نشریه علمی "پدافند الکترونیکی و سایبری"
سال هشتم، شماره ۴، زمستان ۱۳۹۹، ص ۱۳۷-۱۲۹

علمی- پژوهشی

ارائه کران بالا برای احتمال مشخصه‌های تفاضلی پنج ساختار رمز قالبی دارای امنیت اثبات‌پذیر

جواد علیزاده[1*]، قاسم جمشیدیان[2]، احمد گائینی[3]، عبدالرسول میرقدری[4]
۱- استادیار، ۲- کارشناسی ارشد، ۳- استادیار و ۴- دانشیار دانشگاه جامع امام حسین (ع)
(دریافت: ۱۳۹۸/۱۰/۲۵، پذیرش: ۱۳۹۹/۰۵/۱۵)

چکیده

رمزهای قالبی نقش مهم در تأمین امنیت اطلاعات و ارتباطات و پدافند الکترونیکی و سایبری دارند. یک رمز قالبی امن می‌بایست در برابر حملات شناخته‌شده مانند حمله تفاضلی امن باشد. در سال ۲۰۰۸ کیم و همکاران هفت ساختار رمز قالبی با ویژگی امنیت اثبات‌پذیر در برابر حمله تفاضلی ارائه کردند که از آن‌ها برای طراحی برخی رمزهای قالبی استفاده شده است. در این مقاله کران بالای مشخصه‌های تفاضلی با تعداد دورهای مختلف، برای پنج ساختار از ساختارهای ذکرشده ارائه می‌شود. برای این کار از روش تحلیل تفاضلی خودکار مبتنی بر برنامه‌ریزی خطی برای شمارش حداقل تعداد تابع‌های دور فعال استفاده شده است. این روش به‌طور رسمی توسط موها و همکارانش در سال ۲۰۱۱ ارائه شد و تاکنون برای تحلیل و ارزیابی رمزهای قالبی متعددی به‌کار گرفته شده است. بدین ترتیب نشان داده می‌شود مشخصه‌های تفاضلی پنج دوری از ساختارهای ذکرشده، کران بالای p^4 دارند که در مقایسه با کران‌های تفاضلی ارائه‌شده توسط کیم و همکاران مورد تأیید هستند. منظور از p مشخصه تفاضلی تابع دور مورد استفاده در این ساختارها است.

کلیدواژه‌ها: رمز قالبی، مشخصه تفاضلی، تفاضل، کران امنیتی، برنامه‌ریزی خطی عدد صحیح آمیخته

۱- مقدمه

با توجه به گسترش روزافزون و تنوع فناوری‌های ارتباطی مانند شبکه‌های اجتماعی، شناسایی مبتنی بر بسامد رادیویی[1] و اینترنت اشیا[2]، اهمیت اطلاعات و امنیت آن بیشتر از قبل آشکار می‌شود. ابزار اصلی برای تأمین امنیت اطلاعات و ارتباطات، الگوریتم‌ها و پروتکل‌های رمزنگاری هستند. از آنجا که خود پروتکل‌های رمزنگاری از الگوریتم‌های رمزنگاری استفاده می‌کنند، بنابراین، می‌توان گفت استفاده از الگوریتم‌های رمزنگاری امن شرط لازم برای اطمینان از محفوظ ماندن اطلاعات است. رمزهای قالبی[3] یک دسته مهم از الگوریتم‌های رمزنگاری هستند که در مقایسه با الگوریتم‌های رمزنگاری از نوع‌های دیگر، مانند رمزهای دنباله‌ای[4] توجه بیشتری به آن‌ها شده است. برای تأیید این گفته می‌توان به وجود استانداردهایی مانند AES [۱]، CLEFIA [۲]، PRESENT [۳] و HIGHT [۴] اشاره کرد که از نوع رمزهای قالبی هستند. علاوه بر این می‌توان به برگزاری دو مسابقه جهانی در زمینه رمزهای متقارن، به نام‌های مسابقه CAESAR[5] (توسط انجمن بین‌المللی رمز[6]) [۵] و مسابقه LWC[7] (توسط موسسه NIST[8]) [۶] اشاره کرد که اکثر نامزدهای این مسابقات از نوع رمزهای قالبی هستند. در عمل، امنیت یک رمز قالبی، به‌عنوان مقاومت آن در برابر حملات شناخته‌شده تعریف می‌شود. به همین دلیل طراحان تلاش می‌کنند تا روش‌های طراحی جدید را طوری به‌کار بگیرند که بتوانند ادعایی برای امنیت رمز خود داشته باشند. در پاسخ به این روش‌ها، تحلیلگران نیز روش‌های حمله قبلی را بهبود داده و حتی روش‌های جدید ارائه می‌کنند. برای مثال در این مورد می‌توان به پیشرفت‌ها در حوزه تحلیل تفاضلی [۷] و تحلیل خطی [۸] و در رأس آن‌ها تلاش‌ها برای خودکارسازی و کامپیوتری کردن این تحلیل‌ها اشاره کرد. یکی از این تلاش‌ها، استفاده از برنامه‌ریزی خطی[9] برای بهبود تحلیل‌های تفاضلی، خطی، تفاضلی ناممکن [۹] و هم‌بستگی صفر [۱۰] روی رمزهای قالبی است. اگر چه استفاده از برنامه‌ریزی خطی برای تحلیل

*رایانامه نویسنده مسئول: jaalizadeh@ihu.ac.ir
[1] Radio-Frequency Identification (RFID)
[2] Internet of Things (IoT)
[3] Block Ciphers
[4] Stream Ciphers
[5] Competition for Authenticated Encryption: Security, Applicability, and Robustness
[6] International Association for Cryptologic Research (IACR)
[7] Lightweight Cryptography
[8] National Institute of Standards and Technology
[9] Linear Programming

رمزهای متقارن بـه سـال ۲۰۰۹ و کـار بروقـوف[1] و همکـاران در [۱۱] بر می‌گردد ولی تحول اساسـی در ایـن زمینـه بعـد از کـار موهـا[2] و همکـاران در [۱۲] بـه وقـوع پیوسـت. در حـال حاضـر اسـتفاده از برنامـه‌ریـزی خطـی در تحلیـل رمزهـای متقـارن، به‌خصوص رمزهای قالبی، به‌قدری اهمیت پیداکرده است که اکثر تحلیل‌های منتشرشده مبتنی بر این روش هستند. برای مثـال در این مورد می‌توان به تحلیل تفاضلی ناممکن در مدل کلید مرتبط رمز قالبی SIMECK [۱۳]، تحلیل‌های تفاضـلی نـاممکن و هـم-بستگی صفر رمز قالبی SKINNY [۱۴]، تحلیل تفاضلی LED64 و Midori64 [۱۵]، تحلیل مکعبی شـیوه‌هـای عملکـرد کلیـددار Keccak [۱۶]، تحلیل تفاضـلی رمـز قـالبی GIFT [۱۷]، تحلیـل خطی طرح رمزگذاری همـراه بـا احـراز اصـالت MORUS [۱۸]، تحلیل ساختارهای فیستلی و بهبود ساختار فیستلی تعمیم‌یافته[3] (GFS) نـوع دو [۱۹] و تحلیـل خطـی دو نسـخه از رمـز قـالبی SIMON [۲۰] اشاره کرد.

در سال ۲۰۰۸، کیم[4] و همکاران [۲۱]، هفت ساختار جدید رمز قالبی بانام‌های ساختارهای نوع فیستلی A، نـوع فیسـتلی B، CLEFIA، MISTY-FO-A، MISTY-FO-B، MISTY-FO-C و MISTY-FO-D معرفی و نشان دادند که این سـاختارها در برابـر تحلیل تفاضلی، امنیت اثبات‌پذیر دارند. آن‌ها امنیت سـاختارهای خود را اثبات کرده و برای دو دور از ساختار نوع فیستلی A و یک دور از ساختار نوع فیسـتلی B کـران بـالای p^2 و بـرای پـنج دور CLEFIA، MISTY-FO-A، MISTY-FO-B، MISTY-FO-C و MISTY-FO-D به ترتیب کران‌های بالا $p^4 + 2p^5$، p^4، p^4، $2p^4$ و $2p^4$ ارائه کردند که در آن‌ها p ماکسیمم احتمال تفاضـلی یـک تابع دور مانند F است که فرض می‌شود در ساختارهای ذکرشـده به‌کار می‌رود. کار کیم و همکاران از آن جهت اهمیت دارد که بـا توجه به ساختارهای ارائه شده و کران‌های امنیتی آن‌ها می‌تـوان رمزهای قالبی با امنیت اثبات‌پذیر در برابر تحلیل تفاضلی به‌دست آورد. توجه شود که هر تفاضل بـرای یـک رمـز قـالبی بـا تعـداد دورهای مشخص، حاصل جمع چند مشخصه تفاضـلی بـا تفاضـل ورودی و خروجی یکسان و تفاضلات میانی متفاوت است. کـیم و همکـاران از ویژگـی‌هـا و روابـط احتمـالاتی اسـتفاده و بـرای تفاضل‌های پنج دوری ساختارهای ذکرشـده، کـران‌هـای امنیتـی ارائه کردند و در مورد احتمال‌های ممکـن یـا بیشـترین احتمـال ممکن برای مشخصه‌های تفاضلی این سـاختارها بحثـی نکردنـد. علاوه بر این ایشان تنها بـرای پـنج دور از سـاختارهای ذکرشـده اثبات‌های امنیتی ارائه دادند و در مورد تعداد دورهای بیشتر آن‌ها بحث نکردند.

[1] Borghoff
[2] Mouha
[3] Generalized Feistel Structures (GFS)
[4] Kim

۱-۱- دستاوردها

در این مقاله پنج ساختار از ساختارهای ارائه‌شده در [۲۱]، به نام‌هـای CLEFIA، MISTY-FO-A ، MISTY-FO-B، MISTY-FO-C و MISTY-FO-D، با هدف به‌دسـت آوردن مشخصـه‌هـای تفاضلی برای تعداد دورهای مختلف آن‌ها، مورد تحلیل و ارزیـابی قرار می‌گیرند. برای این کار از برنامه‌ریزی عدد صـحیح آمیختـه[5] (MILP) استفاده شده و حداقل تعداد تابع‌های F (تابع‌هـای دور) فعال برای دورهای مختلف رمزهای قالبی مبتنی بر این ساختارها محاسبه می‌شـود. یـادآوری مـی‌شـود ایـن روش در سـال ۲۰۱۱ توسط موها و همکارانش [۱۲] ارائه شد و تـاکنون بـرای تحلیـل ساختارها و الگوریتم‌های رمزنگاری مختلف استفاده شـده اسـت. برای مثال در [۱۹] سجادیه و وزیری با کـاربرد ایـن روش بـرای تحلیل ساختارهای فیستلی، توانسـتند امنیـت سـاختارهای GFS نوع دو را با استفاده از سازوکار تعویض جریان[6] بهبود دهند.

با توجه به نتایج تحلیل در این مقاله مشخص می‌شـود بـرای پنج دور از رمزهای قالبی مبتنی بر ساختارهای ذکر شده، حداقل چهار تابع F فعال وجود دارد. بنابراین، پنج دور این رمزهـا بـرای مقاومت در برابر تحلیل تفاضلی، مشخصه‌هـای تفاضـلی بـا کـران بالای p^4 را خواهند داشت که در مقایسه با کران‌های تفاضلی p^4، $p^4 + 2p^5$ و $2p^4$، مورد تأیید هستند. مقایسه نتایج تحلیـل ایـن مقاله با نتایج اثبات‌های امنیتی ارائه‌شده در [۲۱] مطابق جـدول (۱) خلاصه می‌شود. با توجه به این جدول می‌توان گفت که کران بالای مشخصـه تفاضـلی و تفاضـل پـنج دوری بـرای دو سـاختار MISTY-FO-A و MISTY-FO-B یکسان است. توجـه شـود کـه فرض می‌شود تابع دور بـه‌کاررفتـه (تـابع F) در همـه سـاختارها یکسان بوده و بیشترین احتمال تفاضلی برای آن برابر p باشد.

جدول (۱): مقایسه کران‌های تفاضل‌ها و مشخصه‌های تفاضلی پنج ساختار رمز قالبی

نام ساختار	تعداد دور	کران تفاضلی ارائه‌شده در [۲۱]	کران مشخصه تفاضلی ارائه‌شده در این مقاله
CLEFIA	۵	$p^4 + 2p^5$	p^4
MISTY-FO-A	۵	p^4	p^4
MISTY-FO-B	۵	p^4	p^4
MISTY-FO-C	۵	$2p^4$	p^4
MISTY-FO-D	۵	$2p^4$	p^4

در این مقاله علاوه بر اینکه مشخصه‌های تفاضلی پـنج دوری از ساختارها در نظر گرفته‌شده و کران بالا برای آن‌ها حاصل شده است، این کار برای تعداد دورهای مختلف این ساختارها نیز انجام می‌شود که در مقایسه با [۲۱] می‌توان در مـورد تعـداد دورهـای بیشتر این ساختارها نیز اظهارنظر کرد.

[5] Mixed Integer Linear Programming (MILP)
[6] Switching Mechanism

۱-۲- ساختار مقاله

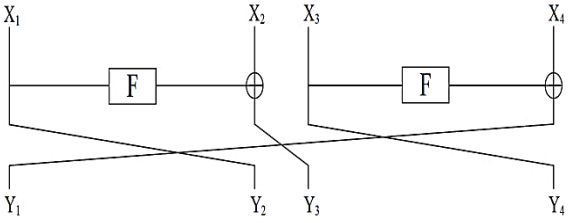
این مقاله به این ترتیب سازمان‌دهی شده است: در بخش (۲)، پنج ساختار رمز قالبی به نام‌های CLEFIA، MISTY-FO-A، MISTY-FO-B، MISTY-FO-C و MISTY-FO-D معرفی می‌شوند. در بخش (۳)، روش تحلیل تفاضلی مبتنی بر برنامه‌ریزی خطی معرفی می‌شود. در بخش (۴)، تحلیل تفاضلی ساختارهای معرفی‌شده در بخش (۲)، با استفاده از برنامه‌ریزی خطی عدد صحیح آمیخته تشریح شده و نتایج تحلیل برای دورهای مختلف آن‌ها ارائه می‌شود. در نهایت، جمع‌بندی و نتیجه‌گیری مقاله در بخش (۵) آورده می‌شود.

۲- ساختارهای رمز قالبی با امنیت اثبات‌پذیر در برابر تحلیل تفاضلی

در این بخش، ساختارهای رمز قالبی CLEFIA، MISTY-FO-A، MISTY-FO-B، MISTY-FO-C و MISTY-FO-D ارائه‌شده در [۲۱]، معرفی و قضایای مربوط به اثبات امنیت آن‌ها در برابر تحلیل تفاضلی بیان می‌شود. از آنجا که ساختارهای MISTY-FO-B و MISTY-FO-D به ترتیب شبیه ساختارهای MISTY-FO-A و MISTY-FO-C هستند، از توصیف آن‌ها در این بخش صرف‌نظر می‌شود. برای آشنایی با این ساختارها و جزییات مربوط به بررسی امنیت آن‌ها در برابر تحلیل تفاضلی می‌توان به پیوست (الف) مراجعه کرد. توجه شود در تمام ساختارهایی که در ادامه معرفی می‌شوند، تابع دور مورد استفاده به‌صورت $F_k: GF(2^n) \rightarrow GF(2^n)$ فرض می‌شود که در آن منظور از k کلید دور است. برای نمایش ساده تابع دور، از نمایش اندیس k اجتناب می‌شود و این تابع با F نشان داده می‌شود. همان‌طور که در بخش اول گفته شد، فرض می‌شود احتمال بهترین مشخصه تفاضلی برای تابع F برابر p باشد.

۱-۲- ساختار CLEFIA

یک دور از ساختار رمز قالبی CLEFIA را می‌توان مطابق شکل (۱) در نظر گرفت.



شکل (۱): یک دور ساختار رمز قالبی CLEFIA

با توجه به این شکل، برای تبدیل حالت ورودی $X = X_1 \| X_2 \| X_3 \| X_4$ به حالت خروجی $Y = Y_1 \| Y_2 \| Y_3 \| Y_4$ (منظور از نماد $\|$، الحاق دو رشته بیت به یکدیگر است)، محاسبات زیر انجام می‌شود:

$$Y_1 = F(X_3) \oplus X_4 ,$$
$$Y_2 = X_1 ,$$
$$Y_3 = F(X_1) \oplus X_2 ,$$
$$Y_4 = X_3 .$$

در [۲۱]، امنیت یک رمز قالبی مبتنی بر ساختار رمز قالبی CLEFIA در برابر تحلیل تفاضلی مورد بررسی قرار گرفته و یک کران بالا برای آن ارائه شده است. این اثبات امنیتی در قضیه (۱) خلاصه شده است.

قضیه ۱ *(امنیت اثبات‌پذیر ساختار CLEFIA)*: فرض کنید یک رمز قالبی با تعداد دور $r \geq 5$، بر اساس ساختار CLEFIA و با تابع دور F طراحی شده باشد. فرض کنید تابع F دو سویی باشد و بهترین احتمال تفاضلی برای آن برابر p باشد. ثابت می‌شود بهترین احتمال تفاضلی برای $r \geq 5$ دور رمز قالبی ذکرشده، کران بالای $p^4 + 2p^5$ دارد.

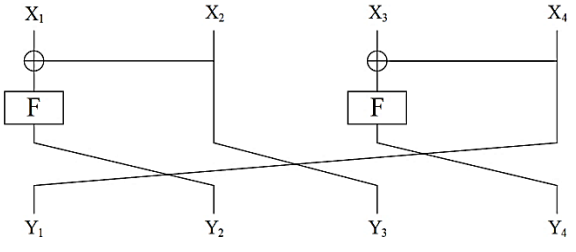
اثبات: [۲۱].

۲-۲- ساختار MISTY-FO-A

ساختارهای MISTY-FO با نوع‌های A، B، C و D که در این مقاله مطالعه شده‌اند، تعمیمی از ساختار رمز قالبی MISTY [۲۲] هستند. در این بخش ساختار MISTY-FO-A معرفی می‌شود. یک دور از این ساختار را می‌توان مطابق شکل (۲) در نظر گرفت.

با توجه به نمادگذاری معرفی‌شده در بخش (۲-۱)، برای تبدیل حالت ورودی X به حالت خروجی Y با استفاده از یک دور ساختار MISTY-FO-A که در آن از تابع دو سویی F به‌عنوان تابع دور استفاده می‌شود، محاسبات زیر لازم است.

$$Y_1 = X_4 ,$$
$$Y_2 = F(X_1 \oplus X_2),$$
$$Y_3 = X_2 ,$$
$$Y_4 = F(X_3 \oplus X_4).$$



شکل (۲): یک دور از ساختار MISTY-FO-A

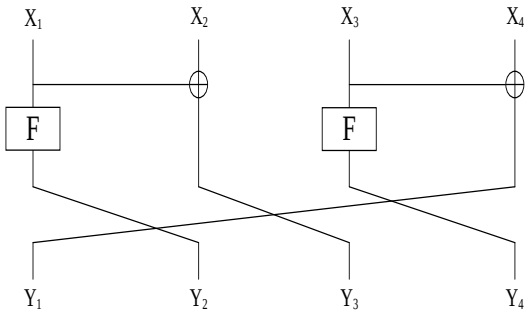
امنیت یک رمز قالبی مبتنی بر ساختار MISTY-FO-A (و به‌طور مشابه MISTY-FO-B) در برابر تحلیل تفاضلی مطابق قضیه (۲) خلاصه می‌شود.

قضیه ۲ *(امنیت اثبات‌پذیر ساختارهای MISTY-FO نوع A و B)*: فرض کنید یک رمز قالبی با تعداد دور $r \geq 5$، بر اساس ساختار MISTY-FO نوع A یا B و با تابع دور F طراحی شده باشد. فرض کنید تابع F دو سویی باشد و بهترین احتمال تفاضلی برای آن برابر p باشد. ثابت می‌شود بهترین احتمال تفاضلی برای $r \geq 5$ دور رمز قالبی ذکرشده، کران بالای p^4 دارد.

اثبات: [۲۱].

۲-۳- ساختار MISTY-FO-C

مشابه توضیحات بخش (۲-۲)، یک دور از ساختار MISTY-FO-C مطابق شکل (۳) قابل بیان است.



شکل (۳): یک دور از ساختار MISTY-FO-C

برای طراحی یک رمز قالبی با استفاده از ساختار MISTY-FO-C و تابع دو سویی F در آن، محاسبات زیر روی حالت ورودی X انجام می‌شود تا حالت خروجی Y حاصل شود.

$$Y_1 = X_3 \oplus X_4 ,$$
$$Y_2 = F(X_1),$$
$$Y_3 = X_1 \oplus X_2 ,$$
$$Y_4 = F(X_3).$$

مشابه بخش (۲-۲)، امنیت یک رمز قالبی مبتنی بر ساختار MISTY-FO-C (و همچنین MISTY-FO-D) در برابر تحلیل تفاضلی مطابق قضیه (۳) خلاصه می‌شود.

قضیه ۳ *(امنیت اثبات‌پذیر ساختارهای MISTY-FO نوع C و D)*: فرض کنید یک رمز قالبی با تعداد دور $r \geq 5$، بر اساس ساختار MISTY-FO نوع C یا D و با تابع دور F طراحی شده باشد. فرض کنید تابع F دو سویی باشد و بهترین احتمال تفاضلی برای آن برابر p باشد. ثابت می‌شود بهترین احتمال تفاضلی برای $r \geq 5$ دور رمز قالبی ذکرشده، کران بالای $2p^4$ دارد.

اثبات: [۲۱].

۳- تحلیل تفاضلی رمزهای قالبی با کمک برنامه‌ریزی عدد صحیح آمیخته

تحلیل تفاضلی یک حمله از نوع متن اصلی انتخابی[1] روی رمزهای متقارن است که در سال ۱۹۹۱ توسط بیهام و شامیر منتشر شد [۷]. در این حمله هدف به‌دست آوردن یک تفاضل ورودی و یک تفاضل خروجی خاص برای الگوریتم رمز یا دورهای کاهش یافته از آن است، به‌طوری‌که احتمال نگاشت تفاضل ورودی به تفاضل خروجی ذکرشده، احتمال بالایی باشد. از آنجا که عملگرهای خطی ویژگی تفاضلی را به‌طور قطعی و با احتمال یک منتقل می‌کنند، نقش اساسی برای مقاومت یک الگوریتم رمز متقارن در برابر حمله تفاضلی بر عهده عملگرهای غیرخطی مانند جعبه‌های جانشینی[2] است. به همین خاطر یک روش برای اثبات امنیت الگوریتم‌های دارای جعبه جانشینی در برابر تحلیل تفاضلی، به‌دست آوردن حداقل جعبه‌های جانشینی فعال در بهترین مشخصه تفاضلی است. برای این کار موها و همکارانش [۱۲] از برنامه‌ریزی خطی عدد صحیح آمیخته برای پیدا کردن حداقل تعداد جعبه‌های جانشینی فعال در تحلیل تفاضلی و خطی الگوریتم‌های رمزنگاری بایت‌گرا مانند رمز AES استفاده کردند. منظور از مدل برنامه‌ریزی خطی عدد صحیح و برنامه‌ریزی عدد صحیح آمیخته، به ترتیب مدل‌هایی هستند که متغیرهای آن اعداد صحیح و یا تعدادی از متغیرها اعداد صحیح باشند. کار موها و همکارانش در مقالاتی مانند [۲۳- ۲۴] روی الگوریتم‌های رمز مبتنی بر بیت بهبود داده شد.

شکل کلی مدل برنامه‌ریزی خطی عدد صحیح آمیخته از نوع کمینه مینیمم و با تابع هدف f را می‌توان به‌صورت زیر نشان داد:

$$\min f = \sum_i c_i x_i$$
$$S.t \quad x \in \{ Ax \leq b, x \geq 0\}$$
$$x \in Z^k \times \mathbb{R}^{n-k} \subseteq \mathbb{R}^n,$$

که در آن $(c_1 , \dots , c_n) \in \mathbb{R}^n$، $A \in \mathbb{R}^{m \times n}$ و $b \in \mathbb{R}^m$ است.

یک چالش در استفاده از برنامه‌ریزی خطی عدد صحیح آمیخته برای تحلیل و ارزیابی رمزهای قالبی، افزایش تعداد معادلات با افزایش تعداد دورهای رمز برای تحلیل است. این موضوع سبب می‌شود تا برای تحلیل رمزهای قالبی با تعداد دورهای بالا یا تعداد دورهای کامل نیاز به زمان بیشتری برای

[1] Chosen Plaintext
[2] Substation Box (Sbox)

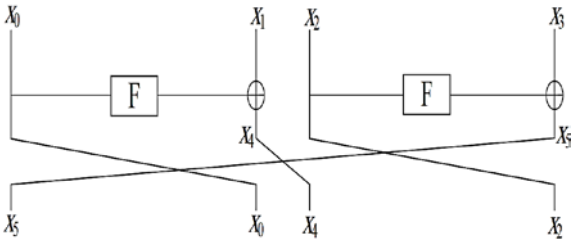
حل مدل برنامه‌ریزی خطی عدد صحیح آمیخته وجود داشته باشد. در مورد تحلیل برخی ساختارها روش‌هایی مطرح شده است که می‌توانند باعث کاهش تعداد معادلات و محدودیت‌های تصمیم‌گیری مدل برنامه‌ریزی خطی شوند. برای مثال سجادیه و وزیری یک روش برای کاهش تعداد معادلات و تحلیل تعداد دورهای بیشتر ساختارهای فیستلی تعمیم‌یافته در [۱۹] ارائه دادند. در این مقاله از روش موها و همکارانش استفاده شده است تا تعداد حداقل توابع دور فعال (توابع F) در یک حمله تفاضلی روی ساختارهای رمز قالبی که در بخش (۲) معرفی شدند، محاسبه شود. برای به‌دست آوردن تابع هدف و همچنین محدودیت‌های تصمیم‌گیری نیز از نمادگذاری و روش مدل‌سازی موها و همکارانش استفاده شده است.

۴- تحلیل ساختارهای رمز قالبی معرفی‌شده با استفاده از برنامه‌ریزی خطی عدد صحیح آمیخته

در این بخش، ساختارهای رمز قالبی معرفی‌شده در بخش (۲)، با استفاده از برنامه‌ریزی خطی عدد صحیح آمیخته مورد تحلیل تفاضلی قرار گرفته و برای اطمینان از صحت نتایج تحلیل و ارزیابی، نتایج حاصل با نتایج ارائه‌شده در [۲۱] مقایسه می‌شود. با توجه به شباهت ساختارهای MISTY-FO-A و MISTY-FO-C، به ترتیب با ساختارهای MISTY-FO-B و MISTY-FO-D از توضیحات روش ارزیابی در مورد دو ساختار اخیر اجتناب می‌شود. برای مشاهده نتایج تحلیل روی این ساختارها می‌توان به پیوست (ب) مراجعه کرد.

۴-۱- به‌دست آوردن حداقل تعداد Fهای فعال برای ساختار CLEFIA

مطابق توضیحات ارائه‌شده، برای به‌دست آوردن بیشترین احتمال مشخصه‌های تفاضلی یک رمز قالبی مبتنی بر ساختار CLEFIA، در وهله اول حداقل تعداد تابع‌های دور (F) فعال در بهترین مشخصه تفاضلی حساب می‌شود. سپس با فرض اینکه بالاترین احتمال برای نگاشت یک تفاضل ورودی به یک تفاضل خروجی خاص توسط تابع F برابر p باشد، می‌توان یک کران امنیتی بالا برای مشخصه‌های تفاضلی با تعداد دور متفاوت، به‌دست آورد. برای این منظور لازم است تا متناسب با مؤلفه‌های به‌کاررفته در ساختار CLEFIA، متغیرهای مناسب انتخاب شود. این کار مطابق شکل (۴) انجام می‌شود.



شکل (۴): تخصیص متغیرهای مناسب برای یک دور ساختار CLEFIA.

در هر دور از ساختار CLEFIA از دو عملگر XOR استفاده شده است. با توجه به شکل (۴)، متغیرهای (x_0, x_1, x_2, x_3) به‌عنوان متغیرهای ورودی در نظر گرفته می‌شود. از آن‌جا که عملگرهای XOR، باعث تولید متغیرهای جدید می‌شوند، خروجی XORها نیز با متغیرهای x_4 و x_5 نشان داده می‌شوند. متناسب با روش موها برای مدل کردن XOR، برای هر XOR استفاده از یک متغیر تصنعی[1] لازم است که در اینجا d_0 و d_1 به‌عنوان نشان‌دهنده این متغیرها در نظر گرفته می‌شوند.

با توجه به متغیرهای تعریف‌شده، محدودیت‌های مربوط به عملگر XOR سمت چپ به‌صورت زیر تعریف می‌شود.

$$x_0 + x_1 + x_4 \geq 2d_0$$
$$d_0 \geq x_0$$
$$d_0 \geq x_1$$
$$d_0 \geq x_4$$

برای عملگر XOR سمت راست به‌صورت مشابه عمل می‌شود. بنابراین، مدل برنامه‌ریزی خطی عدد صحیح آمیخته برای هر دور از ساختار CLEFIA دارای ۸ محدودیت ناشی از عملگرهای XOR در این دور است. با توجه به تعریف تابع هدف یک مدل برنامه‌ریزی خطی در بخش (۳)، در اینجا تابع هدف معادل مجموع متغیرهای متناظر با ورودی تابع دور F خواهد بود. در اینجا چگونگی به‌دست آوردن مدل برنامه‌ریزی خطی عدد صحیح آمیخته برای یک دور از ساختار CLEFIA تشریح شد. این کار برای تعداد دورهای متفاوت به روش مشابه انجام می‌شود. حال مساله‌ای که باقی می‌ماند این است که بتوان تابع هدف (مینیمم) برای تعداد دورهای متفاوت CLEFIA را حل کرد و پاسخ آن را به‌عنوان حداقل تعداد تابع‌های دور F فعال در نظر گرفت. برای این کار می‌توان از نرم‌افزارهایی مانند Groubi [۲۵] یا CPLEX [۲۶] استفاده کرد. در این مقاله از نرم‌افزار اخیر استفاده شده است. نتایج حل تابع هدف برای تعداد دورهای مختلف مطابق جدول (۲) خلاصه شده است.

[1] Dummy Variable

جدول (۲): حداقل تعداد تابع F فعال برای دورهای مختلف ساختار رمز قالبی CLEFIA

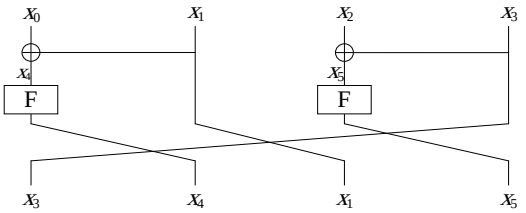
تعداد دور	حداقل تعداد F فعال	تعداد دور	حداقل تعداد F فعال
۱	۰	۱۴	۱۳
۲	۱	۱۵	۱۴
۳	۲	۱۶	۱۵
۴	۳	۱۷	۱۶
۵	۴	۱۸	۱۸
۶	۶	۱۹	۱۸
۷	۶	۲۰	۱۹
۸	۷	۲۱	۲۰
۹	۸	۲۲	۲۱
۱۰	۹	۲۳	۲۲
۱۱	۱۰	۲۴	۲۴
۱۲	۱۲	۲۵	۲۴
۱۳	۱۲		

۴-۲- مقایسه نتایج تحلیل با نتایج ارائه‌شده در [۲۱]

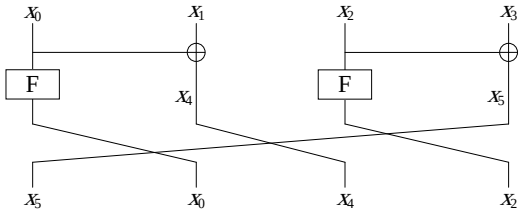
با توجه به جدول (۲)، می‌توان نتیجه گرفت اگر یک رمز قالبی با کاربرد تابع دور F با ماکسیمم احتمال تفاضلی برابر p، در ساختار رمز قالبی CLEFIA طراحی شود، بهترین مشخصه تفاضلی برای پنج دور این رمز حداکثر احتمال p^4 خواهد داشت. این کران با توجه به کران بالای احتمال تفاضل‌های پنج دوری، یعنی $p^4 + 2p^5$ [۲۱]، مورد تأیید است.

۴-۳- به‌دست آوردن حداقل تعداد Fهای فعال برای ساختارهای MISTY-FO-A و MISTY-FO-C

برای استخراج یک مدل برنامه‌ریزی خطی عدد صحیح آمیخته برای تحلیل تفاضلی ساختارهای MISTY-FO-A و MISTY-FO-C مشابه توضیحات بخش (۴-۱) عمل می‌شود. تخصیص متغیرها برای یک دور از ساختار MISTY-FO-A مطابق شکل (۵) و نیز این کار برای یک دور از ساختار MISTY-FO-C مطابق شکل (۶) انجام می‌گیرد.



شکل (۵): تخصیص متغیرهای مناسب برای یک دور ساختار MISTY-FO-A



شکل (۶): تخصیص متغیرهای مناسب برای یک دور ساختار MISTY-FO-C

بعد از به‌دست آوردن مدل برنامه‌ریزی خطی عدد صحیح آمیخته برای تحلیل تفاضلی دورهای مختلف از ساختارهای MISTY-FO-A و MISTY-FO-C و حل تابع هدف آن‌ها با کمک نرم‌افزار CPLEX، پاسخ‌های تابع‌های هدف، به‌عنوان حداقل تعداد تابع‌های دور F فعال، مطابق جدول‌های (۳) و (۴) خلاصه می‌شوند.

جدول (۳): حداقل تعداد تابع F فعال برای دورهای مختلف ساختار رمز قالبی MISTY-FO-A

تعداد دور	حداقل تعداد F فعال	تعداد دور	حداقل تعداد F فعال
۱	۰	۱۴	۱۳
۲	۱	۱۵	۱۴
۳	۲	۱۶	۱۵
۴	۳	۱۷	۱۶
۵	۴	۱۸	۱۸
۶	۶	۱۹	۱۸
۷	۶	۲۰	۱۹
۸	۷	۲۱	۲۰
۹	۸	۲۲	۲۱
۱۰	۹	۲۳	۲۲
۱۱	۱۰	۲۴	۲۴
۱۲	۱۲	۲۵	۲۴
۱۳	۱۲		

جدول (۴): حداقل تعداد تابع F فعال برای دورهای مختلف ساختار رمز قالبی MISTY-FO-C

تعداد دور	حداقل تعداد F فعال	تعداد دور	حداقل تعداد F فعال
۱	۰	۱۴	۱۳
۲	۱	۱۵	۱۴
۳	۲	۱۶	۱۵
۴	۳	۱۷	۱۶
۵	۴	۱۸	۱۸
۶	۶	۱۹	۱۸
۷	۶	۲۰	۱۹
۸	۷	۲۱	۲۰
۹	۸	۲۲	۲۱
۱۰	۹	۲۳	۲۲
۱۱	۱۰	۲۴	۲۴
۱۲	۱۲	۲۵	۲۴
۱۳	۱۲		

۴-۴- مقایسه نتایج تحلیل با نتایج ارائه‌شده در [۲۱]

با توجه به جدول (۳)، می‌توان نتیجه گرفت اگر یک رمز قالبی با کاربرد تابع دور F با ماکسیمم احتمال تفاضلی برابر p، در ساختار رمز قالبی MISTY-FO-A طراحی شود، بهترین مشخصه تفاضلی برای پنج دور این رمز حداکثر احتمال p^4 را خواهد داشت که معادل کران ارائه‌شده در [۲۱] برای تفاضل‌ها است. با توجه به این امر نتایج تحلیل تفاضلی ساختار MISTY-FO-A با استفاده از برنامه‌ریزی خطی تأیید می‌شود.

از طرف دیگر با توجه به جدول (۴)، می‌توان نتیجه گرفت اگر یک رمز قالبی با کاربرد تابع دور F با ماکسیمم احتمال تفاضلی برابر p، در ساختار رمز قالبی MISTY-FO-C طراحی شود، بهترین مشخصه تفاضلی برای پنج دور این رمز حداکثر احتمال p^4 را خواهد داشت. از طرف دیگر کران بالا برای احتمال تفاضل‌های پنج دوری ذکرشده در [۲۱] برابر $2p^4$ حساب شده است که نتایج حاصل را تأیید می‌کند.

۵- نتیجه‌گیری

روش‌های تحلیل خودکار رمزهای متقارن در مقایسه با روش‌های تحلیل که به‌صورت دستی انجام می‌شود، از دقت و سرعت بالایی برخوردار هستند. به همین دلیل این دسته از تحلیل‌ها در سال‌های اخیر مورد توجه تحلیلگران رمزنگاری قرار گرفته است. بسیاری از تحلیل‌های خودکار روی رمزهای متقارن، به‌خصوص رمزهای قالبی از روش برنامه‌ریزی خطی عدد صحیح آمیخته استفاده می‌کنند که یک روش برای حل مسائل بهینه‌سازی است. در این مقاله با استفاده از روش ذکر شده و ایده‌هایی که قبلاً در برخی مقالات مانند [۱۲] و [۱۹] مطرح شده است، امنیت پنج ساختار رمز قالبی در برابر تحلیل تفاضلی مورد بررسی قرار گرفت و تعداد حداقل توابع دور فعال (تابع F) در یک حمله تفاضلی روی دورهای مختلف این ساختارها محاسبه شدند. نتایج این کار در جدول (۵) ارائه شده است.

جدول (۵): حداقل تعداد تابع F فعال برای دورهای مختلف پنج ساختار رمز قالبی

تعداد دور	CLEFIA	MISTY-FO-A	MISTY-FO-B	MISTY-FO-C	MISTY-FO-D
۱	۰	۰	۰	۰	۰
۲	۱	۱	۱	۱	۱
۳	۲	۲	۲	۲	۲
۴	۳	۳	۳	۳	۳
۵	۴	۴	۴	۴	۴
۶	۶	۶	۶	۶	۶
۷	۶	۶	۶	۶	۶
۸	۷	۷	۷	۷	۷
۹	۸	۸	۸	۸	۸
۱۰	۹	۹	۹	۹	۹
۱۱	۱۰	۱۰	۱۰	۱۰	۱۰
۱۲	۱۲	۱۲	۱۲	۱۲	۱۲
۱۳	۱۲	۱۲	۱۲	۱۲	۱۲
۱۴	۱۳	۱۳	۱۳	۱۳	۱۳
۱۵	۱۴	۱۴	۱۴	۱۴	۱۴
۱۶	۱۵	۱۵	۱۵	۱۵	۱۵
۱۷	۱۶	۱۶	۱۶	۱۶	۱۶
۱۸	۱۸	۱۸	۱۸	۱۸	۱۸
۱۹	۱۸	۱۸	۱۸	۱۸	۱۸
۲۰	۱۹	۱۹	۱۹	۱۹	۱۹
۲۱	۲۰	۲۰	۲۰	۲۰	۲۰
۲۲	۲۱	۲۱	۲۱	۲۱	۲۱
۲۳	۲۲	۲۲	۲۲	۲۲	۲۲
۲۴	۲۴	۲۴	۲۴	۲۴	۲۴
۲۵	۲۴	۲۴	۲۴	۲۴	۲۴

با توجه به جدول (۵) مشخص می‌شود که پنج ساختار معرفی‌شده در حالت کلی از نظر امنیتی و حداقل تعداد تابع F فعال با هم تفاوتی ندارند و در یک سطح از امنیت قرار دارند. از طرفی با توجه به توضیحات ارائه‌شده در این مقاله، اگر پنج دور از

این ساختارها در نظر گرفته شده و مشخصه تفاضلی تابع دور F برابر p فرض شود، آنگاه احتمال مشخصه تفاضلی پنج دوری برای این ساختارها، دارای کران بالای p^4 خواهد بود. این کران در مقایسه با مقدار $p^4 + 2p^5$ (کران بالا برای تفاضل‌های پنج دوری ساختار CLEFIA)، مقدار $2p^4$ (کران بالا برای تفاضل‌های پنج دوری ساختار MISTY-FO-C و MISTY-FO-D) و مقدار p^4 (کران بالا برای تفاضل‌های پنج دوری ساختار MISTY-FO-A و MISTY-FO-B) که در [۲۱] ارائه شده است، مورد تأیید است.

۶- مراجع

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

[2] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-bit blockcipher CLEFIA," in International workshop on fast software encryption, Springer, pp. 181-195, 2007.

[3] A. Bogdanov et al., "PRESENT: An ultra-lightweight block cipher," in International Workshop on Cryptographic Hardware and Embedded Systems, Springer, pp. 450-466, 2007.

[4] D. Hong et al., "HIGHT: A new block cipher suitable for low-resource device," in International Workshop on Cryptographic Hardware and Embedded Systems, Springer, pp. 46-59, 2006.

[5] F. Abed, C. Forler, and S. Lucks, "General classification of the authenticated encryption schemes for the CAESAR competition," Computer Science Review, vol. 22, pp. 13-26, 2016.

[6] L. Bassham, Ç. Çalık, K. McKay, N. Mouha, and M. Sönmez Turan, "Profiles for the Lightweight Cryptography Standardization Process (Retired Draft)," National Institute of Standards and Technology, 2017.

[7] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," Journal of CRYPTOLOGY, vol. 4, no. 1, pp. 3-72, 1991.

[8] M. Matsui, "Linear cryptanalysis method for DES cipher," in Workshop on the Theory and Application of of Cryptographic Techniques, Springer, pp. 386-397, 1993.

[9] J. H. Cheon, M. Kim, K. Kim, L. Jung-Yeun, and S. Kang, "Improved impossible differential cryptanalysis of Rijndael and Crypton," in International Conference on Information Security and Cryptology, Springer, pp. 39-49, 2001.

[10] A. Bogdanov and M. Wang, "Zero correlation linear cryptanalysis with reduced data complexity," in International Workshop on Fast Software Encryption, Springer, pp. 29-48, 2012.

[11] J. Borghoff, L. R. Knudsen, and M. Stolpe, "Bivium as a mixed-integer linear programming problem," in IMA International Conference on Cryptography and Coding, Springer, pp. 133-152, 2009.

[12] N. Mouha, Q. Wang, D. Gu, and B. Preneel, "Differential and linear cryptanalysis using mixed-integer linear programming," in International Conference on Information Security and Cryptology, Springer, pp. 57-76, 2011.

[13] S. Sadeghi and N. Bagheri, "Security analysis of SIMECK block cipher against related-key impossible differential," Information Processing Letters, vol. 147, pp. 14-21, 2019.

[14] S. Sadeghi, T. Mohammadi, and N. Bagheri, "Cryptanalysis of reduced round SKINNY block cipher," IACR Transactions on Symmetric Cryptology, pp. 124-162, 2018.

[15] L. Sun, W. Wang, and M. Wang, "More accurate differential properties of LED64 and Midori64," 2018.

[16] W. Bi, X. Dong, Z. Li, R. Zong, and X. Wang, "MILP-aided cube-attack-like cryptanalysis on Keccak Keyed modes," Designs, Codes and Cryptography, vol. 87, no. 6, pp. 1271-1296, 2019.

[17] B. Zhu, X. Dong, and H. Yu, "MILP-based differential attack on round-reduced GIFT," in Cryptographers' Track at the RSA Conference, Springer, pp. 372-390, 2019.

[18] S. SADEGHI and N. BAGHERI, "Linear Cryptanalysis of Reduced-round Versions of MORUS," 2016.

[19] M. Sajadieh and M. Vaziri, "Using MILP in Analysis of Feistel Structures and Improving Type II GFS by Switching Mechanism," in International Conference on Cryptology in India, Springer, pp. 265-281, 2018.

[20] M. A. Abdelraheem, J. Alizadeh, H. A. Alkhzaimi, M. R. Aref, N. Bagheri, and P. Gauravaram, "Improved linear cryptanalysis of reduced-round SIMON-32 and SIMON-48," in International Conference on Cryptology in India, Springer, pp. 153-179, 2015.

[21] J. Kim, C. Lee, J. Sung, S. Hong, S. Lee, and J. Lim, "Seven new block cipher structures with provable security against differential cryptanalysis," IEICE transactions on fundamentals of electronics, Communications and computer sciences, vol. 91, no. 1, pp. 3047-3058, 2008.

[22] M. Matsui, "New block encryption algorithm MISTY," in International Workshop on Fast Software Encryption, Springer, pp. 54-68, 1997.

[23] S. Sun et al., "Towards finding the best characteristics of some bit-oriented block ciphers and automatic enumeration of (related-key) differential and linear characteristics with predefined properties," IACRCryptology ePrint Archive, vol. 747, p. 2014, 2014.

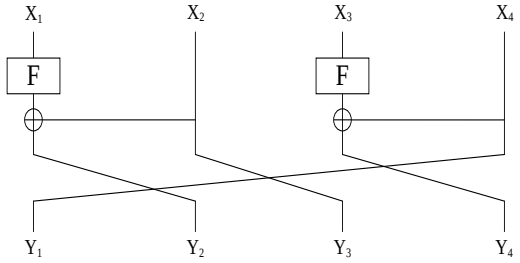
[24] S. Sun, L. Hu, P. Wang, K. Qiao, X. Ma, and L. Song, "Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES (L) and other bit-oriented block ciphers," in International Conference on the Theory and Application of Cryptology and Information Security, Springer, pp. 158-178, 2014.

[25] G. Optimization, "Gurobi Optimizer 5.0," Gurobi: http://www. gurobi. com, 2013.

[26] I. I. C. Optimizer, "urlhttp://www-01. ibm. com/software/integration/optimization/cplex-optimizer," ed: Last, 2010.

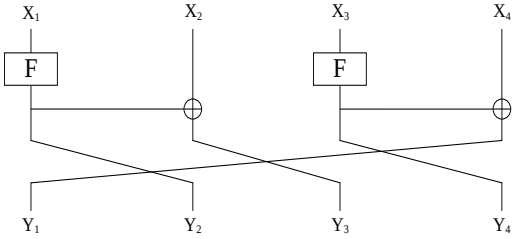
پیوست (الف) ساختارهای MISTY-FO-B و MISTY-FO-D

ساختار MISTY-FO-B مشابه ساختار MISTY-FO-A است. یک دور از این ساختار مطابق شکل (الف-۱) و محاسبات در آن مطابق نمادگذاری‌های بخش (۲-۲) می‌باشد.



شکل (الف -۱): یک دور از ساختار MISTY-FO-B

همچنین ساختار MISTY-FO-D مشابه ساختار MISTY-FO-C است. یک دور از این ساختار مطابق شکل (الف-۲) و محاسبات در آن مطابق نمادگذاری‌های بخش (۲-۳) می‌باشد.



شکل (الف -۲): یک دور از ساختار MISTY-FO-D

پیوست (ب) نتایج تحلیل ساختارهای MISTY-FO-B و MISTY-FO-D با استفاده از برنامه‌ریزی خطی عدد صحیح آمیخته

بعد از به‌دست آوردن مدل برنامه‌ریزی خطی عدد صحیح آمیخته برای تحلیل تفاضلی دورهای مختلف از ساختارهای MISTY-FO-B و MISTY-FO-D و حل تابع هدف آن‌ها با کمک نرم‌افزار CPLEX، پاسخ‌های تابع‌های هدف، به‌عنوان حداقل تعداد تابع‌های دور F فعال، مطابق جدول‌های (ب-۱) و (ب-۲) خلاصه می‌شوند.

جدول (ب-۱):حداقل تعداد تابع F فعال برای دورهای مختلف ساختار رمز قالبی MISTY-FO-B

تعداد دور	حداقل تعداد F فعال	تعداد دور	حداقل تعداد F فعال
۱	۰	۱۴	۱۳
۲	۱	۱۵	۱۴
۳	۲	۱۶	۱۵
۴	۳	۱۷	۱۶
۵	۴	۱۸	۱۸
۶	۶	۱۹	۱۸
۷	۶	۲۰	۱۹
۸	۷	۲۱	۲۰
۹	۸	۲۲	۲۱
۱۰	۹	۲۳	۲۲
۱۱	۱۰	۲۴	۲۴
۱۲	۱۲	۲۵	۲۴
۱۳	۱۲		

جدول (ب-۲): حداقل تعداد تابع F فعال برای دورهای مختلف ساختار رمز قالبی MISTY-FO-D

تعداد دور	حداقل تعداد F فعال	تعداد دور	حداقل تعداد F فعال
۱	۰	۱۴	۱۳
۲	۱	۱۵	۱۴
۳	۲	۱۶	۱۵
۴	۳	۱۷	۱۶
۵	۴	۱۸	۱۸
۶	۶	۱۹	۱۸
۷	۶	۲۰	۱۹
۸	۷	۲۱	۲۰
۹	۸	۲۲	۲۱
۱۰	۹	۲۳	۲۲
۱۱	۱۰	۲۴	۲۴
۱۲	۱۲	۲۵	۲۴
۱۳	۱۲		

با توجه به تشابه ساختارهای MISTY-FO-B و MISTY-FO-D، به ترتیب با ساختارهای MISTY-FO-A و MISTY-FO-C مقایسه نتایج تحلیل این ساختارها در این مقاله با [۲۱] مشابه مقایسه‌ای است که در بخش (۴-۲) انجام گرفت.

Journal of Electronical & Cyber Defence
Vol. 8, No. 4, 2021, Serial No. 32

Upper Bounds for the Probability of Differential Characteristics of Five Block Cipher Constructions Functions

J. Alizadeh*, Gh. Jamshidian, A. Gaeini, A. Mirghadri

*Imam Hossein Comprehensive University

(Received: 15/01/2020, Accepted: 05/08/2020)

ABSTRACT

Block ciphers have the main role in the communication and information security and also electronic and cyber defense. A secure block cipher must be resistant against the known attacks, such as the differential cryptanalysis. Kim et al. presented seven block cipher constructions with provable security against differential cryptanalysis in 2008, which can be used to design the block ciphers. In this paper, for five of the seven mentioned block cipher constructions, the upper bounds on the probability of differential characteristics have been presented. This has been done using an automated differential cryptanalysis approach based on linear programming. This approach formally introduced by Mouha et al. in 2011, was used for the analysis of several block ciphers. Using the Mouha et al.'s approach, it is shown that the five-round differential characteristics of the constructions have the upper bound P^4 which are approvable in comparison with the upper bounds of the differentials obtained by Kim et al. where p is the differential probability of the round function used in the constructions.

Keywords: Block Cipher, Differential Characteristic, Differential, Security Bound, Mixed Integer Linear Programming

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