محاسبه‌ی امنیت اثبات‌پذیر ساختارهای فیستلی در برابر تحلیل‌های خطی و تفاضلی

امید پاکدل آذر [*1]،

۱- گروه مهندسی برق گرایش مخابرات، دانشکده برق و کامپیوتر، دانشگاه آزاد اسلامی، واحد علوم تحقیقات، تهران، ایران.

[1]omidpakdelazar@srbiau.ac.ir

چکیده

رمزنگاری اطلاعات یکی از مهم‌ترین بخش‌های تمامی سیستم‌های دفاعی است و ضعیف بودن الگوریتم‌های به کار رفته ممکن است صدمات جبران‌ناپذیری در پی داشته باشد. با توجه به حساسیت بالای حفظ امنیت داده‌ها، ضروری است که برای اطمینان از عملکرد صحیح بلوک رمزنگاری از الگوریتم‌های بومی استفاده شود. همچنین به منظور افزایش ضریب امنیت می‌بایست به طور مداوم، الگوریتم‌های جدید طراحی و جایگزین طرح‌های قبلی شوند. لازمه‌ی امنیت یک طرح، ارزیابی مقاومت آن در برابر تمامی حملات موجود است. برای تضمین امنیت رمزهای بلوکی در برابر تحلیل‌های موجود، روش‌های اثبات امنیت در مقابل آن‌ها نیز گسترش یافته‌اند. یکی از مهم‌ترین حملات موجود، حملات خطی و تفاضلی هستند و هر طراح، در قدم اول، می‌بایست امنیت طرح خود را در برابر این حملات ارزیابی کند. تلاش‌های زیادی به‌منظور ارائه‌ی روشی جامع برای محاسبه‌ی امنیت اثبات‌پذیر رمزهای بلوکی انجام شده است؛ اما هنوز یک راهکار سیستماتیک، با قابلیت پیاده‌سازی نرم‌افزاری، که بتواند در زمان معقول، نتیجه‌ی مناسبی داشته باشد، ارائه نشده است. برخی از راهکارهای موجود، پیچیدگی محاسباتی بسیار بالایی دارند و تنها برای برخی الگوریتم‌های خاص، قابل استفاده هستند. هم‌اکنون، امنیت یک الگوریتم رمزنگاری، با محاسبه‌ی دستی، صرف زمان بسیار زیاد و دقت پایین انجام می‌شود. ضمن اینکه روش‌های مورد استفاده، فقط در الگوریتم‌های کوچک قابل استفاده هستند. در این مقاله، ابتدا روشی جامع برای محاسبه‌ی امنیت اثبات‌پذیر یک الگوریتم فیستلی در برابر تحلیل‌های خطی و تفاضلی، با امکان پیاده‌سازی عملی و پیچیدگی محاسباتی پایین ارائه می‌کنیم. در مرحله‌ی بعد، نرم‌افزاری تهیه می‌شود که با دریافت پارامترهای رمز فیستلی، میزان امنیت و یا تعداد دورهای لازم برای تامین امنیت را مشخص می‌کند. روش پیشنهادی می‌بایست بر ساختارهایی با تعداد پورت‌های ورودی بالا و شافل‌های نامنظم نیز قابل اعمال باشد و به‌علاوه، نتیجه را در زمان مناسبی نمایش دهد.

کلمات کلیدی: رمز های فیستلی، حملات خطی و تفاضل، رمزهای بلوکی، امنیت اثبات پذیر.

۱. مقدمه

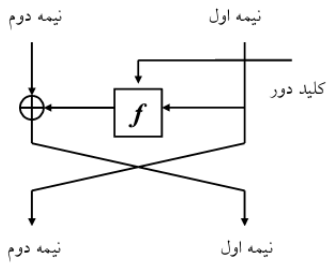
[*] **Corresponding author:** توضیحات مربوط به نویسنده اوّل
Email:

یک الگوریتم رمزنگاری متن مشخصی را، با استفاده از یک پارامتر محرمانه به نام کلید، به متن دیگری تبدیل می‌کند، به‌طوری که دست‌یابی به متن اول با داشتن متن دوم و بدون داشتن کلید از نظر محاسباتی غیر ممکن باشد. متن اول و دوم را به ترتیب متن اصلی و رمز شده می‌نامند و با نمادهای P و C نمایش می‌دهند.

بر حسب اینکه کلید رمزنگاری و رمزگشایی یکسان یا متفاوت باشند، سیستم‌های رمزنگاری به دو دسته‌ی متفارن و نامتقارن تقسیم می‌شوند. در رمز متقارن، کلید رمزنگاری و رمزگشایی یکسان است و یا رابطه ساده‌ای با هم دارند. سیستم‌های رمز متقارن خود به دو دسته‌ی بلوکی و رمزهای جریانی تقسیم می‌شوند. در رمز بلوکی یک طول معین (یک بلوک) را از داده‌ها جدا می‌کنیم و توابعی وابسته به کلید را به گونه‌ای روی آن اعمال می‌کنیم که متن رمز شده تا حد ممکن حامل هیچ اطلاعاتی از متن اصلی و یا کلید نباشد. اما در رمز جریانی، با استفاده از کلید، دنباله‌ای شبه تصادفی و غیرقابل پیش‌بینی از بیت‌ها می‌سازیم و سپس متن ورودی را با این دنباله جمع باینری می کنیم.

در مواردی که خطای انتقال داده‌ها بالاست، رمزهای جریانی به دلیل عدم پخش خطا برتری دارند. همچنین مواردی که می‌بایست در یک زمان تنها یک سمبل پردازش شود (مثلاً به دلیل محدودیت حافظه) از این رمزها استفاده می‌شود. گسترش روش‌های اصولی برای طراحی و تحلیل رمزهای بلوکی، موجب شده است این رمزها قاعده‌مندتر از رمزهای جریانی باشند. در این بخش به‌طور اجمالی، روش‌های طراحی و تحلیل رمزهای بلوکی را معرفی می‌کنیم.

ساختار فیستلی اولین بار هنگام طراحی الگوریتم رمز Lucifer در شرکت IBM استفاده شد. پس از آن، این ساختار بهبود یافت و با تغییراتی که مؤسسه‌ی امنیت ملی آمریکا (NSA) در آن ایجاد کرد تحت عنوان اولین استاندارد رمزنگاری داده DES معرفی شد. ساختارهای فیستلی روند رمزنگاری و رمزگشایی مشابهی دارند. می‌توان با استفاده از یک ماژول رمزنگاری، فقط با معکوس کردن ترتیب کلیدها، هر دو عمل رمزنگاری و رمزگشایی را انجام داد که از نظر هزینه‌ی پیاده‌سازی بسیار مقرون به صرفه است. در این ساختارها، عموماً نیمی از متن اصلی توسط تابعی مشخص با زیرکلید ترکیب و با نیمه‌ی دیگر جمع باینری می‌شود تا نیمه‌ی اول دور بعد را بسازد. نیمه‌ی دوم دور بعد نیز با نیمه‌ی اول یکسان است. شکل1 یک دور از یک ساختار فیستلی را نشان می‌دهد.

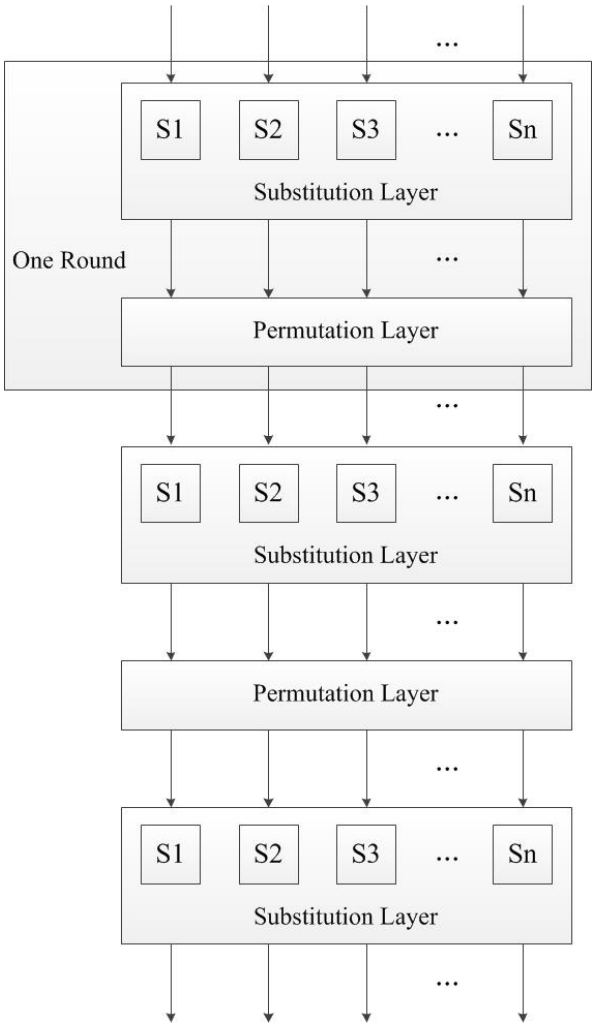


شکل1 – یک دور از ساختار فیستلی معمولی

Plaintext
Ciphertext
Symmetric
Asymmetric
Block Cipher
Stream Cipher
Feistel Structure
National Security Agency
Data Encryption Standard

با گذشت بیش از ۱۰ سال از ارائه‌ی استاندارد رمزنگاری پیشرفته (AES)*، ساختارهای فیستلی دوباره مورد توجه طراحان رمزهای بلوکی قرار گرفته‌اند. از مزایای این ساختارها می‌توان به انعطاف پذیری بیشتر، سرعت بالا و حجم کم‌تر اشاره کرد.

در ساختار شبکه‌ی جانشینی-جایگشتی (SPN)† عمل رمزنگاری با تکرار تبدیل‌های جانشینی و جایگشتی و ترکیب با کلید انجام می‌شود. ویژگی بارز ساختار جانشینی-جایگشتی سادگی ظاهری آن است. در این مورد، بر خلاف ساختار فیستلی، نمی‌توان از ماژول یکسان برای رمزنگاری و رمزگشایی استفاده کرد و برای رمزگشایی، معکوس تبدیل‌های رمزنگاری به کار می‌رود. شکل2 ساختار یک شبکه‌ی جانشینی-جایگشتی سه‌دوری را نشان می‌دهد.



شکل2 – ساختار یک شبکه‌ی جانشینی-جایگشتی سه دوری

دو جزء بنیادی رمزهای بلوکی، لایه‌های خطی و غیرخطی هستند. در ادامه این لایه‌ها را به طور خلاصه معرفی می‌کنیم. وظیفه‌ی لایه‌ی خطی پخش ویژگی‌های غیرخطی در طول بلوک رمزنگاری است. به همین دلیل، به آن لایه‌ی پخش‌ هم

* Advanced Encryption Standard
† Substitution Permutation Network
‡ Diffusion Layer

می‌گویند. غالباً برای سنجش توان یک لایه‌ی خطی از پارامتری به نام عدد انشعاب* استفاده می‌شود. در طراحی لایه‌ی خطی، عدد انشعاب بیشتر و پیچیدگی پیاده‌سازی کمتر مورد نظر است.

یکی از راه‌های متداول برای طراحی لایه‌ی غیر خطی، استفاده از نگاشتی یک به یک به نام SBox† است. معیارهای مختلفی برای ارزیابی SBox وجود دارد. هر یک از این معیارها، امنیت رمز بلوکی را در برابر دسته‌ای از حملات تأمین می‌کند.

۲. مروری بر روش‌های تحلیل رمزهای بلوکی

یک تحلیل‌گر تلاش می‌کند اطلاعاتی از متون رمز شده استخراج کند. تلاش‌های موفق در تحلیل رمز حمله نامیده می‌شوند. برای ارزیابی یک رمز بلوکی، امنیت آن را در برابر حملات موجود آزمایش می کنیم. اصل کرشف‡ مبنای طراحی و تحلیل الگوریتم‌های رمزنگاری است. این اصل می‌گوید امنیت یک ساختار رمز کننده تنها با مخفی ماندن کلید رمزنگاری تأمین نمی‌شود و نه با مخفی ماندن الگوریتم. خروجی هر رمزکننده می‌بایست مشخصه‌های آماری مشابه یک دنباله‌ی تصادفی را داشته باشد. برای برآورد میزان تصادفی بودن یک رمزکننده آزمون‌های آماری زیادی معرفی شده است. اما بررسی امنیت یک رمزکننده در برابر حملات موجود، به سادگی انجام آزمون‌های آماری نیست. هر حمله به جنبه خاصی از یک الگوریتم توجه می‌کند و در اغلب موارد، یک روش سیستماتیک برای اعمال حملات موجود نیست؛ به علاوه، هر ساختار جدید، منشاء ایده‌هایی برای حمله‌های جدید هستند.

هدف تحلیل‌گر یافتن هر گونه اطلاعاتی مربوط به سیستم رمزنگاری است؛ مثلاً یافتن متن آشکار مربوط به یک متن رمز شده و حتی یافتن کل کلید. حمله‌ای موفق است که بتواند اطلاعات مورد نظر (کلید) را، سریع‌تر از جستجوی جامع، استخراج کند؛ در این صورت، الگوریتم رمز به طور کامل شکسته شده است. همچنین یک الگوریتم به طور جزیی شکسته شده است، اگر بتوان قسمتی از متن آشکار را از روی متن رمز شده تشخیص داد. طبق برخی تعاریف، یک الگوریتم رمزنگاری شکسته می‌شود، هرگاه بتوان تنها یک بیت کلید را با احتمال بیش از 0.5 حدس زد. در ادامه حملات مهم وارد بر رمزهای بلوکی را معرفی می‌کنیم.

حمله جستجوی کامل§ ساده‌ترین و ابتدایی‌ترین روش حمله بر رمزهای بلوکی است. این حمله از نوع متن اصلی معلوم است و در آن تحلیل‌گر تمامی کلیدهای ممکن را آزمایش می‌کند. با افزایش سرعت و امکان موازی‌سازی تعداد بسیار زیادی از پردازنده‌های دیجیتال، قدرت حمله‌ی جستجوی فضای کامل کلید روز به روز افزایش می‌یابد. در حال حاضر، طول کلید مورد قبول برای رمزهای بلوکی برابر ۱۲۸ بیت است. پیچیدگی زمانی حمله‌ی جستجوی کامل فضای کلید از مرتبه‌ی $O(2^n)$ است که n تعداد بیت‌های کلید است. همچنین پیچیدگی مورد انتظار این حمله برابر پیچیدگی بدترین حالت آن است، بنابراین اگر پیچیدگی یک حمله نیمی از جستجوی کامل فضای کلید باشد، مزیتی نسبت به این حمله ندارد.

حمله‌ی تفاضلی یکی از معمول‌ترین حملات وارد بر رمزهای بلوکی است و هر طراح می‌بایست در قدم اول، مقاومت الگوریتم خود را در برابر این حمله بسنجد. این حمله، از نوع متن اصلی منتخب است و ایده‌ی اصلی آن، استفاده از تفاضل بین متون پیام، مستقل از بیت‌های کلید است.

---

* Branch Number
† Substitution Box
‡ Kerckhoffs's Maxim
§ Brute Force

فرض کنید که P متن آشکار و C متن رمزشده‌ی متناظر آن با استفاده از کلید باشد، به‌طوری‌که $C = E_K(P)$. اگر P' یک متن آشکار دیگر و C' متن رمز شده‌ی متناظر، با همان کلید باشد داریم $C' = E_K(P')$. تفاضل متون آشکار را به صورت $P^* = P \oplus P'$ تعریف می‌کنیم. به طور مشابه، تفاضل متون مرز شده نیز به صورت $C^* = C \oplus C'$ تعریف می‌شود. عملگر تفاضل برای متون میانی نیز به همین ترتیب بیان می‌شود.

در این حمله، به‌جای بررسی روند رمزنگاری یک متن آشکار، مسیر تفاضل‌ها را دنبال می‌کنیم. مزیت این روش این است که برای تمامی متون آشکار، میانی و رمز شده، تفاضل تمامی کلیدها برابر صفر است؛ فرض کنید که متن X در یکی از دورهای میانی با کلید K ترکیب می‌شود و متن Y را نتیجه می‌دهد. یعنی: $Y = X \oplus K$. از طرف دیگر برای متن X^* نیز داریم: $Y' = X' \oplus K$ و تفاضل خروجی با رابطه (۱) به دست می‌آید.

$$Y^* = Y' \oplus Y = (X \oplus K) \oplus (X' \oplus K) = X \oplus X' = X^* \quad (۱)$$

بنابراین جمع با کلید تفاضل را تغییر نمی‌دهد.

عملیات خطی تاثیری روی تفاضل‌ها ندارد و جایگشت‌ها نیز یک تفاضل را به تفاضل مشخص دیگری تبدیل می‌کنند. تنها توابع غیرخطی، مانند SBoxها، هستند که در آن‌ها تفاضل‌های ورودی و خروجی رابطه‌ی پیچیده‌ای با یکدیگر دارند. در این توابع، از آن‌جایی که توزیع مقادیر تفاضل خروجی، به ازای یک تفاضل ورودی، یکنواخت نیست، می‌توان با یافتن جفت تفاضل‌های ورودی و خروجی، با احتمال انتقال بالا، و در کنار هم قرار دادن آن‌ها در چند دور، یک مسیر تفاضلی با احتمال مناسب از ورودی به خروجی الگوریتم پیدا کرد. یک مسیر تفاضلی را مشخه‌ی تفاضلی می‌نامند. احتمال یک مشخصه‌ی تفاضلی از وردی به خروجی یک الگوریتم، با فرض استقلال زیرکلیدها، برابر حاصل ضرب احتمالات مشخصه‌های هر دور است. بنابراین با افزایش تعداد دورها، احتمال برقراری یک مشخصه کاهش می‌یابد. حمله‌ی تفاضلی منشاء بسیاری از حملات وارد شده به مرزهای بلوکی است. در ادامه برخی از آن‌ها را شرح می‌دهیم.

ساختارهای کلمه‌گرا [*]، به دلیل امکان پیاده‌سازی سریع‌تر، مورد علاقه‌ی طراحان هستند. مفهوم تفاضل‌های بریده‌شده به یکی از مؤثرترین ابزارهای تحلیل رمزهای بلوکی کلمه‌گرا تبدیل شده است. تفاضل‌های برده‌شده تعمیمی از مفهوم تفاضل‌ها هستند. ایده اصلی این است که تنها تفاضل بخشی از بیت‌ها را در نظر بگیریم یا اینکه برای مجموعه‌ای بیت‌ها یک تفاضل قائل شویم.

در حملات تفاضلی از مرتبه بالاتر، به جای استفاده از تفاضل مربته‌ی اول برای تقریب توابع غیرخطی، از تفاضل‌های مرتبه‌ی بالاتر استفاده می‌شود. این تفاضل‌ها به[‡] صورت مشتقات از مرتبه‌ی دوم و بالاترند. همان‌طور که تفاضل مرتبه‌ی اول به دو متن آشکار منتخب نیاز دارد، یک تفاضل مربته‌ی s-ام با 2^s متن آشکار منتخب تولید می‌شود.

حمله‌ی بومرنگ تعمیمی از حمله‌ی تفاضلی است[§] و در رمزهایی که برای کل الگوریتم مشخصه‌ی تفاضلی با احتمال مناسب وجود ندارد، اما با دو نیم کردن الگوریتم، برای هر نیمه‌ی آن مشخصه‌ی مناسبی می‌توان یافت، حمله‌ی بومرنگ قابل اعمال است. در حالت کلی، به جای دو نیم کردن، می‌توان الگوریتم را به دو بخش که لزوماً برابر نیستند، تقسیم کرد. حمله‌ی تفاضلی به دنبال یافتن مسیرهای تفاضلی با احتمال وقوع بالا است. در حمله‌ی تفاضل ناممکن [*]، دقیقاً بر خلاف حمله‌ی تفاضلی معمولی، به دنبال رویدادی با احتمال صفر هستیم، یعنی رویدادی که قطعاً نمی‌تواند در الگوریتم اتفاق بیافتد.

حمله‌ی خطی روشی قدرتمند برای رمزشکنی[†] است که پس از حمله‌ی تفاضلی ابداع شد. این حمله، غیر از حمله‌ی بدیهی جستجوی کامل فضای کلید، تنها حمله‌ای است که به طور عملی روی DES اجرا شده است. این حمله که از نوع

---

[*] Word-Oriented
[†] Truncated Differential
[‡] Higher-Order Differentials
[§] Boomerang Attack
[*] Impossible Differential Attack [*]
[†] Linear Attack [†]

حمله به وسیله متن اصلی معلوم است، به دنبال تقریب‌های خطی‌ای است که درصد جفت‌های متون معلوم و رمزشده‌ای که در آن صدق می‌کند برابر 0.5 نباشد. سپس تقریبی را انتخاب می‌کند که از میان متونی که در اختیار است، احتمال درستی بیشتری داشته باشد. میزان موفقیت تحلیل خطی برای یک الگوریتم به بیشترین احتمال تقریب خطی برای لایه‌ی غیرخطی الگوریتم (SBox) بستگی دارد. تحلیل خطی به صورت زیر فرمول‌بندی می‌شود:

$$\left(\bigoplus_{i\in\{1,\dots,a\}} P^{(i)}\right)\oplus\left(\bigoplus_{j\in\{1,\dots,b\}} C^{(j)}\right)=\left(\bigoplus_{k\in\{1,\dots,c\}} K^{(k)}\right) \qquad (۲)$$

که P نشان دهنده‌ی متن آشکار، C متن رمز شده و K کلید است. عملگر $\oplus$ بیانگر XOR و i,j,k اعداد طبیعی و ثابت هستند.

میزان موفقیت این معادله به اختلاف احتمال درستی آن با 0.5 بستگی دارد. نشان داده می‌شود که اگر انحراف احتمال رابطه‌ی تقریب زننده‌ی کل رمز برابر ϵ باشد، پیچیدگی داده‌ی یک حمله‌ی خطی موفق از مرتبه‌ی $O\left(\frac{1}{\epsilon^2}\right)$ جفت متن اصلی-رمزشده‌ی معلوم است.

حمله تفاضلی-خطی* حمله‌ای با متن اصلی منتخب است. این حمله، در واقع، حمله‌ی خطی به تفاضل‌هاست؛ یعنی بایستی یک رابطه‌ی خطی میان بیت‌های تفاضل گرفته شده پیدا نمود. وجود حمله‌های ترکیبی نشان می‌دهد که علاوه بر تامین امنیت کلی یک الگوریتم، می‌بایست هر تعداد دور از الگوریتم نیز امنیت قابل قبولی داشته باشد. در حمله کلید مرتبط† ، تحلیل رفتار الگوریتم رمز تحت چندین کلید مجهول، که رابطه‌ی ریاضی مشخص بین آن‌ها وجود دارد انجام می‌شود.

حمله‌ی انتگرالی‡ ، که با نام‌های حمله‌ی مربعی§ و حمله‌ی اشباعی* نیز شناخته می‌شود، را می‌توان دوگان حمله‌ی تفاضلی در نظر گرفت. در حمله‌ی انتگرالی نحوه‌ی پخش حاصل جمع تعداد زیادی از ورودی‌ها بررسی می‌کنیم. مشابه حمله‌ی تفاضلی، حمله‌ی انتگرالی را نیز می‌توان به صورت مرتبه‌ی بالاتر† اعمال کرد؛ به این معنی که به‌جای یک پورت، دو یا چندین پورت فعال را به عنوان ورودی در نظر بگیریم.

حمله‌ی درون‌یابی‡ سعی می‌کند به کمک متون آشکار و متون رمزشده‌ی متناظر، یک رابطه‌ی چندجمله‌ای میان آنها و کلید مورد استفاده بیابد و به این وسیله تقریبی از رمز بلوکی به دست آورد. حمله‌ی درون‌یابی در واقع تعمیمی از حمله‌ی تفاضلی مرتبه‌ی بالاتر است؛ در این حالت، مرتبه‌ی تفاضل را آن‌قدر بالا در نظر می‌گیریم که با احتمال ۱ در رمز مربوطه صدق کند.

یکی از ایده‌های جدید تحلیل رمز، توصیف رمز به کمک مجموعه‌ای از معادلات جبری است. اگر بتوان این سیستم معادلات را سریع‌تر از جستجوی کامل فضای کلید حل کرد، رمز شکسته شده است. حمله‌هایی وجود دارند که تنها به دسته‌ای از رمزهای بلوکی قابل اعمال هستند و یا امکانات بیشتری را برای تحلیل‌گر فرض می‌کنند. این حملات اهمیت کمتری دارند، اما مهم است که طراح از آنها مطلع باشد و امنیت طرح خود را در برابر آنها تضمین کند. حمله با استفاده از کلید ضعیف، حمله‌ی کلید همبسته و حمله کانال جانبی§ مثال‌هایی از این نوع حملات هستند.

در این قسمت مباحث کلی رمزهای بلوکی، شامل انواع ساختارها، اجزای مهم و حملات مهم وارد بر آنها معرفی شدند. پس از طراحی یک رمز بلوکی، نخستین مرحله ارزیابی آن توسط آزمون‌های آماری است. اگر رمز کننده در این مرحله موفق

---

* Differential-Linear Attack
† Related Key Attack
‡ Integral Attack
§ Square Attack
* Saturation Attack
† Higher Order Integral Attack
‡ Interpolation Attack
§ Side-Channel Attack

بود، می‌توان تحلیل‌های رمزشکنی را روی آن اعمال کرد. بررسی روش‌های گوناگون رمزشکنی نشان می‌دهد که چگونه کوچکترین خطایی در طراحی منجر به شکست رمز می‌شود.

۳. امنیت اثبات‌پذیر رمزهای فیستلی در برابر حملات خطی و تفاضلی

از مهمترین حملات روی رمزهای بلوکی، تحلیل‌های خطی و تفاضلی است که با یافتن مشخصه‌ای با احتمال بالا انجام می‌شود. در حین طراحی الگوریتم‌های بلوکی، ملاحظاتی صورت می‌گیرد تا بتوان امنیت طرح را در برابر تحلیل‌های موجود تضمین کرد. اگر طراح بتواند برای تعداد دور خاص، یک باند بالایی از احتمال خطی یا تفاضلی را اثبات کند، اصطلاحاً به صورت اثبات‌پذیر توانسته است حدود امنیت سیستم خود را محاسبه کند.

یکی از چالش‌های طراحان رمزهای بلوکی، محاسبه‌ی امنیت اثبات‌پذیر برای طرح پیشنهادی است. فرآیند اثبات امنیت، غالباً بسیار تخصصی و زمان‌بر تلقی می‌شود. در این بخش، مثال‌هایی از ساختارهای فیستلی ارائه می‌کنیم و گزاره‌هایی برای کران بالای احتمال تفاضلی چند دور از آنها بیان می‌کنیم. تمامی گزاره‌ها برای معادل احتمال خطی آنها نیز برقرار هستند.

هدف کلی حملات تفاضلی [1] [۲] و خطی [۳][۴] یافتن کلید دور اول و یا آخر با استفاده از یک مشخصه با احتمال زیاد و با پیچیدگی کمتر از جستجوی جامع است. اما کوچک بودن بیشترین احتمال مشخصه، امنیت رمز بلوکی را در برابر این حملات تضمین نمی‌کند. برای اینکه نشان دهیم یک رمز بلوکی در برابر حملات خطی و تفاضلی امن است باید ثابت کنیم بیشترین احتمال خطی و تفاضلی از یک مقدار به اندازه‌ی کافی کوچک تجاوز نمی‌کند. در مقالات متعددی اشاره شده است که اثبات احتمال خطی مشابه تفاضلی است [۵]–[۸]. بنابراین در این مقاله، محاسبات را برای احتمال تفاضلی انجام می‌دهیم.

در سال ۱۹۹۲، برای نخستین بار مفهوم امنیت اثبات‌پذیر در برابر حمله‌ی تفاضلی معرفی شد و امنیت یک ساختار فیستلی اثبات گردید [۸]. در [۹] اثبات شده است که اگر یک شبکه فیستلی تعمیم‌یافته (GFN)، در هر دور، n تابع F* یک به یک داشته باشد، آنگاه احتمال متوسط هر تفاضل، در حداقل $3n$ دور، کمتر و یا مساوی p است که p بیشترین احتمال تفاضلی متوسط می‌باشد. در [۶]، رمز بلوکی MISTY با امنیت اثبات‌پذیر در برابر حملات خطی و تفاضلی ارائه شد. همچنین در [۱۰], [۱۱] امنیت اثبات‌پذیر ساختارهای شبه-Skipjack و SPN محاسبه شده است. در ادامه مفاهیم اولیه برای محاسبه‌ی امنیت اثبات‌پذیر ساختارهای فیستلی را بیان می‌کنیم.

یک رمز فیستلی n بیتی را به صورت زیر در نظر می‌گیریم:

$$F_k: GF(2^n) \to GF(2^n) \qquad (۳)$$

که k کلید دور است. همچنین فرض می‌کنیم کلید دور به طور تصادفی و مستقل تولید شده است. برای سادگی، F_k را با F نمایش می دهیم. برای هر $\Delta x, \Delta y \in \boldsymbol{GF}$، احتمال تفاضلی تابع دور F به صورت زیر محاسبه می‌شود [۶]:

$$DP^F(\Delta x \to \Delta y) = \frac{\#\{x \in \boldsymbol{GF}(2^n) | F(x) \oplus F(x \oplus \Delta x) = \Delta y\}}{2^n} \qquad (۴)$$

برای هر $\Gamma x, \Gamma y \in \boldsymbol{GF}$، احتمال خطی تابع دور F به صورت زیر محاسبه می‌شود [۶]:

$$LP^F(\Gamma y \to \Gamma x) = \left(\frac{\#\{x \in \boldsymbol{GF}(2^n) | \Gamma x.x = \Gamma y.F(x)\}}{2^{n-1}} - 1\right)^2 \qquad (۵)$$

که « . » بیانگر ضرب داخلی a و b است.

* Generalized Feistel

باید توجه داشت که $DP^F(\Delta x \to \Delta y)$ و $LP^F(\Gamma y \to \Gamma x)$ متوسط احتمالات روی تمام کلیدها هستند. تعریف زیر برای ارزیابی میزان مقاومت در برابر حملات خطی و تفاضلی استفاده می‌شود. بیشینه‌ی احتمالات خطی و تفاضلی تابع F مطابق زیر تعریف می‌شود:

$$DP^F_{\max} = \max_{\Delta x \neq 0, \Delta y} DP^F(\Delta x \to \Delta y) = p \quad (۶)$$

$$LP^F_{\max} = \max_{\Gamma x, \Gamma y \neq 0} LP^F(\Gamma y \to \Gamma x) = q \quad (۷)$$

برای هر تابع F، داریم (قضیه ۱ [۶]):

$$\sum_{\Gamma x} LP^F(\Gamma y \to \Gamma x) = 1 \text{ و } \sum_{\Delta y} DP^F(\Delta x \to \Delta y) = 1 \quad (۸)$$

برای هر تابع یک به یک F، داریم:

$$\sum_{\Gamma y} LP^F(\Gamma y \to \Gamma x) = 1 \text{ و } \sum_{\Delta x} DP^F(\Delta x \to \Delta y) = 1 \quad (۹)$$

به راحتی می‌توان نشان داده که $DP^F(0 \to 0)$ و $DP^F(\Delta x \to \Delta y)$. با استفاده از قضیه‌ی زیر می‌توان احتمالات خطی و تفاضلی را برای دو دور متوالی محاسبه کرد.

با استفاده از قضیه‌ی زیر می‌توان احتمالات خطی و تفاضلی را برای دو دور متوالی محاسبه کرد [۶]:

برای هر $\Delta x, \Delta y, \Gamma x, \Gamma y \in \boldsymbol{GF}$ داریم:

$$DP^{F_1,F_2}(\Delta x \to \Delta y) = \sum_{\Delta y} DP^{F_1}(\Delta x \to \Delta y).\, DP^{F_2}(\Delta y \to \Delta z) \quad (۱۰)$$

$$LP^{F_1,F_2}(\Gamma z \to \Gamma x) = \sum_{\Gamma y} LP^{F_1}(\Gamma z \to \Gamma y).\, LP^{F_2}(\Gamma y \to \Gamma x) \quad (۱۱)$$

در اکثر ساختارهای فیستلی، امنیت برای تعداد دوری اثبات می‌شود که الگوریتم در آن دو به تمامیت* می‌رسد. بنابراین بحثی در مورد تمامیت ساختارهای فیستلی تعمیم‌یافته ارائه می‌کنیم.

تمامیت یکی از ویژگی‌های اساسی یک رمزکننده است و به معنی وابسته بودن همه‌ی بیت‌های خروجی به همه‌ی بیت‌های ورودی است. در رمزکننده‌های فیستلی مقیاس‌پذیر تعمیم‌یافته، بیش از ۲ زیربلوک در هر دور وجود دارد. با افزایش تعداد زیربلوک‌ها، حالات متفاوتی برای ساختار پیش می‌آید که در شکل3 مشخص شده‌اند [۶].

در جدول ۱ می‌بینیم که فیستل نوع دوم و سوم در تعداد دور یکسانی به تمامیت می‌رسند؛ اما با توجه به تعداد کمتر توابع به کار رفته در نوع دوم، طرح‌های بیشتری مبتنی بر آن موجود است. در این جدول، N تعداد زیربلوک‌هاست که برای نوع دوم همیشه زوج است.

جدول ۱ - تعداد دورهای لازم برای تمامیت ساختارهای تعمیم‌یافته

تعداد توابع $\boldsymbol{F}$ به‌کار رفته	حداقل دور لازم برای تمامیت	نوع ساختار تعمیم‌یافته
$2N-1$	$2N-1$	نوع اول تعمیم‌یافته
$\frac{N(N-1)}{2}$	$N+1$	نوع دوم تعمیم‌یافته
$N(N-1)$	$N+1$	نوع سوم تعمیم‌یافته

۱-۳- امنیت اثبات‌پذیر برای ساختارهای فیستلی تعمیم‌یافته‌ی نوع دوم

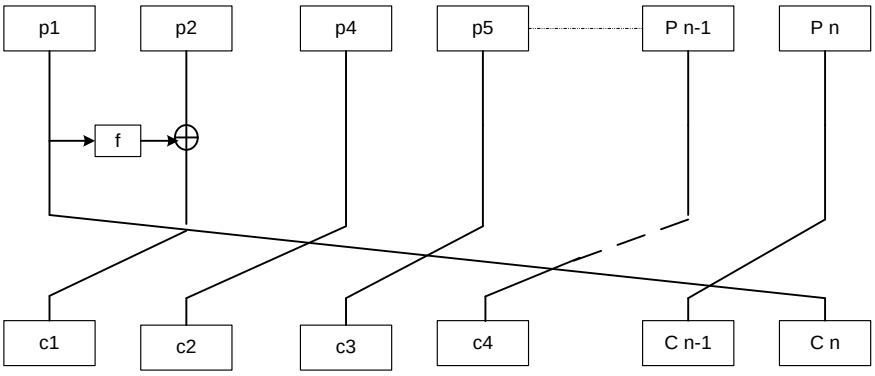
* Completeness

در صورتی که الگوریتم فیستلی تعمیم‌یافته‌ی نوع دوم دارای ۴ زیربلوک باشد، طبق جدول ۱ در ۵ دور به تمامیت می‌رسد. در [۱۲] برای ۵ دور از این ساختار امنیت اثبات‌پذیر ارائه شده است. یک دور از ساختار فیستلی تعمیم‌یافته‌ی نوع دوم، به صورت زیر تعریف می‌شود:

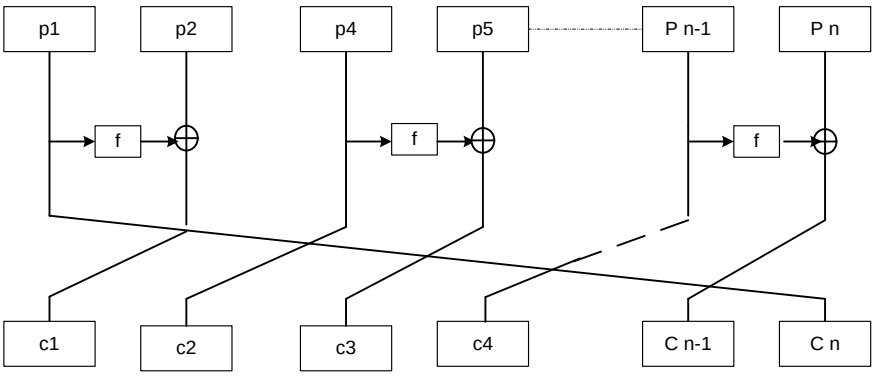
$$Y_1 = F(X_3) \oplus X_4, Y_2 = X_1, Y_3 = F(X_1) \oplus X_2, Y_4 = X_3 \quad (۱۲)$$

که X_1, X_2, X_3 و Y_1, Y_2, Y_3 به ترتیب ورودی و خروجی هر دور هستند. شکل4 پنج دور تفاضلی از این ساختار را نشان می‌دهد. احتمال تفاضل ۵ دور، $DP(\alpha \to \beta)$، با رابطه‌ی زیر محاسبه می‌شود:

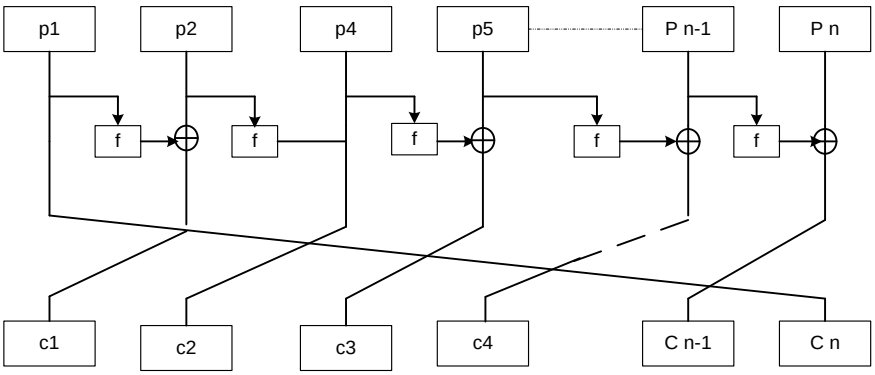
$$DP(\alpha \to \beta) = \sum_{\delta_i, 1 \le i \le 6} DP(\alpha_1 \to \delta).DP(\alpha_3 \to \delta_2).DP(\alpha_4 \oplus \delta_2 \to \delta_3).DP(\alpha_2 \oplus \delta_1 \to \delta_4).DP(\alpha_3 \oplus \delta_4 \to \delta_5).DP(\alpha_1 \oplus \delta_3 \to \delta_6).DP(\alpha_2 \oplus \delta_1 \oplus \delta_6 \to \alpha_3 \oplus \beta_3 \oplus \delta_4).DP(\alpha_4 \oplus \delta_2 \oplus \delta_5 \to \alpha_1 \oplus \beta_1 \oplus \delta_3).DP(\beta_1 \to \alpha_2 \oplus \beta_2 \oplus \delta_1 \oplus \delta_6).DP(\beta_3 \to \alpha_4 \oplus \beta_4 \oplus \delta_2 \oplus \delta_5) \quad (۱۳)$$



الف– ساختار فیستلی تعمیم یافته ی نوع اول



ب– ساختار فیستلی تعمیم یافته ی نوع دوم



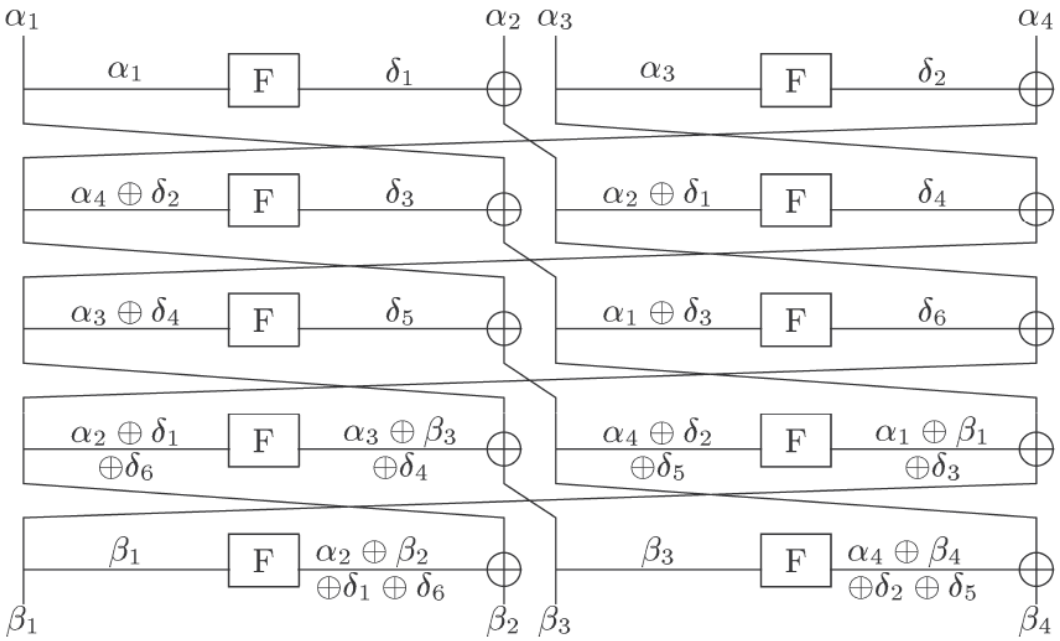
ج– ساختار فیستلی تعمیم یافته ی نوع سوم

شکل3 – ساختارهای فیستلی تعمیم‌یافته

می‌دانیم اگر تابع F یک به یک و غیر صفر باشد، داریم:

$$\sum_{\delta_1,\delta_2} DP(\alpha \oplus \delta_1 \to \delta_2).DP(\beta \to \delta_2) = \sum_{\delta_2} DP(\beta \to \delta_2).(\sum_{\delta_1} \alpha \oplus \delta_1 \to \delta_2) = \sum_{\delta_2} DP(\beta \to \delta_2) = 1 \quad (۱۴)$$

فرض کنید $\alpha = \alpha_1, \alpha_2, \alpha_3$ تفاضل ورودی و $\beta = \beta_1, \beta_2, \beta_3$، تفاضل خروجی پس از ۵ دور باشد. با شرط یک به یک بودن تابع F، تنها حالات α و β را در نظر می‌گیریم. روشن است که حالات $\alpha_1 = 0, \alpha_2 = 0, \alpha_3 = 0, \alpha_4 \neq 0$ و



شکل 4 – نمادگذاری ۵ دور برای ساختار فیستلی تعمیم‌یافته نوع دوم

$\alpha_1 = 0, \alpha_2 \neq 0, \alpha_3 = 0, \alpha_4 = 0$ یکسان هستند. این حالات را دوگان یکدیگر می‌نامیم. از طرف دیگر، ۵ دور از ساختار مورد نظر تفاضلات غیر ممکن زیادی نیز داراست. برای مثال داریم:

$$(\alpha_1 = 0, \alpha_2 = 0, \alpha_3 \neq 0, \alpha_4 \neq 0) \nrightarrow (\beta_1 = 0, \beta_2 = 0, \beta_3 \neq 0, \beta_4) \quad (۱۵)$$

همه‌ی این حالات از روند اثبات حذف می‌شوند. در ادامه جزئیات تحلیل یکی از حالات شرح داده می‌شود.

برای حالت ورودی $(\alpha_1 = 0, \alpha_2 \neq 0, \alpha_3 = 0, \alpha_4 = 0)$ (دوگان $(\alpha_1 = 0, \alpha_2 = 0, \alpha_3 = 0, \alpha_4 \neq 0$ خواهیم داشت: $\delta_1 = \delta_2 = \delta_4 = \delta_5 = 0$ و $\delta_3 \neq 0, \delta_6$ و β_3 . بنابراین تنها متغیرهای مذکور در رابطه‌ی (۱) حضور دارند و مقادیر $DP(\alpha_4 \to \delta_3), DP(\delta_6 \to \beta_3)$ محدود است. پس داریم:

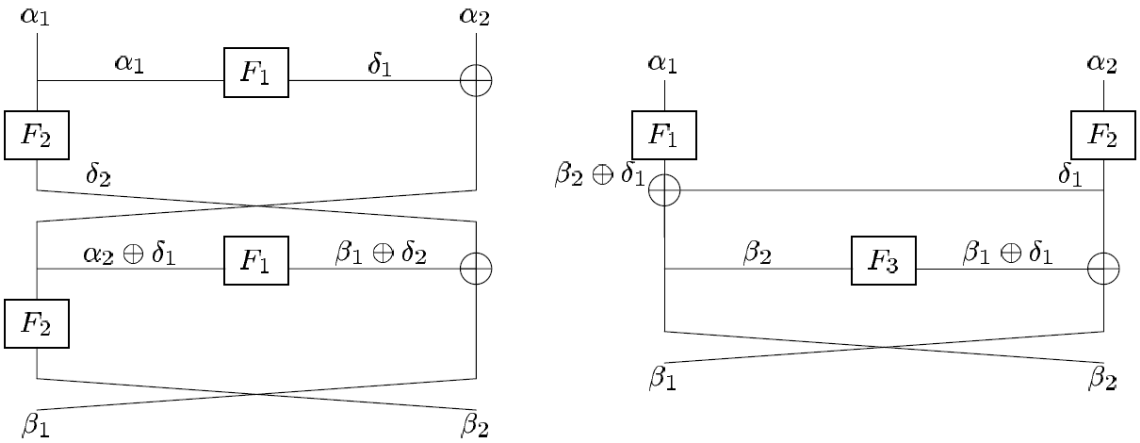
$$DP(\alpha \to \beta) = \sum_{\delta_3,\delta_6} DP(\alpha_4 \to \delta_3).DP(\delta_3 \to \delta_6).DP(\delta_6 \to \beta_3).DP(\alpha_4 \to \beta_1 \oplus \delta_3).DP(\beta_1 \to \beta_2 \oplus \delta_6).DP(\beta_3 \to \alpha_4 \oplus \beta_4) \leq p^4.\sum_{\delta_3,\delta_6} DP(\delta_3 \to \delta_6).DP(\beta_1 \to \beta_2 \oplus \delta_6) \leq p^4.\sum_{\delta_6} DP(\beta_1 \to \beta_2 \oplus \delta_6).(\sum_{\delta_3} DP(\delta_3 \to \delta_6)) = p^4 \quad (۱۶)$$

با محاسبه کلیه‌ی حالات می‌توانیم نتیجه‌گیری کنیم که اگر تابع F یک به یک و پوشا باشد، احتمال تفاضلی r دور از الگوریتم‌های مبتنی بر ساختار فیستلی نوع دوم، دارای کران بالای p^4 است که p احتمال تفاضلی تابع دور می‌باشد [۱۲].

۲-۳- امنیت اثبات‌پذیر برای ساختارهای فیستلی نوع A و B

ساختارهای فیستلی نوع A و B به ترتیب از دو و سه تابع F در هر دور استفاده می‌کنند. ساختارهای آنها در شکل5 نشان داده شده است. برای ساختار فیستلی نوع A داریم:

$$DP(\alpha \to \beta) = \sum_{\delta_1,\delta_2} DP(\alpha_1 \to \delta_1).DP(\alpha_1 \to \delta_2).DP(\alpha_2 \oplus \delta_1 \to \beta_2).DP(\alpha_2 \oplus \delta_1 \to \beta_1 \oplus \delta_2) \quad (۱۷)$$



ساختار فیستلی نوع A ساختار فیستلی نوع B

شکل5 – تفاضل‌های ۲ و ۱ دور از ساختارهای فیستلی نوع A **و** B.

همچنین اگر تابع F یک به یک و پوشا باشد، احتمال تفاضلی برای r دور از ساختار فیستلی نوع A برابر است، که احتمال تفاضلی تابع دو می‌باشد [۱۳].

برای ساختار نوع B داریم:

$$DP(\alpha \to \beta) = \sum_{\delta_1} DP(\alpha_1 \to \beta_2 \oplus \delta_1).DP(\alpha_2 \to \delta_1).DP(\beta_2 \to \beta_1 \oplus \delta_1). \quad (۱۸)$$

این را هم می‌توانیم نتیجه بگیریم که اگر تابع F یک به یک و پوشا باشد، احتمال تفاضلی r دور ساختن از ساختار فیستلی نوع B برابر با p^2 است که p احتمال تفاضلی تابع دور می‌باشد [۱۳].

۳–۳– امنیت اثبات‌پذیر برای ساختارهای A, B, C, D از MISTY-FO

شکل6 شمای کلی ساختارهای MISTY-FO را نشان می‌دهد. ساختارهای A, B, C, D از MISTY-FO بر اساس موقعیت XOR در شکل6 تعریف می‌شوند. هر کدام از ساختارهای A, B, C, D دو تابع F یک به یک و پوشا در هر دور دارند. برای ساختار MISTY-FO نوع A داریم:

$$DF(\alpha \to \beta) = \sum_{\delta_I, 0 \le I \le 6} (\alpha_1 \oplus \alpha_2 \to \delta_1)(\alpha_3 \oplus \alpha 4 \to \delta_2)(\delta_1 \oplus \alpha_4 \to \delta_3)(\delta_3 \oplus \alpha_2 \to \delta_4)(\delta_2 \oplus \delta_3 \to \delta_5)(\delta_1 \oplus \delta_4 \to \delta_6)(\delta_5 \oplus \delta_4 \to \beta_2)(\delta_3 \oplus \delta_6 \to \beta_6)(\beta_2 \oplus \delta_6 \to \beta_1)(\beta_4 \oplus \delta_5 \to \beta_3) \quad (۱۹)$$

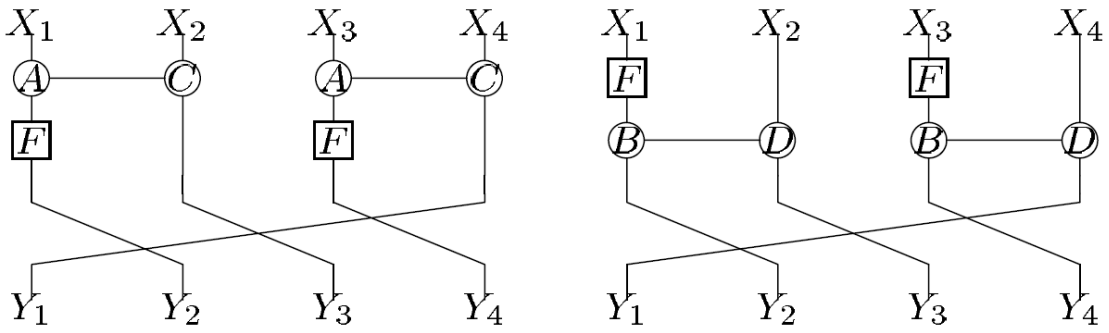
برای ساختار MISTY-FO نوع B داریم:

$$DF(\alpha \to \beta) = \sum_{\delta_I, 0 \le I \le 6} (\alpha_1 \to \delta_1)(\alpha_3 \to \delta_2)(\alpha_4 \to \delta_3)(\alpha_2 \to \delta_4)(\delta_1 \oplus \alpha_2 \to \delta_6)(\alpha_4 \oplus \delta_2 \to \delta_5)(\alpha_4 \oplus \delta_2 \oplus \delta_4 \to \delta_1 \oplus \alpha_2 \oplus \delta_3 \oplus \delta_5 \oplus \beta_2)(\alpha_2 \oplus \delta_1 \oplus \delta_3 \to \delta_2 \oplus \alpha_4 \oplus \delta_4 \oplus \delta_6 \oplus \beta_4)(\delta_2 \oplus \alpha_4 \oplus \delta_4 \oplus \delta_6 \to \beta_2 \oplus \beta_1)(\delta_1 \oplus \alpha_2 \oplus \delta_3 \oplus \delta_5 \to \beta_3 \oplus \beta_4) \quad (۲۰)$$

پس می‌توان نتیجه گرفت که اگر تابع F یک به یک و پوشا باشد، احتمال تفاضلی r دور از ساختارهای MISTY-FO نوع A , B برابر p^4 است، که p احتمال تفاضلی تابع F می‌باشد [۱۳]. برای ساختار MISTY-FO نوع C داریم:

$$DF(\alpha \to \beta) = \sum_{\delta_I, 0 \le I \le 6} (\alpha_1 \to \delta_1)(\alpha_3 \to \delta_2)(\alpha_4 \oplus \alpha_3 \to \delta_3)(\alpha_2 \oplus \alpha_1 \to \delta_4)(\delta_2 \oplus \alpha_2 \to \delta_5)(\alpha_4 \oplus \delta_1 \oplus \alpha_3 \to \delta_6)(\alpha_3 \oplus \delta_1 \oplus \delta_4 \oplus \alpha_4 \to \delta_2 \oplus \alpha_2 \oplus \delta_3 \oplus \delta_6 \oplus \beta_3)(\alpha_2 \oplus \delta_2 \oplus \delta_3 \to \delta_1 \oplus \alpha_3 \oplus \delta_4 \oplus \delta_5 \oplus \beta_1 \oplus \alpha_4)(\delta_2 \oplus \alpha_2 \oplus \delta_3 \oplus \delta_6 \oplus \beta_3 \to \beta_1)(\delta_1 \oplus \alpha_3 \oplus \alpha_4 \oplus \delta_5 \oplus \delta_4 \oplus \beta_1 \to \beta_3) \quad (۲۱)$$

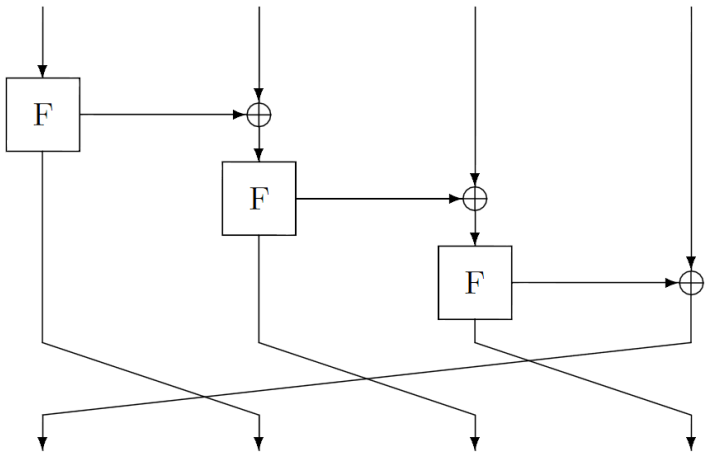
برای ساختار MISTY-FO نوع D داریم:



شکل6 – **شمای کلی ساختار** MISTY-FO

$$DF(\alpha \to \beta) = \sum_{\delta_I, 0 \le I \le 6} (\alpha_1 \to \delta_1)(\alpha_3 \to \delta_2)(\delta_1 \oplus \alpha_3 \to \delta_4)(\delta_2 \oplus \alpha_4 \to \delta_3)(\delta_2 \oplus \delta_4 \to \delta_5)(\delta_1 \oplus \delta_3 \to \delta_6)(\delta_5 \oplus \delta_3 \to \beta_3 \oplus \beta_4)(\delta_4 \oplus \delta_6 \to \beta_1 \oplus \beta_2)(\beta_3 \oplus \beta_4 \oplus \delta_6 \to \beta_1)(\beta_1 \oplus \beta_2 \oplus \delta_5 \to \beta_3) \quad (۲۲)$$

پس می‌توانیم نتیجه بگیریم که اگر تابع F یک به یک و پوشا باشد، احتمال تفاضلی r دور از ساختارهای MISTY-FO نوع C, D برابر $2p^4$ است، که p احتمال تفاضلی تابع F می‌باشد [۱۳].



شکل 7 – **ساختار شبه**–Skipjack

۴–۳– امنیت اثبات‌پذیر برای ساختار شبه–Skipjack

شکل7 ساختار شبه-Skipjack را نشان می‌دهد. برای ساختار شبه-Skipjack داریم:

$$DP(\alpha \to \beta) = \sum_{\delta_i, 1 \le i \le 11} DP(\alpha_1 \to \delta_1).DP(\alpha_2 \oplus \delta_1 \to \delta_2).DP(\alpha_3 \oplus \delta_2 \to \delta_3).DP(\alpha_4 \oplus \delta_3 \to \delta_4).DP(\delta_1 \oplus \delta_4 \to \delta_5).DP(\delta_2 \oplus \delta_5 \to \delta_6).DP(\delta_3 \oplus \delta_6 \to \quad (۲۳)$$

$\delta_7).DF(\delta_4 \oplus \delta_7 \to \delta_8).DP(\delta_5 \oplus \delta_8 \to \delta_9).DP(\delta_6 \oplus \delta_9 \to \delta_{10}).DP(\delta_7 \oplus \delta_{10} \to \delta_{11}).DP(\delta_8 \oplus \delta_{11} \to \beta_3 \oplus \beta_4).DP(\delta_9 \oplus \beta_3 \oplus \beta_4 \to \beta_1).DP(\delta_{10} \oplus \beta_1 \to \beta_2).DP(\delta_{11} \oplus \beta_2 \to \beta_3)$

و می‌توان اینگونه نتیجه گرفت که اگر تابع F یک به یک و پوشا باشد، احتمال تفاضلی $r \geq 15$ دور از ساختار شبه-Skipjack برابر p^4 است، که p احتمال تفاضلی تابع F می‌باشد [۱۱] [۱۴].

در این قسمت، مثال‌هایی از نحوه‌ی اثبات امنیت رمزهای فیستلی در برابر حملات خطی و تفاضلی ارائه شد. روش‌های موجود برای محاسبه‌ی احتمال تفاضلی، نوشتن معادلات تفاضلی کل ساختار و حل آن برای تمامی حالات ممکن ورودی و خروجی است. برای اعمال این روش، افرادی با تجربه و تخصص بالا و صرف زمانی بسیار زیاد، حتی برای ساختارهای ۴ پورتی، مورد نیاز است. به علاوه، برای طرح‌های سبک‌وزن جدید، که عموماً ۸ پورتی هستند، محاسبه‌ی امنیت اثبات‌پذیر با روش های موجود تقریباً غیر ممکن است. در قسمت بعد، ایده‌های جدیدی برای محاسبه‌ی سیستماتیک امنیت اثبات پذیر ساختارهای فیستلی ارائه می‌کنیم. روش پیشنهادی برای ساختارهای ۸ پورتی نیز قابل اعمال است و همچنین، به صورت نرم‌افزاری و بدون دخالت کاربر امنیت اثبات‌پذیر ساختارهای فیستلی را محاسبه می‌کند.

۴. راهکار پیشنهادی برای محاسبه‌ی نرم‌افزاری امنیت اثبات‌پذیر ساختارهای فیستلی

تلاش‌های زیادی به‌منظور ارائه‌ی روشی جامع برای محاسبه‌ی امنیت اثبات‌پذیر در رمزهای بلوکی انجام شده است؛ اما هنوز یک راهکار سیستماتیک، با قابلیت پیاده‌سازی نرم‌افزاری، که بتواند در زمان معقول، نتیجه‌ی مناسبی داشته باشد، ارائه نشده است.برخی از راهکارهای موجود، پیچیدگی محاسباتی بسیار بالایی دارند و تنها برای برخی الگوریتم‌های خاص، قابل استفاده هستند. هم‌اکنون، امنیت یک الگوریتم رمزنگاری، با محاسبه‌ی دستی، صرف زمان بسیار زیاد و دقت پایین انجام می‌شود. ضمن اینکه روش‌های مورد استفاده، فقط در الگوریتم‌های کوچک قابل استفاده هستند.

در این مقاله، ابتدا راهکاری جامع برای محاسبه‌ی سیستماتیک امنیت اثبات‌پذیر ساختارهای فیستلی در برابر تحلیل-های خطی و تفاضلی، با امکان پیاده‌سازی عملی و پیچیدگی محاسباتی پایین ارائه کردیم. در مرحله‌ی بعد، نرم‌افزاری تهیه می‌شود که با دریافت پارامترهای رمز فیستلی، میزان امنیت و یا تعداد دورهای لازم برای تامین امنیت را مشخص می‌کند. روش پیشنهادی می‌بایست برای ساختارهایی با تعداد پورت‌های ورودی بالا و شافل‌های نامنظم نیز قابل اعمال باشد و به‌علاوه، نتیجه را در زمان مناسبی نمایش دهد.

۵. نتیجه‌گیری

الگوریتم پیشنهادی، با تکنیک‌های موجود برای اثبات امنیت کاملا متفاوت است و پیچیدگی محاسباتی بسیار پایین‌تری دارد.نرم‌افزار نهاییبرای انواع ساختارهای فیستلی، اعم از فیستلی تعمیم‌یافته، A/B/C/DMISTY-FO، Skipjack-like، ساختارهای ۸ پورتی و ساختارهای با شافل‌های بهینه کاربرد دارد. همچنین برنامه به گونه‌ای تهیه می‌شود که کاربر کمترین دخالت ممکن را داشته باشد و تنها نحوه‌ی ارتباط پورت‌های ورودی و خروجی در یک دور الگوریتم را به برنامه بدهد.

۶. مراجع

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, 1991.

[2] P. A. Bagane and S. Kotrappa, "Bibliometric Survey for Cryptanalysis of Block Ciphers towards Cyber Security," *Libr. Philos. Pract.*, pp. 1–18, 2020.

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

[4] K. Nyberg, "Affine linear cryptanalysis," *Cryptogr. Commun.*, vol. 11, no. 3, pp. 367–377, 2019.

[5] K. Aoki and K. Ohta, "Strict evaluation of the maximum average of differential probability and the maximum average of linear probability," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 80, no. 1, pp. 2–8, 1997.

[6] M. Matsui, "New structure of block ciphers with provable security against differential and linear cryptanalysis," in *International Workshop on Fast Software Encryption*, 1996, pp. 205–218.

[7] K. Nyberg and L. R. Knudsen, "Provable security against differential cryptanalysis," in *Annual International Cryptology Conference*, 1992, pp. 566–574.

[8] K. Nyberg, "Linear approximation of block ciphers," in *Workshop on the Theory and Application of of Cryptographic Techniques*, 1994, pp. 439–444.

[9] K. Nyberg, "Generalized feistel networks," in *International conference on the theory and application of cryptology and information security*, 1996, pp. 91–104.

[10] S. Hong, S. Lee, J. Lim, J. Sung, D. Cheon, and I. Cho, "Provable security against differential and linear cryptanalysis for the SPN structure," in *International Workshop on Fast Software Encryption*, 2000, pp. 273–283.

[11] J. Sung, S. Lee, J. Lim, S. Hong, and S. Park, "Provable security for the Skipjack-like structure against differential cryptanalysis and linear cryptanalysis," in *International Conference on the Theory and Application of Cryptology and Information Security*, 2000, pp. 274–288.

[12] C. Lee, J. Kim, J. Sung, S. Hong, and S. Lee, "Provable security for an RC6-like structure and a MISTY-FO-like structure against differential cryptanalysis," in *International Conference on Computational Science and Its Applications*, 2006, pp. 446–455.

[13] 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 Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 91, no. 10, pp. 3047–3058, 2008.

[14] J. Zhang, T. Cui, and C. Jin, "Structural Attack on Reduced-Round Skipjack," *IEEE Access*, vol. 6, pp. 3176–3183, 2017.