

بررسی اثر نويز در حملات عليه سيستم‌های رمز دنباله‌ای

وحید نحوی
شرکت مهندسی پیام پرداز
nahvi@payampardaz.net

محمد دخیل علیان
دانشگاه صنعتی اصفهان
mdalian@cc.iut.ac.ir

سید مهدی سجادیه
دانشگاه صنعتی اصفهان
sadjadieh@ec.iut.ac.ir

چکیده: به دلیل عبور سیگنال‌های مخابراتی از کانال‌های مختلف و تضعیف آن ممکن است تعدادی از بیت‌های سیگنال ارسالی اشتباه دریافت شود. با توجه به اینکه در حمله متن اصلی معلوم علیه سیستم‌های رمز دنباله‌ای متن اصلی بدون اثر نويز در دسترس است تعدادی از بیت‌های کلید اجرایی تغییر پیدا می‌کند و دنباله کلید اجرایی به دست آمده همانند دنباله خروجی مولد شبه تصادفی نیست. در این مقاله اثر تغییر بیت‌های کلید اجرایی (اثر نويز) در حملات مهم علیه سیستم‌های رمز دنباله‌ای مانند حمله جبری، معاوضه زمان حافظه و همبستگی بررسی شود. در انتها نیز یک ویژگی مهم حمله معاوضه زمان حافظه در حمله به متن رمز شده بیان می‌گردد که می‌توان از آن به عنوان حمله متن رمز شده در بسیاری از کاربردها استفاده نمود.

واژه‌های کلیدی: رمز دنباله‌ای، حمله عام، نويز حمله معاوضه زمان-حافظه، حمله همبستگی، حمله جبری، حمله متن رمز شده

مواقع مناسب بوده و کاربرد آنها در برخی موارد اجتناب‌ناپذیر می‌باشد (مانند مخابرات راه دور که حافظه موقت محدودی در دسترس است یا در جاهایی که لازم است در هر زمان که کاراکترها دریافت می‌شوند به طور تک به تک روی آنها پردازش صورت گیرد). از آنجا که این رمزکننده‌ها دارای عدم انتشار خطا و یا انتشار خطای کمی هستند، در موقعیت‌هایی که احتمال خطاهای انتقال بالاست بسیار مفیدتر از رمزکننده‌های قالبی می‌باشند.

۱- مقدمه

رمزکننده‌های دنباله‌ای^۱ یک دسته از الگوریتم‌های رمزگذاری متقارن می‌باشند که از نظر سخت‌افزاری سریع‌تر از رمزکننده‌های قالبی^۲ هستند و پیچیدگی سخت‌افزاری کمتری دارند. این رمزکننده‌ها در بسیاری از

¹Stream Ciphers
²Block Ciphers

در بخش ۴ اثر نويز در حملات معرفی شده در بخش ۲ بررسی می‌شود و در بخش ۵ حمله معاوضه زمان-حافظه در حمله متن رمز شده بررسی می‌شود و در نهایت به نتیجه‌گیری از مقاله پرداخته خواهد شد.

۲- حملات مهم علیه سیستم‌های رمز دنباله‌ای

همزمان با روند تکاملی مولدهای رمز دنباله‌ای، روش‌های تحلیل این نوع مولدها نیز رشد یافته است. در این روش‌ها، با توجه به نوع مولد و خصوصیات آن، ایده‌های مختلفی جهت تحلیل آنها ابداع و ارایه شده است. یکی از معیارهای طراحی مولدهای رمز، مقاومت در برابر حملات می‌باشد. بنابراین در کاربردهای عملی و طراحی ساختار مطلوب، این معیار باید مورد توجه قرار گیرد. بسیاری از تحلیل‌های رمز صورت گرفته بر روی رمزکننده‌های دنباله‌ای از نوع حملات متن اصلی معلوم می‌باشند.

در بسیاری از حملات تلاش می‌شود که از روی دنباله کلید اجرایی به کلید مخفی دست پیدا کنیم. در حملات برای به دست آوردن کلید اجرایی فرض می‌شود متن اصلی معلوم است و در نتیجه با دریافت متن رمز شده و دریافت آن و XOR کردن دنباله رمز شده با متن اصلی کلید اجرایی متناظر به دست می‌آید.

حملات علیه سیستم‌های رمز دنباله‌ای شامل حملات عمومی که به همه رمزکننده‌های دنباله‌ای همزمان قابل اعمال هستند و حملاتی که علیه رمزکننده دنباله‌ای خاصی به کار برده می‌شوند، می‌باشند. یکی از مهم‌ترین انواع حملات عمومی علیه رمزکننده‌های دنباله‌ای، حمله همبستگی^۳ می‌باشد [۲ و ۳]. این حمله در ابتدا برای اعمال به مولدهای ترکیب غیر خطی به کار گرفته شده است، اما چون می‌توان یک مولد فیلتر غیرخطی را نیز به صورت مولد ترکیب غیرخطی معادل‌سازی نمود، حمله همبستگی به این ساختارها نیز قابل اعمال است. در صورتی که بین

در این رمزکننده‌ها ابتدا یک دنباله شبه تصادفی برابر طول متن اصلی و وابسته به کلید تولید شده، سپس دنباله حاصل با متن اصلی ترکیب می‌شود. به عبارت دیگر این رمزکننده‌ها با استفاده از یک تبدیل رمز متغیر با زمان، متن اصلی را به متن رمز شده تبدیل می‌نمایند. ابتدا با تعریف رمزکننده‌های دنباله‌ای بحث را شروع می‌کنیم. فرض کنید M ، مجموعه نمادهای ممکن برای متن اصلی، C مجموعه نمادهای ممکن برای متن رمز شده، Z مجموعه نمادهای ممکن برای دنباله کلید اجرایی و K مجموعه نمادهای ممکن برای کلید رمز باشد. همچنین دنباله $\tilde{m} = m_1, m_2, \dots$ دنباله متن اصلی است که می‌خواهیم به صورت رمز شده $\tilde{C} = c_1, c_2, \dots$ درآید. رمزکننده شامل یک مولد کلید اجرایی است که یک دنباله شبه تصادفی $Z_i \in Z, i \geq 1$ ، به نام دنباله کلید اجرایی تولید می‌کند. در بسیاری از سیستم‌های رمز دنباله‌ای (که به آن سیستم‌های رمز دنباله‌ای همزمان گفته می‌شود) مطابق رابطه (۱)، Z_i تابعی از کلید $k \in K$ می‌باشد [۱].

$$Z_i = f_i(k) \quad (1)$$

دنباله کلید اجرایی با استفاده از یک تابع رمز e ، دنباله پیام \tilde{m} را نماد به نماد رمز می‌کند تا دنباله متن رمز شده \tilde{c} به وجود آید. در بسیاری از سیستم‌های رمز دنباله‌ای برای تولید متن رمز شده از XOR متن اصلی و کلید اجرایی استفاده می‌شود.

همان‌طور که اشاره شد رمزکننده‌های دنباله‌ای دارای انتشار خطای کمی هستند ولی در حین حمله در صورت عدم اطلاع از وجود نويز ممکن است مشکلاتی به وجود آید. در این مقاله سعی بر آن است تأثیر نويز در حملات به طور کامل مورد بررسی قرارگیرد و به همین دلیل در بخش ۲ ابتدا حملات همبستگی، معاوضه زمان-حافظه و جبری علیه سیستم‌های رمز دنباله‌ای معرفی گردیده و سپس در بخش ۳ اثر نويز در حملات عام مورد بررسی قرار می‌گیرد.

³Correlation Attack

حمله جبری نیز یکی دیگر از حملات علیه سیستم‌های رمز دنباله‌ای است. در این حمله ابتدا دستگاه معادلاتی غیر خطی بر حسب کلید اصلی و کلید اجرایی تشکیل می‌شود و سپس با ساده کردن حل دستگاه معادلات غیر خطی حمله کامل می‌شود. باید توجه داشت در تمام روش‌های حل معادلات غیر خطی تعداد معادلات بسیار بیشتر از تعداد مجهولات است. مهمترین پارامتر در حمله جبری علیه سیستم‌های رمز دنباله‌ای بدون حافظه، مرتبه تابع چندجمله‌ای مورد استفاده در سیستم است [۶].

۳- انواع نويز و تأثیرات آن در حملات عام

در هنگام حملات متن اصلی معلوم علیه سیستم‌های رمز دنباله‌ای، فرض بر آن است متن اصلی و متن رمز شده معلوم است و از XOR کردن این دو متن کلید اجرایی به دست می‌آید. در صورت وجود نويز در کانال‌های مخابراتی، ممکن است در متن رمز شده تغییراتی به وجود آید. با توجه به اینکه فرض می‌شود متن اصلی بدون نويز موجود است هر بیتی که از متن رمز شده در کانال تغییر پیدا می‌کند، کلید اجرایی متناظر آن نیز اشتباه آشکار سازی می‌شود و در نتیجه دنباله حاصل از XOR کردن دو متن دنباله کلید اجرایی صحیح نیست.

در حالت کلی خطاهای ناشی از نويز به دو دسته تقسیم می‌شود. اولین دسته خطاهای ممکن، خطاهایی هستند که تعداد خطاها به طور آماری مشخص است ولی مکان آنها معلوم نیست که به این خطاها، خطای با محل نامعین می‌گوییم. برای مثال اگر در یک متن به طول l ، e خطا وجود داشته باشد برای دنباله کلید اجرایی آن $\binom{l}{e}$ کاندید وجود دارد. در حالت دوم مکان خطا مشخص است ولی مقدار آن خطا مشخص نیست که به این خطاها خطای با محل معین^۶ می‌گوییم. در این حالت اگر در یک

خروجی i امین $LFSR$ ، و خروجی مولد رمز، یک همبستگی وجود داشته باشد یعنی اگر داشته باشیم $P(u_j^{(i)} = z_j) \neq 0.5$ ، حمله همبستگی بدون نیاز به ساختار دیگر $LFSR$ ها، می‌تواند به آشکارسازی حالت اولیه $LFSR$ مورد نظر منجر شود. به دنبال حملات همبستگی، الگوریتم‌های دیگری برای سرعت بخشیدن به آنها پیشنهاد شده است که به حملات همبستگی سریع معروف می‌باشند [۲] و با استفاده از مفاهیم کدینگ کانال صورت می‌گیرند. یکی دیگر از مشتقات حملات همبستگی حمله خطی است. این حمله علیه سیستم‌های حافظه‌دار کاربرد دارد [۴].

حمله مهم دیگر، حمله معاوضه زمان-حافظه است که برای سیستم‌های رمز دنباله‌ای که از ماشین حالت محدود استفاده می‌نمایند قابل اجراست [۵]. این حمله روشی برای بهبود حمله جستجوی کامل می‌باشد که از تناقض روز تولد استفاده می‌نماید. در این حمله در مرحله پیش پردازش M حالت تصادفی N بیتی در نظر گرفته می‌شود (کلید اصلی N بیتی است) که به ازای هر کدام N بیت کلید اجرایی تولید و ذخیره می‌شود و در نهایت جدول بر اساس خروجی‌ها مرتب می‌شود. در مرحله زمان واقعی^۵ D بیت کلید اجرایی در دسترس است. در این صورت ابتدا $D-N+1$ دنباله کلید اجرایی N بیتی متوالی (با تداخل) دسته‌بندی می‌شود. حال $D-N+1$ دنباله کلید اجرایی N بیتی متوالی با هر کدام از M حالت مقایسه می‌شود و در صورت برخورد با توجه به خواص $LFSR$ می‌توان به کلید اصلی دست یافت. برای اینکه احتمال برخورد بیش از 0.5 باشد طبق تناقض روز تولد باید $M(D-N+1) > 2^N$ برقرار باشد (در حالت حدی $M(D-N+1) = 2^N$). باید توجه داشت در بسیاری از حالات عملی $D \approx (D-N+1)$ است که رابطه فوق به $M D = 2^N$ تبدیل می‌شود.

⁴ Time-Memory Tradeoff

⁵ Real Time

⁶ erasure error

تأثیر نویز باید تمام بیت‌ها در یک فریم N بیتی صحیح باشد که احتمال آن برابر است با:

$$B = \left(1 - \frac{e}{I}\right)^N \quad (2)$$

به ازای $N=64$ و مقادیر $\frac{e}{I} = 0.01$ و $\frac{e}{I} = 0.001$ مقادیر B به ترتیب $0/52$ و $0/937$ به دست می‌آیند که B در احتمال موفقیت حمله ضرب می‌شود. با توجه به رابطه (۲)، اگر $\frac{e}{I}$ مقدار کوچکی باشد و N نیز عدد بزرگی نباشد (حداکثر ۱۲۸) نویز تأثیر شگرفی در این حمله نخواهد گذاشت.

حمله دیگری که در این مقاله به آن می‌پردازیم حمله همبستگی است که قبلاً نیز به نوعی بیان شده است [۲]. فرض کنید یک رابطه با احتمال P صحیح باشد ($P > 0.5$). در صورت وجود خطای با احتمال $\frac{e}{I}$ مقدار P' به صورت زیر تصحیح می‌شود:

$$\frac{1}{2} < P' = \frac{I-e}{I}P + \frac{e}{I}(1-P) < P \quad (3)$$

در این صورت باید پارامترهای حمله بر اساس P' تنظیم شود. اگر $\frac{e}{I} < 0.001$ باشد و با توجه به $P < 1$ می‌توان گفت که نویز در این حمله تأثیر چندانی ندارد زیرا:

$$\frac{I-e}{I}P + \frac{e}{I}(1-P) > 0.998P + 0.001 \approx P \quad (4)$$

در انتهای حملات به بررسی حمله جبری می‌پردازیم. فرض کنید برای حمله به دنباله‌ای از کلید اجرایی با طول I نیاز داریم. اگر هر کدام از بیت‌های کلید اجرایی تغییر یابد پس از تشکیل دستگاه معادلات، جواب نادرستی به ما خواهد داد و در نتیجه حمله به کلید اشتباه منجر می‌شود. بر این اساس اثر نویز در این حمله همانند حملات عام است و پیچیدگی این حمله با وجود نویز برابر می‌شود. $\left(\frac{I}{e}\right)$

متن به طول I با e خطای با محل معین وجود داشته باشد برای دنباله کلید اجرایی آن 2^e کاندید وجود دارد [۷]. بنابراین راه‌حلی که می‌توان برای تمام حملات در نظر گرفت آن است که به ازای هر کاندید دنباله کلید اجرایی یک کلید محاسبه کنیم و سپس با امتحان تمام کلیدهای حاصل شده، کلید اصلی را به دست آوریم. حال فرض کنید برای شکستن یک سیستم رمز دنباله‌ای با N بیت از کلید اجرایی به A عملیات در زمان واقعی نیاز داریم. در صورت داشتن خطای با محل نامعین برای یک دنباله زمان لازم برای شکستن سیستم برابر $\left(\frac{I}{e}\right)^A$ خواهد بود. برای مثال اگر $I=1000$ و $e=5$ باشد این مقدار برابر $A \times 10^{12} \times 1/8$ است. در صورت خطای با محل معین مقدار این خطا $A \times 2^e$ است که به ازای مقادیر قبلی برابر $32A$ است [۷]. این مقادیر نشان می‌دهد که با فرض‌های فوق وجود نویز، پیچیدگی حملات را بسیار افزایش می‌دهد.

۴- اثر نویز در حملات معاوضه زمان-حافظه،

همبستگی، جبری

پیچیدگی بیان شده در قسمت قبل بدترین شرایط را در نظر گرفت، به این معنا که اگر حتی یک بیت از دنباله کلید اجرایی خراب شود، باید تمام حالات ممکن برای کلید اجرایی بررسی شود. اما در بسیاری حملات قسمتی از کلید اجرایی مورد استفاده قرار می‌گیرد یا معادلات به صورت احتمالی بیان می‌شوند. به همین دلیل می‌توان با شرایط خاص پیچیدگی حملات مخلوط شده با نویز را کم نمود. اولین حمله‌ای که مورد نظر است حمله زمان-حافظه است. همان طور که اشاره شد در حمله معاوضه زمان-حافظه، N بیت از کلید اجرایی با حافظه مقایسه می‌شود و در صورت تطابق، با انجام مراحل کلید اصلی به دست می‌آید. بنابراین با توجه به این حمله اگر خطایی در بیت‌هایی که در غیر از محل تطابق هستند اتفاق افتد به این حمله آسیبی نمی‌رسد. در این صورت برای عدم

۵- حمله متن رمز شده با ساختاری خاص

در برخی از حملات متن رمز شده، فقط ابهامی در بین چند متن به عنوان متن اصلی وجود دارد. فرض کنید که می توان متن اصلی را به چند قسمت تقسیم نمود به طوری که می دانیم هر قسمت متعلق به مجموعه D_1 تا D_b ($m_i \in \{D_1, D_2, \dots, D_b\}$) است. برای مثال فرض کنید می توان متن اصلی را به 2^{16} متن های ۱۰۲۴ بیتی تبدیل نمود به طوری که برای هر کدام از این متن ها (m_i) ۲۵۶ حالت و چو داشته باشد. فرض کنید متن اصلی و کلید اجرایی و متن رمز شده متناظر به صورت $m_i \in \{D_1, D_2, \dots, D_b\}$ و $\tilde{m} = \{m_1 \| m_2 \| \dots \| m_a\}$ $\tilde{C} = \{C_1 \| C_2 \| \dots \| C_a\}$ و $\tilde{Z} = \{z_1 \| z_2 \| \dots \| z_a\}$ نمایش داده شود. با توجه به مقادیر a و b تعداد حالات ممکن برای نمایش \tilde{m} برابر a^b است که در نتیجه در حالت کلی اگر در حمله ای با داشتن \tilde{m} و \tilde{C} به A عملیات نیاز داشته باشد (حمله متن اصلی معلوم) برای پیدا کردن کلید در حالتی که فقط C در دسترس است به Aa^b عملیات نیاز دارد.

حال به بررسی حملات بیان شده در بخش قبل می پردازیم. حمله جبری همانند حمله عام است. در حمله همبستگی نیز اگر فرض کنیم m_i ها به طور یکنواخت در متن توزیع شده اند آنگاه برای پیدا کردن احتمال مناسب به حداقل b برابر متن های اصلی در حمله متن اصلی معلوم، نیاز داریم.

شاید مهمترین حمله در این راستا حمله معاوضه زمان-حافظه است. فرض کنید طول m_i به اندازه کافی بزرگ است که احتمال قرار گرفتن تطابق بین کلید اجرایی و مقادیر پیش پردازش شده دو متن متوالی m_i و m_{i+1} بسیار کم است که در نتیجه تطابق با احتمال بسیار زیادی در یکی از Z_i ها خواهد افتاد و احتمال وقوع انطباق بین Z_i و Z_{i+1} بسیار کم است (هر Z_i متناظر با یک m_i است). فرض کنید در بلوک Z تطابقی رخ دهد. در این صورت

فرض معلوم بودن C_j در رابطه $Z_j = m_j \oplus C_j$ و اینکه می دانیم $m_j \in \{D_1, D_2, \dots, D_b\}$ است می توان به جای به جای m_j همه مقادیر D_1 تا D_b را جایگزین کرد تا سرانجام در یکی از این موارد، Z_j را به دست آورد. تنها مشکلی که باقی می ماند آن است که مکان j ام نیز مجهول است.

اگر متن رمز شده متناظر $C = \{C_1 \| C_2 \| \dots \| C_a\}$ را هر بار با یک $\tilde{m}_i = \{D_i \| D_i \| \dots \| D_i\}$ ($1 < i < b$) XOR نموده و کلید اجرایی متناظر با آن را به دست می آوریم ($\tilde{m}_i \oplus C = \tilde{Z}_i$)، الزاماً یک برخورد متناظر با Z_j وجود دارد لذا یکی از کلیدهای به دست آمده کلید اصلی است که می توان آن را با آزمایش کردن کلیه کلیدهای به دست آمده به دست آورد.

با توجه به اینکه i می تواند بین 1 تا b تغییر کند، در حمله زمان حافظه مقدار عملیات فقط b برابر می شود. دقت کنید در حملات عام با مقادیر ابتدایی این بخش هزینه حمله A 2^{56} خواهد شد در صورتی که با حمله زمان-حافظه این مقدار فقط A ۲۵۶ خواهد شد. دقت کند طول m_i (که در مثال ۱۰۲۴ است) در حمله هیچ تأثیری ندارد.

۶- نتیجه گیری

در این مقاله ابتدا حملات مهم علیه سیستم های دنباله ای بیان شد و سپس بررسی اثر نویز پرداخته شد. همان طور که مشاهده شد اگر حملات را به طور عام مورد بررسی قرار دهیم نویز باعث عدم موفقیت حملات خواهد شد ولی در بعضی از حملات مانند همبستگی و معاوضه زمان-حافظه در صورت ناچیز بودن احتمال نویز می توان تدابیری اندیشید که نویز تأثیری نداشته باشد. حالت دیگری که مورد بررسی قرار گرفت حمله در حالتی بود که متن اصلی در اختیار ما نیست ولی الگوهایی از آن موجود است. نشان داده شد با شرایط خاصی حمله معاوضه زمان-حافظه بهترین تأثیر را در این حمله دارد.



Vol.LNCS 1008, pp154-169.

[5] Biryukov A., Shamir A., "Cryptanalysis time/memory/data tradeoffs for stream ciphers", In Advances in Cryptology-ASIACRYPT 2000, Vol. LNCS 1976, pp. 1-13, 2000.

[۶] سید مهدی سجادیه، حمله جبری علیه سیستم‌های

رمز دنباله‌ای دانشگاه صنعتی اصفهان، پایان‌نامه کارشناسی

ارشد برق-مخابرات، فروردین ۱۳۸۵.

[7] Barkan E., , Ph.D Thesis , Cryptanalysis of Ciphers and Protocols, Technion- Israel 2006.

مراجع

[۱] سید محمود مدرس هاشمی، طراحی رمزکننده‌های پی‌درپی، دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی اصفهان، پایان‌نامه کارشناسی ارشد برق-مخابرات، اسفند ۱۳۷۰.

[2]Sertkaya I., Nonlinearity Preserving Post-Transformations, PhD Thesis ,The Middle East Technical University, June 2004.

[3] Chepizhov V.,Smeets E.,"On a fast correlation attack certain stream ciphers" , Proceeding of Eurocrypt 1991,Vol. LNCS 547 , pp. 176-185.

[4]Golic D., "Linear cryptanalysis of stream ciphers", Fast Software Encryption 1994,