵ بایت کلید را حدس زده و صفر شدن مقدار m_4 را برای ۲۵۶ متن رمزی را بررسی می‌کنیم.



شکل (۵): تمایزگر انتگرال چهار دوری برای حالت ۱۶ بایتی فرضی

این فیلتر (با احتمال یک) برای هر دسته از مجموعه ۲۵۶ متن اصلی، ۲۵۵ حدس کلید غلط را از ۲۵۶ مورد برمی‌گرداند. برای حدس ۹ بایت کلید نیاز به ۱۰ گروه ۲۵۶ تایی متن رمزی (یا بیشتر) داریم. این گروه تنها به ۴ بایت اول (از ۹ بایت) حدس زده شده کلید بستگی دارد. بنابراین، دیده می‌شود که این حمله نیاز به 2^{32} متن اصلی انتخابی، 2^{32} حافظه برای ذخیره زوج متن اصلی / متن رمزی و 2^{72} گام برای حدس ۹ بایت از کلید دارد.

۳-۲-۱- بهبود در حمله انتگرال تک دوری به رمز بومی

حمله انتگرال تک دوری به رمز بومی را می‌توان کمی توسعه داد. به‌جای حدس ۴ بایت k_0 (کلید اصلی) ما از همه 2^{32} متن اصلی که ۴ بایت قطری حالت آن‌ها فعال باشد استفاده می‌کنیم. بنابراین حدس ۵ بایت کلید در انتهای رمز، انجام رمزگشایی جزئی از تنها یک بایت از r_4 (بعد ازRK در دور چهارم AES)، جمع این مقدار روی همه 2^{32} عمل رمز و بررسی صفر شدن نتیجه اقداماتی است که باید انجام بدهیم. در این صورت در مقایسه با نسخه اصلی تنها ۴۰ بیت از ۷۲ بیت را حدس می‌زنیم. به‌عبارت‌دیگر باید 2^{24} عمل را برای هر حدس انجام بدهیم. درمجموع، این بهبود مقدار محاسبات لازم را با ضریب 2^8 کاهش می‌دهد، گرچه نیاز به $2^{32}\times 6$ متن اصلی (برای ۶ ساختار) برای تعیین صحیح ۵ بایت کلید داریم. به‌عبارت دیگر 2^{32} قالب متن رمزی داریم. ۵ بایت کلید را حدس زده و رمزگشایی جزئی یک بایت از متن رمز را در r_4 انجام می‌دهیم. سپس این بایت را روی کل متن رمز جمع می‌کنیم. این رمزگشایی جزئی را در نظر بگیرید. سپس از ۴ بایت از هر متن رمز استفاده می‌کنیم. هرکدام از آن‌ها با کلید XOR می‌شود. سپس معکوس جعبه جانشانی (S-Box) را به هر بایت اعمال می‌کنیم و هرکدام را در معکوس ماتریس MDS ضرب می‌کنیم. این ۴ بایت سپس باهم XOR

شده و با بایت پنجم کلید هم XOR می‌شوند، سپس معکوس جعبه جانشانی روی نتیجه اعمال می‌شود و مقدار نهایی مطابق معادله (۱) روی همه متن رمزی جمع می‌شود.

فرض $c_{i,j}$ بایت j ام از قالب رمز i ام است. برای سادگی ما ۴ بایت از هر متن رمز را از ۰ تا ۳ شماره‌گذاری می‌کنیم. فرض k_0 تا k_4 پنج بایت کلید حدسی هستند. می‌خواهیم عبارت (۱) را محاسبه کنیم.

$$\sum_{i} S^{-1}\left[S_0[c_{i,0} \oplus k_0] \oplus S_1[c_{i,1} \oplus k_1], S_2[c_{i,2} \oplus k_2], S_3[c_{i,3} \oplus k_3] \oplus k_4\right] \quad (۱)$$

که در آن، متغیرهای $S_0, \dots, S_3$ همان جعبه‌های جانشانی هستند (هریک از این جعبه‌های جانشانی تحت عمل ضرب معکوس‌پذیرند). با 2^{32} متن رمز و 2^{40} حدس کلید ممکن، باید $2^{32} \times 2^{40} = 2^{72}$ مقدار مختلف را جمع کنیم که تقریباً برحسب مقدار محاسبات حدود 2^{64} عمل رمزگذاری می‌شود.

برای هر k جمع جزئی x_k را به هر متن رمز c به‌صورت معادله (۲) مرتبط می‌کنیم.

$$x_k := \sum_{j=0}^{k} S_j[c_j \oplus k_j] \quad (۲)$$

این رابطه به ما نگاشت$(c_0, c_1, c_2, c_3) \mapsto (x_k, c_{k+1}, \dots, c_3)$ را می‌دهد که (اگر مقادیر $k_0, \dots, k_k$ را بدانیم) آن را به هر متن رمزی می‌توانیم اعمال کنیم. ما با 2^{32} قالب از متن رمز آغاز می‌کنیم. مقادیر k_0 و k_1 را حدس زده و تعداد رخداد سه‌تایی‌های (x_1, c_2, c_3) در لیست را محاسبه می‌کنیم. برای هر i ما مقدار سه بایت

$$(S_0[c_{i,0} \oplus k_0] \oplus S_1[c_{i,1} \oplus k_1], c_{i,2}, c_{i,3})$$

را به‌عنوان تابع متن رمزی i ام و کلید حدس زده‌شده محاسبه می‌کنیم. سپس می‌شماریم که چند بار هر مقدار ۳ بایتی در طول این محاسبه روی می‌دهند. با توجه به این‌که 2^{24} مقدار ممکن برای سه بایت وجود دارد، نیازی نیست همه (x_1, c_2, c_3) را لیست کنیم، بلکه تعداد رخداد هر سه‌تایی را می‌شماریم. سپس k_2 را حدس‌زده و تعداد رخداد هر زوج (x_2, c_3) را محاسبه می‌کنیم. سپس k_3 را حدس‌زده و تعداد رخداد مقدار x_3 را محاسبه می‌کنیم و درنهایت k_4 را حدس زده و جمع دلخواه را محاسبه می‌کنیم. همه جمع‌ها با استفاده از عمل XOR انجام می‌شود. چون برای هر بار شمارش یک بیت کافی است، فضای موردنیاز برای 2^{24} شمارنده تنها 2^{24} بیت است.

در مرحله اول ۱۶ بیت را حدس زدیم و 2^{32} متن رمزی را پردازش کردیم. لذا پیچیدگی این مرحله $2^{48} = 2^{32} \times 2^{16}$ است. در مرحله بعدی ما ۲۴ بیت را حدس می‌زنیم اما تنها باید 2^{24} سه‌تایی را پردازش کنیم. لذا در این بار پیچیدگی $2^{48} = 2^{24} \times 2^{24}$ است. بنابراین کل پیچیدگی شامل 2^{48} ارزیابی از معادله (۱) یا حدود 2^{50} محاسبه عملگر جعبه جانشانی است.

این مقدار محاسبه برای یک ساختار شامل 2^{32} متن رمزی (از ۶ ساختار ممکن) است. معمولاً اولین ساختار، تعداد زیادی از حدس‌های کلید غلط را حذف می‌کند، در ادامه باید گام اول محاسبه جمع جزئی را برای هر شش ساختار انجام دهیم.

برای بیان تک بایت r_4 در کلید و متن رمز ما فرمولی شبیه معادله (۱) داریم با این تفاوت که اینجا سه سطح، ۱۶ بایت متن رمز و ۲۱ بایت کلید داریم. فن جمع جزئی تنها در طول قسمت آخر محاسبه مفید است. درصورتی‌که متن رمزهای بیشتری نسبت به مقادیر ممکن برای نتیجه میانی وجود داشته باشد، این فن باعث ذخیره‌سازی می‌شود. با2^{32} زوج متن اصلی/ متن رمزی در یک ساختار، این فن تا دور پایانی محاسبه مفید نخواهد بود.

برای کلیدهای ۲۵۶ بیتی، هم ترازی[1] در الگوریتم تولید زیر کلید (نسبت به ۱۲۸ بیتی) متفاوت است. در دور دوم از رمز بومی حدس کلید دور آخر زیر کلید دور پنجم را به دست می‌دهد اما اطلاعاتی درباره کلید دور ششم نمی‌دهد. با کارکرد مشابه قبل، ما ۱۲۸ بیت (۱۶ بایت) کلید دور آخر را حدس زده و چهار بایت موردنظر را پس از دور ششم برای همه 2^{32} متن محاسبه می‌کنیم .هزینه این عملیات $2^{160} = 2^{32} \times 2^{128}$ جستجو خواهد بود. در مرحله بعدی ۱۶ بیت کلید یا بیشتر را با 2^{24} شمارنده تک‌بیتی حدس می‌زنیم. هزینه کل 2^{176} خواهد بود. مرحله‌های باقیمانده هزینه یکسانی خواهند داشت. بنابراین هزینه به ازای هر ساختار 2^{170} جستجو یا حدود 2^{170} رمزگذاری آزمایشی است. همچنین نیاز به ۵ ساختار پیش از شروع حدس کلید دور آخر داریم، بنابراین پیچیدگی زمانی این حمله حدود 2^{172} و پیچیدگی داده 2^{32} و پیچیدگی حافظه 2^{32} است (جدول ۱). این حمله نیز سریع‌تر از جستجوی جامع کلید برای کلید (یعنی 2^{256}) است.

۳-۳- حمله انتگرال دو دوری به رمز بومی

ایده دوم بهبود بر مبنای توازن بین زمان و داده با هدف افزایش پیچیدگی داده استوار است. می‌توانیم این ایده را برای شکستن دو دور از رمز بومی نیز توسعه دهیم. در ابتدا تعداد 2^{119} تا 2^{128} متن ایجاد می‌کنیم. این تعداد را به 2^{23} گروه تقسیم می‌کنیم و تمرکز حمله را بر یک مجموعه و این واقعیت که یک تک بایت در r_5 (بعد از عمل RK دور چهارم AES وقتی روی همه 2^{104}

[1] Alignment

رمزگذاری در مجموعه جمع شود) منجر به صفر می‌شود، معطوف می‌کنیم. بااین‌حال، این بایت در r_5 بستگی به‌کل متن رمز و ۲۱ بایت زیر کلید در پایان رمز دارد. حال ما باید فن جمع جزئی را اعمال کنیم. جهت حدس زدن ۴ بایت کلید دور نخست، ابتدا مجموعه را تعریف کرده و جمع‌های جزئی x_k را محاسبه کنیم. محاسبه جمع‌های جزئی در زمان 2^{104} بیت حافظه و کار معادل با 2^{202} رمزگذاری آزمایشی انجام می‌شود . نیاز به انجام این کار برای حدود ۴ گروه داریم. (در کل نیاز به ۲۶ مجموعه برای دست‌یابی به یک راه‌حل منحصربه‌فرد داریم، اما بار محاسبات بیشتر روی ۴ مجموعه اول است.) پیچیدگی کلی حمله 2^{204} رمزگذاری است؛ بنابراین، این حمله سریع‌تر از جستجوی جامع کلید برای کلید ۲۵۶ بیتی است.

هر بایت از r_5 بستگی به ۲۱ بایت زیرکلید (یعنی ۱۶ بایت از k_8 ، ۴ بایت از k'_7 و یک بایت از k'_6) دارد. ثابت کردن کلید دور آخر k_8، باعث تعیین ۲ بایت از ۴ بایت k'_7 می‌شود. بسته به اینکه کدام بایت r_5 هدف است، احتمالاً بایت زیر کلید مرتبط ازk'_6 است. به عبارت دقیق‌تر با انتخاب ۳ ستون (۱۲ بایت) از k_8 می‌توان ۲ ستون از k'_7 را تعریف کرد و ستون چهارم k_8 نیز یک ستون از ستون‌های k'_6 را تعریف می‌کند. در هر ستون از k'_7 یک بایت زیر کلید را که برای حمله نیاز داریم می‌یابیم. به‌عبارت‌دیگر، ثابت کردن k'_8 (حتی تنها سه ستون ازk'_8) ۲ بایت کلید مفید از k'_7 را به ما می‌دهد.

برای تشریح حمله [۱۸]، به فن جمع جزئی از منظر دیگری می‌نگریم. برای حمله به دو دور رمز بومی منهای لایه انتشار دور دوم، مجموع مقادیر گرفته‌شده توسط یک بایت را در 2^{104} رمزگذاری مربوط به یک گروه می‌گیریم. بدین منظور معادله (۱) را ۵ بار ارزیابی می‌کنیم. ابتدا ۴ بار ارزیابی می‌کنیم و سپس (در بار پنجم) ۴ نتیجه به‌دست‌آمده را به‌جای $c_{i,0}, \dots, c_{i,3}$ جایگزین می‌کنیم. هر ارزیابی از معادله (۱) با محاسبه شمارنده در پیمانه برای

$$(c_0, c_1, c_2, c_3, < other >)$$

انجام می‌شود. جایی که بایت c_i و کلیدهای مرتبط در یک ستون قرار می‌گیرند. این ارزیابی در گام‌های زیر انجام می‌شود،

- حدس دو بایت کلید k_0 و k_1 و محاسبه شمارنده در پیمانه ۲ برای

$$(x_{0,1}, c_1, c_2, c_3, < other >)$$

- حدس یک بایت کلید k_2 و محاسبه شمارنده در پیمانه ۲
- حدس یک بایت کلید k_3 و محاسبه شمارنده در پیمانه ۲

برای محاسبه جمع‌های جزئی کاری معادل با 2^{202} رمزگذاری آزمایش انجام می‌شود. ما برای انجام این کار نیاز به حدود چهار گروه داریم. (با این‌که در کل نیاز به ۲۶ مجموعه برای دست‌یابی به یک راه‌حل منحصربه‌فرد داریم، اما بارکاری بیشتر روی چهار مجموعه اول است.) بنابراین، پیچیدگی زمانی حمله 2^{206}= 2^{202}× ۲۶ رمزگذاری و پیچیدگی داده 2^{128} زوج متن اصلی/متن رمزی و پیچیدگی حافظه 2^{32} است (جدول ۱). بنابراین، این حمله سریع‌تر از جستجوی جامع کلید برای کلید (یعنی 2^{256}) است.

جدول (۱): پیچیدگی حملات پیشنهادی

تعداد دورهای حمله انتگرال	پیچیدگی زمانی	پیچیدگی داده	پیچیدگی حافظه
یک دور رمز بومی	2^{172}	2^{32}	2^{32}
دو دور رمز بومی	2^{206}	2^{128}	2^{32}
جستجوی کامل فضای کلید	2^{256}	۱	۱

۴- راه‌کارهای مقاوم‌سازی رمز قالبی بومی

همان‌طور که قبلاً گفته شد در طراحی رمزهای قالبی علاوه‌بر توجه به استفاده از اولیه‌های رمزنگاری امن و کارآمد برای مقاومت در برابر حملات خطی و تفاضلی، لازم است به استحکام ساختاری ناشی از ترکیب این اولیه‌ها نیز به‌اندازه کافی توجه شود تا مقاومت این رمزها در مقابل حملات ساختاری نیز حفظ شود. به‌عنوان نمونه در رمز قالبی بومی دیده شد که مقاومت رمز در برابر حملات خطی و تفاضلی را به‌خوبی تضمین‌شده ولی به ترکیب ساختاری آن به‌اندازه کافی توجه نشده است. با توجه به این‌که حمله انتگرال انجام‌شده در این مقاله به دو دور از رمز قالبی بومی انجام‌شده است، پیشنهاد می‌شود طراحان به‌منظور افزایش تغییرات آرایش بایت‌های فعال در هر دور از رمز بومی، ساختار این رمز را به‌طور مناسبی تغییر بدهند. به‌عنوان مثال به نظر می‌رسد با افزایش تعداد دور رمز بومی به‌اندازه حداقل یک دور دیگر (به‌عنوان حاشیه امنیتی) و افزایش تعداد جعبه‌های جانشانی فعال به‌اندازه حداقل یک جعبه جانشانی دیگر در هر دور، می‌توانند این رمز بومی را در مقابل حمله انتگرال مورد بحث در این مقاله مقاوم کنند. همچنین برای مقاوم‌سازی رمز بومی در مقابل حمله انتگرال طراحان می‌توانند به‌جای استفاده از AES چهار دوری (که حمله انتگرال شناخته شده دارد) در ساختار پیشنهادی از AES هشت دوری یا یک رمز قالبی با ساختاری غیر از ساختار جانشانی- جایگشتی (که مقاومت بیشتری در برابر حمله انتگرال داشته باشد) استفاده کنند.

۵- نتیجه‌گیری

رمز بومی مورد اشاره در بالا که در هر دور آن از الگوریتم رمز AES چهاردوری استفاده می‌کند، الگوریتمی قالبی با خواص انتشار به‌نسبت خوب است. ما برای اولین بار در این مقاله نشان دادیم که این رمز بومی در دو دور ابتدایی‌اش نسبت به تحلیل انتگرال آسیب‌پذیر است. این حمله با استفاده از تمایزگر انتگرال AES چهار دوری و فن جمع جزئی به یک دور و به دو دور از این رمز و با پیچیدگی کمتر از جستجوی جامع انجام شده است.

بر اساس مقادیر جدول (۱)، برای حمله پیشنهادی اول مقدار پیچیدگی حافظه 2^{32} (بر اساس [۱۹-۲۱])، پیچیدگی داده 2^{32} متن اصلی و پیچیدگی زمانی 2^{172} عمل رمزگذاری است که با توجه به طول کلید رمز، کمتر از مقدار پیچیدگی حمله جستجوی جامع فضای کلید (2^{256}) است و برای حمله پیشنهادی دوم نیز مقدار پیچیدگی حافظه 2^{32} (بر اساس [۱۹-۲۱])، پیچیدگی داده 2^{128} متن اصلی و پیچیدگی زمانی 2^{206} عمل رمزگذاری است که با توجه به طول کلید رمز، کمتر از مقدار پیچیدگی حمله جستجوی جامع فضای کلید (2^{256}) است و درنتیجه یک حمله میان‌بر مؤثر محسوب می‌شود.

نتایج این مقاله نشان می‌دهند که در طراحی رمزهای قالبی جدید، لازم است علاوه‌بر، استفاده از اولیه‌های رمزنگاری قوی برای مقاومت رمز در برابر حملات خطی، تفاضلی و جبری به استحکام ساختاری کافی حاصل از ترکیب این اولیه‌ها نیز برای مقاومت رمز در برابر حملات ساختاری توجه شود.

۶- منابع

[1] A. Mirghadri, B. Madadi, and Y. Pourebrahim, "A New Block Cipher Algorithm for Wireless Sensor Networks," Passive Defense Sci. & Tech., vol. 3, pp. 169-177, 2011.

[2] J. Daemen, L. R. Knudsen, and V. Rijmen, "The block cipher square," in FSE, Springer, 1997.

[3] C. H. Lim, "A revised version of CRYPTON: CRYPTON V1. 0," in FSE, Springer, 1999.

[4] J. Daemen and V. Rijmen, "The design of Rijndael: AES-the advanced encryption standard," Science & Business Media, Springer, 2013.

[5] S. Lucks, "The saturation attack—a bait for Twofish," in International Workshop on Fast Software Encryption, Springer, 2001.

[6] L. KnudsenM and D. Wagner, "Integral cryptanalysis," in Fast Software Encryption, Springer, 2002.

[7] M. Matsui, "New block encryption algorithm MISTY," in FSE, Springer, 1997.

[8] J. Wallen, "Design principles of the kasumi block cipher," in Proceedings of the Helsinki University of Technology Seminar on Network Security, 2000.

[9] X. Sun and X. Lai, "Improved Integral Attacks on MISTY1," in Selected Areas in Cryptography, Springer, 2009.

[10] H. Gilbert and M. Minier, "A Collision Attack on 7 Rounds of Rijndael," in AES Candidate Conference, 2000.

[11] Y. Li, W. Wu, and L. Zhang, "Improved Integral Attacks on Reduced-Round CLEFIA Block Cipher," in WISA, Springer, 2011.

[12] Y. Sasaki and L. Wang, "Comprehensive study of integral analysis on 22-round LBlock," in International Conference on Information Security and Cryptology, Springer, 2012.

[13] H. Zhang and W. Wu, "Structural Evaluation for Simon-Like Designs against Integral Attack," in International Conference on Information Security Practice and Experience, Springer, pp. 194-208, 2016.

[14] P. Morawiecki, "Practical Attacks on the Round-reduced PRINCE," IET Information Security, vol. 11, no. 3, pp. 146-151, 2016.

[15] Y. Todo, "Integral cryptanalysis on full MISTY1," Journal of Cryptology, vol. 20, no. 3, pp. 920-959, 2017.

[16] A. Mirghdri and M. Yussefipour, "One Secure Block Cipher Based on Recursive Diffusion Layers and Four Rounds of AES," Journal of Electronical & Cyber Defence, vol. 4, no. 2, pp. 77-84, 2016.

[17] L. R. Knudsen and M. Robshaw, "The block cipher companion," Springer Science & Business Media, 2011.

[18] A. Tajadod, "Structural Cryptanalysis of Block Ciphers and Offer an Attack on Block Cipher with a Hybrid Structure," M. SC. Thesis, IHCU, Iran, 2017.

[19] S. Rønjom, N. G. Bardeh, and T. Helleseth, "Yoyo Tricks with AES," in International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2017.

[20] L. Grassi, C. Rechberger, and S. Rønjom, "Subspace trail cryptanalysis and its applications to AES," IACR Transactions on Symmetric Cryptology, vol. 20, pp. 192-225, 2016.

[21] S. Lucks, "Attacking Seven Rounds of Rijndael under 192-bit and 256-bit Keys," in AES Candidate Conference, 2000.

Journal of Electronical & Cyber Defence
Vol. 7, No. 3, 2019, Serial No. 27

Structural Analysis based on Integral Characteristic of a Reduced Round Block Cipher with Making an Improvement

B. Khadem*, A. Tajadod, K. Bakhtiari

*Imam Hossein Comprehensive University

(Received: 05/01/2019, Accepted: 11/03/2019)

ABSTRACT

In symmetric encryption, block ciphers are more important than stream ciphers, message authentication codes and authenticated encryption schemes, because they are often used as the secure building blocks of other types. Structural analysis is one of the block ciphers cryptanalysis methods which performs attacks without prior knowledge of their internal operators such as permutations and s-boxes. In this paper, using a known 4-rounds integral distinguisher on AES, for the first time, two integral attacks are made on a new native block cipher with a 256-bit key and block length. These attacks, are made on 1-round and 2-rounds of this 3-rounds block cipher due to the weaknesses of the round function. The memory, data, and time complexities of the best attack in this article are 232 bytes, 2128 plaintexts and 2206 encryption operations. Given the key's length, the complexity of the attack is less than the complexity of the comprehensive search key space attack (2256) and therefore it is an effective shortcut attack. In addition, some recommendations are made to improve this native cipher.

Keywords: Block Cipher, Structural Analysis, Integral Characteristic

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