دانشگاه صنعتی امیرکبیر

(پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر و فن‌آوری اطلاعات

گزارش کتبی سمینار

درس معماشناسی کاربردی

عنوان

حمله تلاقی در میان به ساختارهای فایستل

نگارش

سید محمدمهدی احمدپناه

۹۴۱۳۱۰۸۶

استاد راهنما

دکتر بابک صادقیان

بهمن ۱۳۹۴

چکیده

در گزارش پیش‌رو، به مطالعه ساختارهای فایستل و انواع آن‌ها پرداخته می‌شود. با بیان ویژگی‌های این‌گونه ساختارها، به روش‌های گوناگون حمله و تحلیل آن‌ها اشاره خواهد شد. از بین انواع حملات، حمله تلاقی در میان به طور ویژه مطرح می‌شود. روش‌ها و تکنیک‌های مختلف برای بهبود این حمله ذکر شده، ویژگی‌ها و سناریو حمله هر یک توضیح داده می‌شود.

از جمله نتایجی که در این گزارش بیان شده است، می‌توان به توصیه برای استفاده از حداقل شش دور برای سیستم‌های رمز مبتنی بر ساختار فایستل و کاهش پیچیدگی‌های زمانی و حافظه‌ای حمله تلاقی در میان به کمک تکنیک‌های گوناگون مطرح شده، اشاره داشت.

واژه‌های کلیدی:

حمله تلاقی در میان، ساختار فایستل، سیستم رمز قطعه‌ای، حملات عام، پیچیدگی زمانی و حافظه‌ای

فهرست عناوین

صفحه

فهرست اشکال

صفحه

صفحه

فهرست جداول

فصل اول

مقدمه

مقدمه

با توجه به این‌که سیستم رمز قطعه‌ای از ساختارهای اولیه و پایه‌ای با کاربرد گسترده و متنوع در معماشناسی محسوب می‌شود، به عنوان فناوری ضروری در رمزنگاری نوین در نظر گرفته می‌شود. علاوه بر این، مطالعه بر روی طراحی یک سیستم رمز قطعه‌ای امن و کارا، در طراحی ساختارهای پایه‌ای متقارن دیگر، مانند توابع درهم‌ساز و سیستم‌های رمز دنباله‌ای، کاربرد زیادی خواهد داشت [۸].

پس از توسعه سیستم رمز DES در سال ۱۹۷۷، پیشرفت‌های زیادی در این حوزه پدید آمد. اکنون نیاز به توسعه سیستم‌های رمز سبک‌وزن و با تأخیر کم، به دلیل کاربرد امنیت در شبکه‌های کامپیوتری، بیش از پیش احساس می‌شود. سیستم‌های رمزی مانند PRESENT، KATAN/KTANTAN، LED و Piccolo از این حیث مطرح شدند.

به طور کلی، یک سیستم رمز دارای ساختار جانشینی-جایگشتی یا SPN به یک تابع وارون‌پذیر برای پشتیبانی از ترجمه رمز نیاز دارد [۸]. پس یک سیستم رمز SPN به همراه یک تابع ترجمه رمز، از نظر تعداد گیت‌های سخت‌افزاری، به مساحت اضافه‌ای نیاز خواهد داشت. اما یک ساختار رمز فایستل، به عنوان یکی از ساختارهای رمز شناخته‌شده، برای یک سیستم رمز سبک‌وزن که هم از عملیات رمزکردن و هم از عملیات ترجمه رمز پشتیبانی کند، بسیار مناسب خواهد بود. به این خاطر که نیازی به تهیه یک تابع وارون‌پذیر وجود ندارد. از طرفی، می‌توان از تعداد دورهای کم ساختار فایستل استفاده کرد که این باعث داشتن یک سیستم رمز با تأخیر کم می‌شود. البته هنوز مشخص نیست که چه تعداد دور کافی است تا یک ساختار فایستل امن تلقی شود.

ساختارهای فایستل یکی از مهم‌ترین و پرکاربردترین انواع طرح‌های رمزنگاری در پژوهش‌ها و کاربردها به شمار می‌روند. ساختارهای فایستل توسط هورست فایستل[1] در طراحی سیستم رمزنگاری لوسیفر[2] ابداع شد و پس از آن، در طراحی سیستم رمز DES مشهور شد. این ساختار، پایه بسیاری از سیستم‌های رمز قطعه‌ای است که بعد از آن مطرح شد. از جمله این سیستم‌های رمز می‌توان به FEAL،

[1] Horst Feistel

[2] Lucifer

GOST، Khufu و Khafre، LOKI، CAST-128، Blowfish و RC5 اشاره کرد [۸]. همان‌طور که مطرح شد، این ساختار تأثیر بسزایی در پیشرفته رمزنگاری، چه در بخش نظری و چه در بخش عملی، داشته است. به عنوان مثال، در ساختار لوبی-راکوف برای جایگشت‌های شبه‌تصادفی و سیستم‌های رمز قطعه‌ای بسیاری کاربرد داشته است.

پس می‌توان دید که مطالعه درباره امنیت ساختار فایستل، به طراحی و تولید سیستم‌های رمز با امنیت بالاتر و کارایی بیشتر خواهد انجامید. در این گزارش، به مروری بر حملات گوناگون و عام روی این ساختار، و به طور ویژه حمله تلاقی در میان، خواهیم پرداخت.

فصل دوم

ساختار فایستل، ویژگی‌ها و انواع آن

۱.۲ ساختار فایستل

همان‌طور که قبلا گفته شد، ساختار فایستل توسط هورست فایستل و در طراحی سیستم رمزنگاری لوسیفر مطرح شد. اما شهرت و کاربرد گسترده آن به واسطه استفاده از آن در سیستم رمز DES می‌باشد.

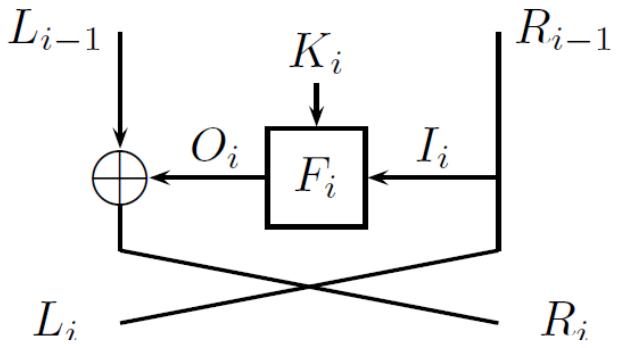
نکته ارزش‌مند آن است که در سیستم‌های رمز مبتنی بر ساختار فایستل، الگوریتم‌های رمز و ترجمه تنها با استفاده از یک طرح قابل انجام است، که این خود یکی از مزایای اصلی این ساختار در پیاده‌سازی به شمار می‌رود. این ساختار در سیستم‌های رمز بسیاری کاربرد دارد. از جمله این سیستم‌های رمز می‌توان به DES، Triple-DES، Camellia، CAST و بسیاری از نامزدهای AES نیز اشاره کرد. علاوه بر سیستم‌های رمز قطعه‌ای استاندارد مطرح‌شده، این ساختار یکی از گزینه‌های جذاب برای سیستم‌های رمز سبک‌وزن خواهد بود که برای سیستم‌های رمز SIMON، LBlock و Piccolo از آن استفاده شده است. از طرفی، کاربرد ساختار فایستل تنها محدود به سیستم‌های رمز نمی‌شود و در طراحی ساختارهای پایه‌ای دیگر معماشناسی مانند توابع درهم‌ساز نظیر SHAvite-3، پیشنهاد CAESAR برای طرح تصدیق اصالت LAC و دیگر ساختارهای پایه‌ای کاربرد فراوان دارد [۲].

در [۱] به ساختارهای فایستل عام، که دور i-ام آن در شکل ۱ آمده است، توجه می‌شود. این ساختار، یک قطعه n-بیتی را به دو بخش مساوی (L_i, R_i) تقسیم می‌کند. هم‌چنین از زیرکلیدهای n/2-بیتی مسقل در l-دور خود استفاده می‌کند و توابع دور F_i دارند که روی ورودی‌ها، خروجی‌ها و زیرکلیدهای n/2-بیتی عمل می‌کند. این توابع دور، از حیث آن‌که با حملات سریع‌تر از جستجوی جامع شکسته نمی‌شوند، کامل و بی‌نقص هستند. این انتخاب متغیرها در این ساختار باعث می‌شود که هر دو دور متوالی در یک ساختار فایستل، مانند یک دور در یک ساختار غیرفایستلی که n-بیت ورودی، خروجی و زیرکلید دارد، در نظر گرفته شود.

برای تعریف دقیق‌تر این ساختار، نمادگذاری زیر را می‌توان در نظر داشت [۵]:

- $I_n = \{0,1\}^n$ مجموعه همه رشته‌های با طول n باینری.
- F_n مجموعه همه توابع از I_n به I_n است.

- مجموعه همه جایگشت‌های از I_n به I_n را B_n می‌گیریم. پس B_n زیرمجموعه F_n است و تعداد اعضای آن برابر با $(2^n)!$ خواهد بود.



شکل ۱ - دور i-ام از یک ساختار فایستل [۱]

- اگر f_1 را یکی از توابع F_n، و L، R، S و T را عناصری از I_n بگیریم، پس می‌توان چنین تعریف کرد که:

$$\Psi(f_1)[L,R] = [S,T] \overset{\text{def}}{\Leftrightarrow} \begin{cases} S = R \\ \text{and} \\ T = L \oplus f_1(R) \end{cases}$$

- اگر f_1، f_2، ...، f_k، k تابع از F_n باشند، پس می‌توان تعریفی به شکل زیر داشت:

$$\Psi^k(f_1,\ldots,f_k) = \Psi(f_k) \circ \cdots \circ \Psi(f_2) \circ \Psi(f_1)$$

جایگشت $\Psi(f_1, \ldots, f_k)$ را یک طرح فایستل k-دوری می‌نامیم.

۲.۲ ویژگی‌های ساختار فایستل

همان‌طور که می‌دانیم، به سادگی اثبات می‌شود که ساختار فایستل، مستقل از تابع دور، یک به یک و پوشاست. این ویژگی باعث می‌شود تا در انتخاب تابع دور محدودیت خاصی نداشته باشیم.

با توجه به متقارن بودن این ساختار، می‌توان از یک طرح یکسان هم برای رمزکردن و هم برای ترجمه رمز استفاده کرد. البته باید گفت که ممکن است ترتیب زیرکلیدها با توجه به طرح سیستم رمز، تغییر کند.

ویژگی دیگری که در این ساختار قابل ذکر است، مستقل بودن زیرکلیدهای هر دور از زیرکلیدهای دیگر است. به این معنا که گرچه ممکن است یک کلید اصلی وجود داشته باشد و با یک طرح برنامه‌ریز، زیرکلیدهای دورهای مختلف تولید شوند، اما هریک از زیرکلیدها را می‌توان نسبت به زیرکلید دیگر، مستقل در نظر گرفت.

از طرف دیگر، این ویژگی‌ها و ساختار کلی فایستل باعث می‌شود تا هر دو دور متوالی از یک طرح با ساختار فایستل را معادل با یک دور در یک ساختار غیرفایستلی n-بیتی در نظر گرفت.

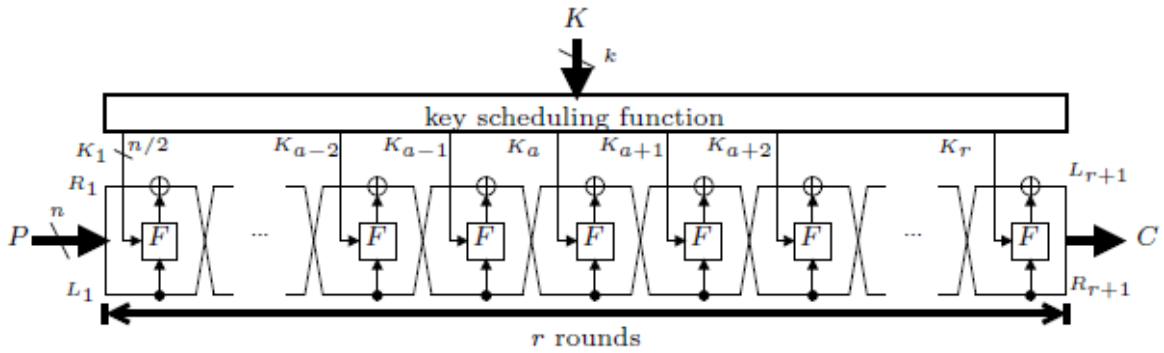
۳.۲ انواع ساختارهای فایستل

در یک دسته‌بندی، می‌توان انواع ساختارهای فایستل را به دو دسته زیر تقسیم کرد:

- متوازن

-نامتوازن

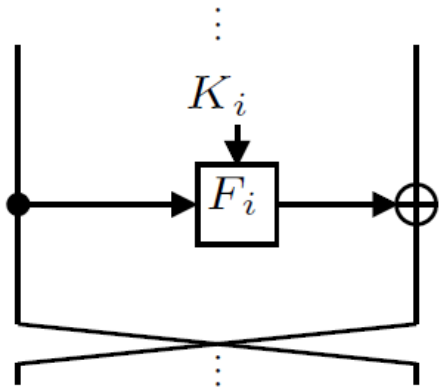
ساختار فایستلی متوازن گفته می‌شود اگر طول دو قسمت سمت چپ (L) و سمت راست (R) در آن، یکسان باشد [۸]. به طور مشابه، اگر تعداد بیت‌های دو قسمت مجزای ساختار یکسان نباشد، به آن ساختار نامتوازن گفته خواهد شد. در شکل ۲، نمونه‌ای از یک ساختار فایستل متوازن مشاهده می‌شود.



شکل ۲ - نمونه‌ای از ساختار فایستل متوازن [۸]

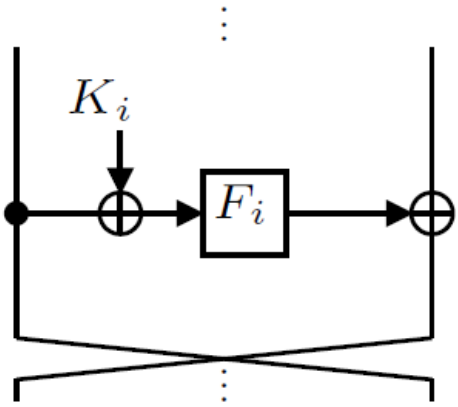
در دسته‌بندی دیگری، می‌توان ساختارهای فایستل را به سه نوع تقسیم‌بندی کرد:

- فایستل-۱: ساختار فایستلی که توابع دور با کلیدهای تصادفی[۳] دارند. هر زیرکلید مستقل و دلخواه در نظر گرفته می‌شود. پس، هر تابع دور از دیگری مستقل خواهد بود.



شکل ۳ – نمایی از ساختار فایستل-۱ [۸]

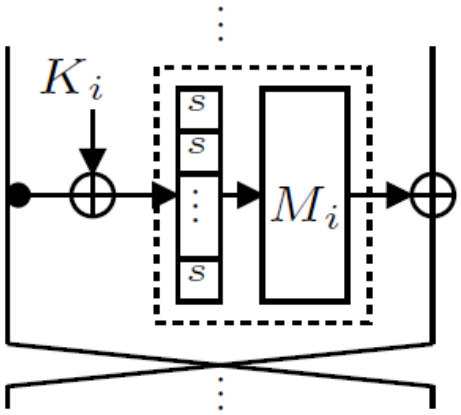
- فایستل-۲: ساختار فایستلی که هر زیرکلید قبل از ورود به تابع دور، XOR می‌شود. می‌توان اینگونه بیان کرد که $Y_i = F_i(X_i \oplus K_i)$، که در آن F_i بیانگر تابع دور برای دور i-ام است.



شکل ۴ – نمایی از ساختار فایستل-۲ [۸]

[3] Random

- فایستل-۳: ساختار فایستل-۲ای است که تابع دور در آن، یا همان F_i، باید یک تابع دور از نوع SP باشد؛ یعنی باید شامل یک لایه S-box دوطرفه (لایه S) و یک لایه پخش‌کننده خطی (لایه P) باشد، که البته زیرکلید n/2-بیتی هر دور در آن، باید قبل از ورود به لایه S، XOR شده باشند. هر لایه S باید شامل m عدد S-box l-بیتی و هر لایه P شامل یک ماتریس خطی m در m به نام M_i باشد.



شکل ۵ – نمایی از ساختار فایستل-۳ [۸]

شایان ذکر است که طبق تعاریف فوق، فایستل-۳ زیرمجموعه‌ای فایستل-۲، و آن نیز زیرمجموعه فایستل-۱ است و اندازه کلید اصلی با فایستل-[k] بیان می‌شود.

فصل سوم

حمله‌های عام به ساختار فایستل

۱.۳ تعریف حملات عام

حملات عام به حملاتی گفته می‌شود که در برابر بیشتر طرح‌های رمز کاراست [۵]. نکته مهم دیگر این است که این حملات باید دارای پیچیدگی ناچیزی در مقایسه با جستجوی جامع برای همه ورودی‌های ممکن جایگشت باشند. اگر فرض کنیم که یک جایگشت 2n-بیت به 2n-بیت داشته باشیم، یک حمله عام، حمله‌ای خواهد بود که دارای پیچیدگی بسیار کم‌تری نسبت به $O(2^{2n})$ باشد، زیرا برای 2n-بیت، 2^{2n} ورودی ممکن وجود دارد.

۲.۳ حملات عام روی ساختارهای فایستل

به سادگی می‌توان دید که برای یک طرح فایستل با تنها یک دور، حمله عامی با یک پرس‌وجو از جایگشت‌ها و $O(1)$ محاسبه وجود دارد. به این ترتیب که فقط کافی است تا این بررسی صورت بگیرد که آیا نیمه اول خروجی با نیمه دوم ورودی یکسان است یا خیر.

برای یک طرح فایستل دو دوری نیز می‌توان نشان داد که حمله عامی با پیچیدگی $O(1)$ برای ورودی‌های منتخب یا پیچیدگی $O(2^{\frac{n}{2}})$ برای ورودی‌های دلخواه وجود دارد.

برای طرح‌های با بیش از سه دور نیز لوبی و راکوف نشان داده‌اند که همه حملات عام به طرح‌های فایستل، حداقل به $O(2^{\frac{n}{2}})$ ورودی، حتی اگر منتخب باشند، نیاز دارند.

علاوه بر این، برای چهار دور نیز همه حملات عام به طرح‌های فایستل به $O(2^{\frac{n}{2}})$ ورودی نیاز دارند، حتی اگر مهاجم قوی‌تری وجود داشته باشد که بتواند از ورودی‌های منتخب و خروجی‌های منتخب بهره ببرد.

برای پنج دور و بیشتر از آن، این سوال به طور کلی باز مانده است. البته می‌توان ثابت کرد که برای پنج دور و بیشتر، حداقل تعداد پرس‌وجوها باید $O(2^{\frac{2n}{3}})$ باشد، حتی اگر پیچیدگی محاسباتی نامحدود داشته باشیم. همچنین، نشان داده شده است که برای شش دور و بیشتر از آن نیز باید تعداد پرس‌وجوها حداقل $O(2^{\frac{3n}{4}})$ باشد.

باید دقت داشت که اگر پیچیدگی محاسباتی نامحدود در نظر گرفته شود، می‌توان با یک جستجوی جامع روی همه توابع دور ممکنِ یک طرح فایستل، حمله‌ای انجام شود که نیازمند $O(2^n)$ پرس‌وجو است. با این حال، کماکان به عنوان یک مسئله باز می‌توان دانست که آیا حملات عامی برای طرح‌های بیشتر از پنج دور وجود دارد یا نه، به شرطی که پیچیدگی خیلی کوچکتر از $O(2^{2n})$ داشته باشد.

دو حمله عام مطرح‌شده در مقاله [۵]، دارای این مشخصات هستند:

- حمله‌ای با $O(2^{\frac{7n}{4}})$ محاسبه بر روی $O(2^{\frac{7n}{4}})$ زوج ورودی/خروجی دلخواه.
- حمله‌ای با $O(2^{\frac{3n}{2}})$ محاسبه بر روی $O(2^{\frac{3n}{2}})$ ورودی منتخب.

اما باید توجه داشت که این سوال برای طراحان سیستم‌های رمز وجود دارد که چه تعداد دور برای یک سیستم رمز امن و کارای مبتنی بر ساختار فایستل مناسب است. زیرا به خاطر افزایش سرعت الگوریتم رمز و کاهش پیچیدگی محاسباتی و سبک‌وزن بودن سیستم رمز برای اکثر کاربردها، باید تعداد دورهای طرح فایستل کم باشد. از طرف دیگر، بیان شد که تعداد دورهای کم برای یک سیستم رمز باعث تحلیل آن سیستم رمز می‌شود. پس برای افزایش امنیت الگوریتم رمز مبتنی بر ساختار فایستل، باید تعداد دور زیاد لحاظ کرد. به همین دلیل، یک طراح سیستم رمز با چالشی برای انتخاب تعداد دور مناسب مواجه است و این سوال نیز یکی از مسائل باز این حوزه محسوب می‌شود. گرچه طبق یافته‌های کنونی، توصیه می‌شود حداقل شش دور برای یک سیستم رمز با پایه ساختار فایستل در نظر گرفته شود تا امنیت لازم فراهم شود.

۳.۳ انواع حملات رایج

حملات و تکنیک‌های مختلفی برای تحلیل سیستم‌های رمز وجود دارد که هر کدام نقاط قوت و ضعف مخصوص به خود را دارا می‌باشند. از جمله این حملات می‌توان به جستجوی جامع، تلاقی در میان، تحلیل خطی، تحلیل تفاضلی، انتگرال، تحلیل تفاضلی-خطی، تمایز، افراز، بومرنگ، تحلیل چرخشی، حمله زمانی، کلیدهای ضعیف و موازنه زمان-حافظه-داده اشاره داشت. در فصل بعد، به حمله تلاقی در میان پرداخته می‌شود و به طور خاص، درباره ساختارهای فایستل صحبت خواهد شد.

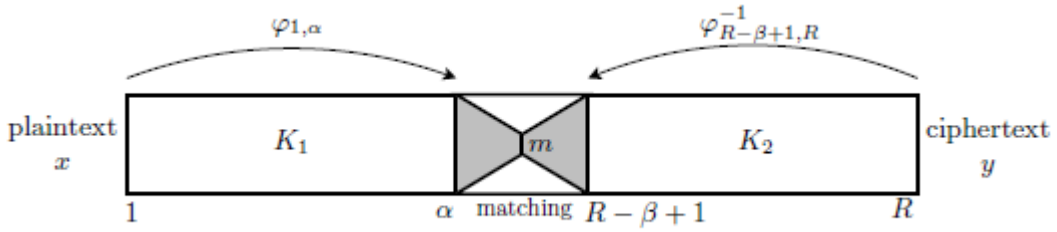
فصل چهارم

حمله تلاقی در میان و انواع تکنیک‌ها

۱.۴ حمله تلاقی در میان

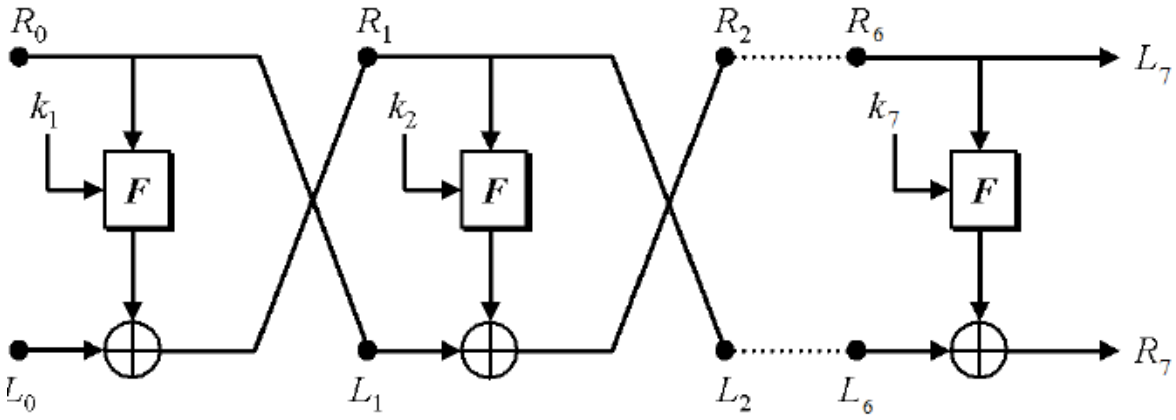
حمله تلاقی در میان پایه بسیاری از حملات رایج و مرسوم است. البته این تکنیک به نسبت حملات خطی یا تفاضلی بر روی سیستم‌های رمز قطعه‌ای کمتر رایج است. تکنیک تلاقی در میان اولین بار توسط دیفی و هلمن [۱۰] در سال ۱۹۷۷ به عنوان روشی برای تحلیل رمز طرح‌های رمزکردن دوگانه معرفی شد. در سال ۱۹۸۵، زمانی‌که چاوم و اورتس، این روش را روی انواع مختلف سیستم رمز DES دورکاهش‌یافته استفاده کردند، شهرت بیشتری کسب کرد. هم‌اکنون، این روش به عنوان یکی بخش مهم در تحلیل رمز مطرح است. در ادامه به شرح حمله تلاقی در میان اولیه می‌پردازیم.

از نماد $\varphi_{i,j}$ برای بیان یک تبدیل جزئیِ یک سیستم رمز R–دوری، با شروع از دور i–ام و پایان در بلافاصله بعد از دور j–ام آن $(1 \le i \le j \le R)$ استفاده می‌کنیم. اگر $\varphi_{1,\alpha}$ و $\varphi_{\alpha+1,R}$ از زیرکلیدهای با بیت‌های کلید مجزا استفاده می‌کنند، کلید را می‌توان با استفاده از قواعدی به دست آورد که این عمل، کارایی بهتری نسبت به brute-force روی دو زیرکلید دارد. ایده مطرح‌شده بر روی DES کاهش‌یافته اعمال شده است. هر حدس برای زیرکلید اول، اجازه محاسبه $\varphi_{1,\alpha}(p)$ را به دشمن می‌دهد، که در آن p بیانگر متن واضح است، و هر حدس برای زیرکلید دوم، باعث به دست‌آوردن $\varphi^{-1}_{\alpha+1,R}(c)$ می‌شود، که در آن c بیانگر متن رمزشده است. کلید درست آن است که در معادله $\varphi^{-1}_{\alpha+1,R}(c) = \varphi_{1,\alpha}(p)$ صدق کند.



شکل ۶ – حمله تلاقی در میان حالت اولیه [۶]

حمله تلاقی در میان، یکی از انواع حملات کم‌داده[۴] است که می‌توان روی ترکیب‌های چنددوری اعمال کرد. [۱] منظور از حمله کم‌داده این است که داده‌های کمتری نسبت به کل کتاب کد نیاز است و از طرفی تعداد کمی متن واضح معلوم لازم است. در ادامه حمله استاندارد تلاقی در میان به یک ساختار فایستل هفت دوری را بررسی خواهیم کرد.



شکل ۷ – ساختار فایستل هفت دوری

گام‌های یک حمله تلاقی در میان هفت دوری به شرح زیر است:

۱- چهار زوج متن واضح-متن رمزشده (P^i, C^i) را انتخاب می‌کنیم. $(i = 1,2,3,4)$

۲- به ازای هر مقدار از K_1، K_2 و K_3:

P_i ،که i یکی از اعداد یک تا چهار است، را از طریق سه دور اول رمز می‌کنیم و پیشنهادهای R^i_3 را مشخص می‌کنیم. این پیشنهادها را در قالب یک لیست به نام List حاوی مقادیر R^i_3 در آن ذخیره می‌کنیم.

۳- برای هر مقدار K_5، K_6 و K_7:

[4] Low-Data Attack

C_i،که i یکی از اعداد یک تا چهار است، را از طریق سه دور پایانی ترجمه می‌کنیم و پیشنهادهای حاصل از این کار را در List جستجو می‌کنیم. به ازای هر تطابق، زیرکلیدهای K_1، K_2 و K_3 را بازیابی می‌کنیم. به کمک پیش‌محاسبه یا حدس‌زدن، K_4 را به دست می‌آوریم. در پایان، همه کلید را برای رمزکردن متن واضح استفاده می‌کنیم (رمزکردن آزمایشی) تا از صحت کلید به دست آمده، اطمینان حاصل کنیم.

پیچیدگی زمانی گام دوم حدود $2^{1.5n}$ است که معادل با اندازه List نیز می‌باشد. برای محاسبه پیچیدگی زمانی گام سوم، باید گفت که با از هر طرف رمزکردن، $2^{1.5n}$ پیشنهاد کلید به دست می‌آید که هر یک مرتبط با چهار مقدار R^i_3 (شرط صافی) است. پس تعداد کل کلیدهای باقی‌مانده بعد از تطابق 2n-بیتی در گام سوم برابر است با $2^{1.5n + 1.5n - 2n} = 2^n$. به ازای هر پیشنهاد، حدسی درباره K_4 زده می‌شود. پس انتظار می‌رود که $2^{1.5n}$ رمزکردن آزمایشی در مرحله آخر داشته باشیم. به این ترتیب، پیچیدگی زمانی گام سوم معادل است با $2^{1.5n}$ که همان پیچیدگی زمانی کل حمله می‌باشد.

حمله‌ای که در این‌جا مطرح شد، از تعداد دور فرد بود و اساساً حمله تلاقی در میان، به واسطه مطرح بودن دور میانه، برای تعداد دورهای فرد معنادار خواهد بود. در ادامه به بیان تکنیک تلاقی در میان برای تعداد دورهای زوج خواهیم پرداخت [۱].

یک حمله تلاقی در میان روی ساختار فایستل 2r-دوری در نظر بگیرید. در حالت استاندارد، حمله نامتوازن خواهد بود. زیرا r زیرکلید از یک طرف از حمله تلاقی در میان حدس‌زده شده، در حالی‌که r-1 زیرکلید از طرف دیگر حدس زده شده است. هدف این است که به کمک دونیم‌کردن حدس یکی از زیرکلیدهای بین دو طرف حمله، این حمله دوباره متوازن شود. ایده اصلی برای این کار آن است که اگر در همه متن‌های واضح شرکت‌کننده در حمله، نیمه راست آن‌ها برابر با یک مقدار ثابت R_0 باشد، پس در همه رمزها خواهیم داشت: $R_1 = \text{Const} \oplus L_0$، که Const یک مقدار ثابت ناشناخته است که به K_1 بستگی دارد. با این کار می‌توان فایستل 2r-دوری را معادل با طرحی در نظر گرفت که در آن یک فایستل 2r-1-دوری و پیش از آن افزودن مقدار Const به نیمه سمت راست متن واضح است. این باعث

می‌شود تا بتوان از تکنیک پیوند و برش[5] برای دونیم‌کردن حدس درباره Const بین دو طرف تلاقی در میان، در ازای بهره‌گیری از $2^{n/4}$ متن واضح منتخب، استفاده کرد. در نتیجه، حمله متوازن شده، و پیچیدگی زمانی آن از $2^{0.5rn}$ به $2^{(0.5r-0.25)n}$ کاهش می‌یابد [۱].

۲.۴ انواع تکنیک‌های حمله

در سال‌های اخیر، پژوهش‌ها حول حمله تلاقی در میان، از جهات گوناگون و متعددی گسترش یافته است؛ مانند تطابق جزئی[6]، تطابق احتمالاتی[7]، استفاده از گراف‌های کامل دوبخشی[8]، غربال در میان[9] و تلفیق با حمله تشریح[10]. در ادامه به طور اجمالی به هر یک از آن‌ها خواهیم پرداخت.

۱.۲.۴ تطابق جزئی

به دلیل تعداد دور زیاد در الگوریتم‌های رمز کاربردی، در عمل فضای نگه‌داری مقادیر میانی دچار محدودیت است. تطابق جزئی روشی برای کاهش این مشکل در حمله تلاقی در میان است. به این گونه که به جای تطابق همه بیت‌ها در دور میانه، تنها تعداد کمی از بیت‌های انتخاب‌شده مقادیر میانی مورد توجه قرار بگیرند. این ایده اولین بار در مقاله [۶] مطرح شده است. به این ترتیب، حجم فضای نگه‌داری مقادیر میانی کاهش می‌یابد اما ممکن است سرعت به دست آوردن کلید کاهش یابد. باید دقت کرد که از این تکنیک برای کمک به حمله تلاقی در میان استفاده می‌شود.

---

[5] Splice-and-Cut

[6] Partial Matching

[7] Probablisitc Matching

[8] Bicliques

[9] Sieve-In-The-Middle

[10] Dissection

۲.۲.۴ تطابق احتمالاتی

راه‌کار دیگری برای کاهش فضای نگه‌داری مقادیر میانی در حمله تلاقی در میان است. همان‌طور که قبلا مطرح شد، به دلیل تعدد دورهای الگوریتم رمز، نمی‌توان همه مقدارهای پیشنهادی زیرکلیدها را ذخیره و جستجو کرد. در این روش، به جای تطابق قطعی همه مقادیر میانی، تطابق تعدادی از بیت‌های انتخاب‌شده یا همه بیت‌های مقادیر میانی به صورت احتمالاتی مطرح می‌شود. به این ترتیب، می‌توان زیرکلیدهای با احتمال بیشتر را به عنوان گزینه‌های مناسب برای کلید دانست.

۳.۲.۴ استفاده از گراف‌های کامل دوبخشی

ابتدا لازم است گراف کامل دوبخشی را تعریف کرد:

گراف کاملی که بتوان مجموعه رئوس آن را به دو زیرمجموعه افراز کرد، به گونه‌ای که یک یال بین دو رأس وجود داشته باشد اگر و فقط اگر یکی از آن‌ها از مجموعه اول و دیگری از مجموعه دوم باشد.

همان‌طور که در مقاله [۹] آمده است، از این تکنیک برای بهبود کارایی حمله تلاقی در میان می‌توان استفاده کرد و تعداد دورهای ممکن برای حمله را گسترش داد. با توجه به این‌که این تکنیک بر پایه حمله تلاقی در میان است، پس می‌توان از آن هم در سیستم‌های رمز قطعه‌ای و هم در توابع درهم‌ساز بهره برد. این دسته از حملات به خاطر شکستن AES کامل و IDEA کامل شناخته‌شده هستند. البته حملات ذکرشده، تنها مزیت کوچکی نسبت به جستجوی جامع دارد. این گونه که پیچیدگی محاسباتی $2^{126.1}$ برای AES-128، $2^{189.7}$ برای AES-192 و $2^{254.4}$ برای AES-256 نیاز خواهد بود. گرچه هنوز هم این حمله، بهترین حمله برای AES شناخته شده است و تنها حمله تک‌کلیده برای همه دورهای AES مطرح می‌شود.

جدول ۱ – نتایج بازیابی کلید با روش گراف کامل دوبخشی بر روی AES [۹]

rounds	data	computations/succ.rate	memory	biclique length in rounds
AES-128 secret key recovery				
8	$2^{126.33}$	$2^{124.97}$	2^{102}	5
8	2^{127}	$2^{125.64}$	2^{32}	5
8	2^{88}	$2^{125.34}$	2^{8}	3
10	2^{88}	$2^{126.18}$	2^{8}	3
AES-192 secret key recovery				
9	2^{80}	$2^{188.8}$	2^{8}	4
12	2^{80}	$2^{189.74}$	2^{8}	4
AES-256 secret key recovery				
9	2^{120}	$2^{253.1}$	2^{8}	6
9	2^{120}	$2^{251.92}$	2^{8}	4
14	2^{40}	$2^{254.42}$	2^{8}	4

ایده اولیه این تکنیک ابتدا برای تحلیل توابع درهم‌ساز مطرح شد که نشئت گرفته از روش پیوند و برش است.در صورتی که سیستم رمز در برابر حمله تلاقی در میان برای m-دور از r-دور انجام بشود، دو رویکرد مختلف برای این تکنیک بیان می‌شود که یکی بایکلیک (گراف کامل دوبخشی) طولانی[۱۱] و دیگری بایکلیک مستقل[۱۲] نامیده می‌شوند.

در بایکلیک طولانی، هدف ساختن یک گراف کامل دوبخشی برای r-m-دور باقی‌مانده است. با این‌که با افزایش r، ابعاد گراف کامل دوبخشی کوچک می‌شود، گراف‌های کامل دوبخشی کوچک-بُعدی می‌توانند با روش‌ها و ابزارهای فراوانی از تحلیل تفاضلی سیستم‌های رمز قطعه‌ای و توابع درهم‌ساز مانند حملات ارتجاعی[۱۳]، پیمایش برگشتی دنباله‌ای[۱۴] و برخوردهای محلی[۱۵] ساخته شوند. همچنین، از

[11] Long Biclique

[12] Independent Biclique

[13] Rebound

[14] Trail Backtracking

[15] Local Collisions

نقطه‌نظر نظریه اطلاعات، وجود گراف‌های کامل دوبخشی با بعد یک در یک سیستم رمز، مستقل از تعداد دورها، بسیار محتمل است.

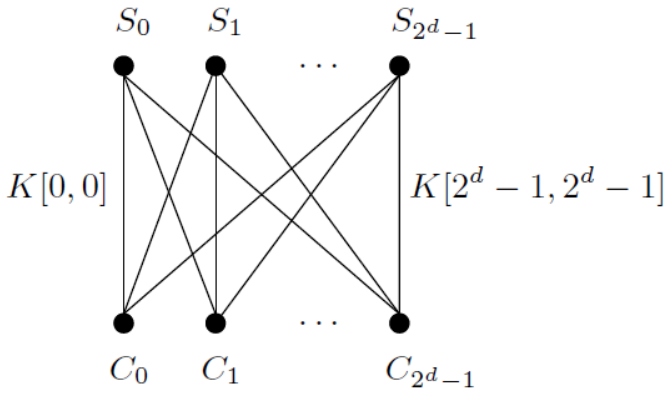
در بایکلیک مستقل، هدف ساختن گراف‌های کامل دوبخشی بزرگ‌ابعاد کارا برای bهای کوچکتر از r-m دور است که دورهای باقی‌مانده را با یک روش جدید به نام تطابق با پیش‌محاسبه پوشش دهد. همچنین، تعداد کم‌تر دورها باعث می‌شود تا از ابزارهای ساده‌تر برای ساخت گراف کامل دوبخشی استفاده کرد. این رویکرد برای سیستم‌های رمز با پخش‌کنندگی کند نسبت به r-m دور، مانند AES، بهترین است.

در ادامه مفهوم کلی یک بایکلیک را مطرح می‌کنیم. f را یک زیرسیستم رمز می‌گیریم که یک مقدار میانی S را به متن رمزشده C نگاشت می‌دهد؛ یعنی $f_K(S) = C$. پس f، 2^d مقدار میانی $\{S_j\}$ را به 2^d متن رمزشده $\{C_i\}$ با 2^{2d} کلید $\{K[i,j]\}$ متصل می‌کند.

$$\{K[i,j]\} = \begin{bmatrix} K[0,0] & K[0,1] & \dots & K[0,2^d-1] \\ \dots & & & \\ K[2^d-1,0] & K[2^d-1,1] & \dots & K[2^d-1,2^d-1] \end{bmatrix}$$

سه‌تایی $[\{C_i\}, \{S_j\}, \{K[i, j]\}]$ را یک بایکلیک d-بُعدی می‌نامند اگر برای هر i و j متعلق به $\{0, \dots, 2^d-1\}$، داشته باشیم: $C_i = f_{K[i, j]} (S_j)$.

به عبارت دیگر، در یک بایکلیک، کلید $K[i, j]$، مقدار میانی S_i را به متن رمزشده C_j نگاشت می‌دهد و بالعکس.



شکل ۸- بایکلیک d-بعدی [۹]

در حمله با استفاده از گراف‌های کامل دوبخشی، مهاجم بخشی از فضای کلید را به گروه‌هایی از کلیدها با کاردینالیتی 2^d، به ازای بعضی مقادیر d، انتخاب می‌کند و سیستم رمز را ترکیبی از دو زیرسیستم رمز f و g می‌گیرد، چنان که E = fog. پس گام‌های تحلیل با استفاده از این روش به شرح زیر خواهد بود:

- مهاجم همه کلیدهای ممکن را به زیرمجموعه‌های کلید با اندازه 2^{2d}، به ازای مقداری از d، گروه‌بندی می‌کند که کلید در یک گروه، توسط K[i, j]، که یک ماتریس $2^d \times 2^d$ است، مشخص می‌شود. مهاجم سیستم رمز را به دو زیرسیستم کوچک‌تر به نام‌های f و g می‌شکند، به طوری که E = fog، مانند یک حمله تلاقی در میان معمولی. مجموعه کلیدهای زیرسیستم‌های رمز از کاردینالیتی 2^d است و K[i,0] و K[0, j] نامیده می‌شوند.

- مهاجم برای هر گروه از 2^{2d} کلید، یک بایکلیک می‌سازد. بایکلیک d-بعدی خواهد بود، زیرا 2^d حالت میانی S_j را به 2^d متن رمزشده C_i با استفاده از 2^{2d} کلید نگاشت می‌کند.

- مهاجم 2^d متن رمزشده ممکن را می‌گیرد و با بهره‌گیری از یک اوراکل ترجمه، متن‌های واضح P_i متناظر را به دست می‌آورد.

- مهاجم یک حالت میانی S_j و متن واضح متناظر P_i را انتخاب می‌کند. سپس حمله رایج تلاقی در میان را روی f و g انجام می‌دهد.

- هر زمان که یک کاندیدای کلید یافت شد که S_j با P_i تطابق داشت، آن کلید را برای زوج دیگری از متن واضح-متن رمزشده آزمون می‌کنیم. اگر کلید برای زوج دوم نیز معتبر باشد، با احتمال بالایی کلید درست خواهد بود.

۳.۴ غربال در میان

تکنیک دیگری که در سال ۲۰۱۳ مطرح شده است [۴]، روش غربال در میان است. به کمک این روش، امکان حمله به تعداد دورهای بیشتری از طریق حمله تلاقی در میان به وجود می‌آید.

در روش غربال در میان، به جای یافتن به دنبال برخوردها در میانه، به محاسبه تعدادی از بیت‌های ورودی و خروجی یک S-box مشخص میانی پرداخته می‌شود. در این الگوریتم، به کمک کنار

گذاشتن همه کلیدهای کاندیدا که با گذار[۱۶] معتبر، متناظر نیستند، کارایی حمله افزایش می‌یابد. واضح است که این روش اجازه می‌دهد تا حملات با تعداد دورهای بیشتری به نسبت حمله تلاقی در میان کلاسیک داشته باشیم. به این دلیل که دورهای متناظر با S-box میانی S نیز پوشش داده می‌شود.

نکته دیگر آن است که این روش را می‌توان با تکنیک استفاده از گراف‌های کامل دوبخشی نیز ترکیب کرد. در بایکلیک‌های کوتاه نیز امکان افزوده‌شدن تعدادی دور به حمله بدون افزایش پیچیدگی زمانی وجود دارد، اما پیچیدگی داده‌ای بیشتری را می‌طلبد.

۴.۴ ترکیب با حمله تشریح

همان‌طور که در مقاله [۱] گفته شده، یکی از رویکردها، حمله تشریح است که توسط دینور و همکاران در CRYPTO2012 معرفی شد. تشریح می‌تواند گستره زیادی از مسائل جستجوی ترکیبیاتی را با ترکیب‌های بهبودیافته‌ای از پیچیدگی زمانی و حافظه‌ای حل کند. تشریح در کاربردهای تحلیل رمزنگاری، موازنه[۱۷] زمان-حافظه مطرح در حملات تلاقی در میان روی طرح‌های رمزکردن چندگانه با بیش از سه دور را بهبود چشمگیری می‌دهد.

تفاوت اصلی بین این دو نوع حمله کم‌داده را می‌توان چنین بیان کرد: در حمله تلاقی در میان حالت ابتدایی، دشمن از متن‌های واضح و متن‌های رمزشده معلوم در نقاط انتهایی[۱۸] آغاز می‌کند، و با پیشروی از دو نقطه انتهایی تا میانه، سعی در حدس تعدادی از زیرکلیدها و ساخت جدول جستجو[۱۹] مناسب دارد. تساوی مقادیر زوج‌ها در میانه سیستم رمز به عنوان یک شرط صافی[۲۰] برای تشخیص کلیدهای درست است، و نیازی به دانستن آن‌ها برای شروع حمله نیست. در حمله‌های تشریح، دشمن کار را با حدس‌زدن درباره مقادیر مرتبط در میانه آغاز می‌کند و از میانه تا دو نقطه انتهایی پیش می‌رود.

---

[16] Transition

[17] Trade-Off

[18] End Points

[19] Lookup Table

[20] Filtering Condition

در واقع، دانستن مقادیر میانی، این امکان را به مهاجم می‌دهد تا مسئله تحلیل سیستم رمز را به دو مسئله مستقل کوچک‌تر بشکند که در آن‌ها، زوج‌های متن واضح و متن رمزشده معلوم جدیدی در نقاط انتهایی هر یک مشخص است که می‌توان مسئله را به کمک تکنیک تشریح دیگری، به صورت بازگشتی حل کرد و یا این‌که در برگ‌های درخت بازگشتی از روش تلاقی در میان برای حل بهره برد.

مزایا و معایب این دو روش را در ساختارهای با تعداد فرد، یعنی $l = 2r+1$ می‌توان این‌گونه توضیح داد: حمله تلاقی در میان می‌تواند دور میانه را با مقایسه‌ی فقط نیم‌قطعه‌های $n/2$-بیتی توسط این دور در ساختار فایستل متأثر نشده است، در نظر نگیرد. از آن‌جا که نیازی به حدس‌زدن زیرکلید دور میانه نیست، پس باعث می‌شود که حمله تلاقی در میان از نظر زمان، در ساختارهای فایستل کاراتر باشد. البته طبیعتاً تکنیک تشریح کاراتر از تلاقی در میان است، اما به خاطر آن‌که باید همه مقدار n-بیتی میانه را حدس بزند تا بتواند از این مقدار حدس‌زده‌شده در رمز و ترجمه استفاده کند، از نظر زمانی کارایی کم‌تری خواهد داشت.

می‌توان ترکیبی از روش تلاقی در میان و تشریح با افزودن تکنیک‌های دیگر مثل تکرار پیمایش روی مقادیری که بعدها در تلاقی در میان استفاده نمی‌شوند، و استفاده از برخورد[21]های چندگانه و ویژگی‌های تفاضلی در میانه ساختار فایستل را به کار برد.

با تعداد دور فرد شروع می‌کنیم. می‌توانیم پیچیدگی حافظه‌ای بیشتر حملاتِ از نظر زمانی کارا را کاهش دهیم. نشان داده می‌شود که پیچیدگی حافظه‌ای حمله تلاقی در میان روی ساختار با $l=2r+1$ دوری، به ازای r بزرگتر مساوی سه، بدون افزایش پیچیدگی زمانی، از $2^{0.5rn}$ به $2^{\left\lceil \frac{r}{2} \right\rceil 0.5n}$ کاهش می‌یابد، به شرط آن‌که پیچیدگی داده‌ای به حدود $2^{\left\lceil \frac{r-3}{r+1} \right\rceil 0.5n}$ متن واضح معلوم برسد. اگر متن‌های واضح اضافی مجاز نباشد، باز هم می‌توان کاهش حافظه داشت، اما فقط تا حدود $2^{\left\lceil \frac{2r}{3} \right\rceil 0.5n}$. به طور خاص، پیچیدگی حافظه‌ای حمله تلاقی در میان استاندارد روی فایستل هفت دوری، بدون تغییر در پیچیدگی داده‌ای، از $2^{1.5n}$ به 2^n کاهش می‌یابد.

[21] Collision

هدف دیگر، کاهش پیچیدگی زمانی بیشتر حملات غیربدیهی حافظه‌ای کارا است؛ که در آن‌ها دشمن تنها به $2^{0.5n}$ محدود شده است، یعنی تنها می‌تواند همه مقادیر یک نیم‌قطعه یا یک زیرکلید را ذخیره کند. البته در این‌جا نیز روش مطرح شده در مقاله، کاراتر بوده است.

برای تعداد دور زوج، بدون حدس‌زدن کلید اضافی، می‌توان از همین الگوریتم استفاده کرده و یک دور به ساختار فایستل اضافه کنیم که منوط به افزایش پیچیدگی زمانی به $2^{0.25n}$ و استفاده از $2^{0.25n}$ متن واضح منتخب است.

با توجه به این‌که تکنیک‌های گفته‌شده در مقاله [۱]، کلی بوده و درباره حالت خاص نیست، پس می‌توان بهترین حمله شناخته‌شده روی سیستم‌های رمز موجود را به طرز قابل توجهی بهبود داد.

به این ترتیب به بیان مختصری از انواع تکنیک‌های مورد استفاده در انواع پیشرفته‌تر حملات تلاقی در میان اشاره شد. در فصل بعدی، به بیان مسائل باز این حوزه و پروژه کارشناسی ارشد خواهیم پرداخت.

فصل پنجم

جمع‌بندی، مسائل باز و پروژه کارشناسی ارشد

۱.۵ جمع‌بندی

در این گزارش، به مروری بر ساختارهای فایستل پرداخته شد. بعد از آن، انواع و ویژگی‌های آن‌ها بیان شد که در حملات مختلف درباره آن‌ها بحث می‌شود. پس از آن، به حملات عام بر روی این ساختارها پرداختیم. در ادامه، پس از ذکر انواع حملات مطرح، حمله تلاقی در میان به عنوان یکی از حملات رایج در سال‌های اخیر بر روی سیستم‌های رمز شرح داده شد که با معرفی تکنیک‌های مختلف بهبود این حمله، نشان داده شد که امکان بهبود پیچیدگی زمانی، حافظه‌ای و داده‌ای این حمله وجود دارد. می‌توان با تلفیق روش‌های مختلف مطرح‌شده و ایده‌های دیگر، به میزان پیچیدگی حداقلی مورد نظر برای یک حمله تلاقی در میان کارا دست یافت.

۲.۵ مسائل باز

یکی از مسائل باز مطرح‌شده در این گزارش، تعداد دور بهینه برای یک طرح فایستل بود. به این معنا که با توجه به ویژگی‌های طرح فایستل، یک طراح سیستم رمز چگونه می‌تواند به یک موازنه‌ای از امنیت و سرعت مطلوب برای الگوریتم رمز خود برسد. اینکه یک سیستم رمز باید دارای چه تعداد دوری از طرح فایستل باشد که نه امنیت آن به مخاطره بیافتد و نه سرعت و کارایی آن کاهش یابد، از مسائل باز این حوزه است.

مسئله باز دیگری که درباره حمله تلاقی در میان قابل طرح است، نحوه ترکیب تکنیک‌های مختلف و ایده‌های دیگر در حمله تلاقی در میان است، به نحوی که باعث بهبود پیچیدگی‌های زمانی و حافظه‌ای شود و از طرف دیگر، مفروضات روش‌های مختلف را تا حد امکان کاهش داده و حمله را کلی کند.

این‌که چگونه می‌توان این حملات و تکنیک‌ها را بر روی یک سیستم رمز کاربردی اعمال کرد، به نحوی که تعداد دورهای بیشتری از سیستم رمز مورد نظر تحلیل شود، پرسش دیگری است که نیاز به مطالعه و دانش بالایی در حوزه ساختارهای سیستم‌های رمز کاربردی دارد.

همان‌طور که قبلا نیز اشاره شد، کاربرد حمله تلاقی در میان صرفا در طرح‌های مبتنی بر فایستل نیست و می‌توان از این حمله، برای طرح‌های غیرفایستلی نیز بهره بود. گرچه تحقیقاتی در این باره انجام شده است، اما به دلیل گستردگی طرح‌های غیرفایستلی، می‌توان این پرسش را به عنوان محور پژوهشی دیگری در این حوزه دانست.

۳.۵ پروژه کارشناسی ارشد

پروژه کارشناسی ارشد پیشنهادی در این گزارش، با استفاده از مسائل باز مطرح‌شده در بخش قبلی به دست آمده است. به این ترتیب که، حمله تلاقی در میان برای یک سیستم رمز کاربردی، با رویکرد بهبود پیچیدگی زمانی و حافظه‌ای انجام شود. لازمه انجام این پروژه مطالعه روی انواع تکنیک‌ها و گونه‌های حمله تلاقی در میان است که بخشی از آن در این گزارش به طور اجمالی ذکر شد. انتخاب سیستم رمز کاربردی و واقعی مناسب دیگر چالش این پروژه خواهد بود. باید از بین سیستم‌های رمز فراوانی که وجود دارد، یک سیستم رمز یا دسته‌ای از سیستم‌های رمز انتخاب شود و مطالعه دقیق‌تر درباره ویژگی‌های آن‌ها صورت پذیرد. تعیین تعداد دور برای تحلیل، پارامتر دیگری است که باید به آن توجه ویژه داشت. از آن‌جا که هر یک از روش‌های موجود دارای نقاط قوت و ضعف مخصوص به خود هستند، باید تعداد دورهای مورد نظر برای تحلیل، مشخص شده باشد. در ادامه، با تلفیق تکنیک‌ها و ایده‌های مختلف، پژوهشگر می‌تواند با توجه به پیچیدگی زمانی و حافظه‌ای حمله، به یک راهکار تحلیل سیستم رمز تعیین‌شده دست پیدا کند. در نظر گرفتن حداقل مفروضات روش‌ها و کلی‌سازی حمله برای سیستم‌های دیگر نیز می‌تواند به عنوان بخش‌های دیگر پروژه مطرح شود.

منابع و مراجع

[۱] I. Dinur, O. Dunkelman, N. Keller and A. Shamir, “New Attacks on Feistel Structures with Improved Memory Complexities ", Advances in Cryptology, CRYPTO 2015, 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I, pp. 433-454.

[۲] J. Guo, J. Jean, I. Nikolic and Y. Sasaki, “Meet-in-the-Middle Attacks on Generic Feistel Constructions”, Advances in Cryptology, ASIACRYPT 2014, 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I, pp. 458-477.

[۳] T. Isobe and K. Shibutani, “All Subkeys Recovery Attack on Block Ciphers: Extending Meet-in-the-Middle Approach”, Selected Areas in Cryptography, 19th International Conference, SAC 2012, Windsor, ON, Canada, August 15-16, 2012, Revised Selected Papers, pp. 202-221.

[۴] A. Canteaut, M.Naya-Plasencia and B. Vayssiere, “Sieve-in-the-Middle: Improved MITM Attacks,” Advances in Cryptology, CRYPTO 2013, 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I, pp. 222-240.

[۵] J. Patarin, “Generic Attacks on Feistel Schemes”, Advances in Cryptology, ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, Australia, December 9–13, 2001 Proceedings, pp. 222-238.

[۶] A. Bogdanov and C. Rechberger, “A 3-Subset Meet-in-the-Middle Attack: Cryptanalysis of the Lightweight Block Cipher KTANTAN”, Selected Areas in Cryptography, 17th International Workshop, SAC 2010, Waterloo, Ontario, Canada, August 12-13, 2010, Revised Selected Papers, pp. 229-240.

[۷] H. Feistel, W. A. Notz and J. L. Smith, “Some cryptographic techniques for machine-to-machine data communications", Proceedings of the IEEE , Volume:63 , Issue: 11, 1975, pp. 1545-1554.

[۸] T. Isobe and K. Shibutani, “Generic Key Recovery Attack on Feistel Scheme”, Advances in Cryptology, ASIACRYPT 2013, 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I, pp. 464-485.

[۹] A. Bogodanov, D. Khovratovich and C. Rechberger, “Biclique Cryptanalysis of the Full AES”, Advances in Cryptology, ASIACRYPT 2011, 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings, pp. 344-371.

[۱۰] W. Diffie and M. E. Hellman “Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard”, Journal Computer IEEE Computer Society Press Los Alamitos, CA, USA, Volume 10, Issue 6, June 1977, pp. 74-84.