مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"
سال چهارم، شماره ۱، بهار ۱۳۹۵، ص ۸۹- ۸۱

تحلیل رفتاری زنجیره‌های رمز هلمن مبتنی بر گراف توابع تصادفی

ناصر حسین غروی*[۱]، عبدالرسول میرقدری[۲]، محمد عبداللهی ازگمی[۳]، حسین سلطانی[۴]

۱- دانشجوی دکتری، دانشگاه جامع امام حسین(ع)
۲- دانشیار، دانشگاه جامع امام حسین(ع)
۳- دانشیار، دانشگاه علم و صنعت ایران
۴- دانشجوی دکتری، پژوهشگاه مخابرات و الکترونیک نصر

(دریافت: ۹۴/۰۸/۳۰، پذیرش: ۹۵/۰۲/۱۴)

چکیده

علی‌رغم تحقیقات متعدد و تلاش‌های به‌عمل‌آمده در خصوص تحلیل الگوریتم‌های رمزنگاری با روش مصالحه زمان و حافظه، سطح پوشش جداول هلمن و روش‌های مشابه در عمل کمتر از نصف بوده و احتمال موفقیت آنها به همین میزان و یا کمتر است. زنجیره‌های رمز هلمن در واقع مسیرهایی با رئوس آغازین و پایانی معین روی نمودار گراف تابع هستند. در این مقاله به تحلیل رفتار این زنجیره‌ها از دیدگاه گراف توابع تصادفی پرداخته شده است. در ابتدای مقاله پارامترهای گراف توابع تصادفی تعریف و سپس رفتار زنجیره‌های هلمن بر اساس این پارامترها تحلیل می‌شود. نتیجه تحلیل نشان می‌دهد که به دلایلی مانند وجود درصدی قابل توجه (حدود ۳۷٪) از رئوس پایانه‌ای و عدم امکان رخداد آنها روی زنجیره‌ها (مگر در رئوس آغازین)، وجود پارامترهای مناسبی همانند تعداد مؤلفه‌ها و طول مسیرهای بدون تکرار برای ساخت زنجیره‌ها، عدم توجه به احتمال ساخت یک زنجیره غیردوری برحسب پارامتر طول زنجیره و عدم توجه به احتمال برای ادغام زنجیره‌ها برحسب پارامترهای طول و تعداد آنها، سطح پوشش چنین جداولی نمی‌تواند در حد انتظار باشد. لذا عوامل مذکور باعث می‌شوند که سطح پوشش یک جدول هلمن از نقطه‌ای به بعد به سرعت کاهش یافته و در عمل ساخت آنها بی‌اثر باشد. این روش به طور عملی روی الگوریتم رمز mAES پیاده شده که نتایج آن تاییدکننده نتایج تحقیق می‌باشد.

واژه‌های کلیدی: حملات مصالحه‌ای، زنجیره‌های هلمن، جداول رنگین کمانی، گراف توابع تصادفی، رئوس پایانه‌ای، حالت پنهان.

۱- مقدمه

در بحث تحلیل رمز، حمله ایجاد مصالحه بین زمان و حافظه، در حقیقت برقراری توازن بین حمله جستجوی جامع و حمله لعت‌نامه‌ای است. ایده‌ی ساخت زنجیره‌های رمز، به منظور ایجاد مصالحه بین حافظه و زمان، به عنوان روشی برای معکوس کردن توابع یک‌طرفه (مانند توابع رمزنگاری)، اولین بار در سال ۱۹۸۰ توسط هلمن[۱] ارائه شد [۱] و تا زمان حاضر تحقیقات زیادی روی بهبود این حمله (به لحاظ حافظه و سرعت) به عمل آمده و ادامه دارد. این ایده با نام حمله TMTO[۲] هلمن به‌منظور شکست الگوریتم‌های رمز شناخته می‌شود. ویژگی‌های مهم حمله هلمن که موجب محبوبیت آن تاکنون شده است در عملی بودن آن (حداقل روی طیف وسیعی از الگوریتم‌های موجود) و عدم نیاز به ساختار داخلی تابع مورد حمله (الگوریتم رمز) نهفته است. حمله هلمن، در واقع یک حمله جعبه سیاه است. این حمله، به‌طور خلاصه از دو مرحله تشکیل شده است. مرحله اول که فقط یک‌بار انجام می‌شود، مرحله پیش پردازش یا برون‌خط نام دارد. در این فاز هر زنجیره با شروع از یک نقطه تصادفی مانند x و با t بار اعمال متوالی تابع یک‌طرفه مفروض f به‌صورت $f(x), f^2(x), f^3(x), \dots, f^t(x)$ ساخته می‌شود و در نهایت فقط نقاط ابتدائی (x) و انتهایی هر زنجیره $(f^t(x))$ ذخیره می‌شوند. در یک جدول هلمن، به همین روش با شروع از m نقطه تصادفی غیرتکراری، به تعداد m زنجیره ساخته شده و فقط نقاط ابتدایی و انتهایی آنها ذخیره می‌شود. مرحله دوم که مرحله حمله یا برخط نام دارد، از این داده‌ها، به نحوی که در مقاله هلمن شرح داده شده است (که موضوع بحث این مقاله نیست)، برای معکوس کردن تابع f (شکست الگوریتم رمز و به‌دست آوردن کلید) استفاده می‌شود. مهمترین مشکل زنجیره‌هایی که به این روش ساخته می‌شوند این است که پس از مدتی ۱) در یک حلقه گرفتار می‌شوند و ۲) به‌علت وجود تصادم، با زنجیره‌هایی که قبلاً تولید شده‌اند، برخورد کرده و ادغام می‌شوند و در نتیجه کارآیی

* رایانامه نویسنده مسئول: nh.gharavi@chmail.ir

1-Hellman
2-Time Memory Trade-Off

روش در معکوس کردن تابع f به شدت کاهش پیدا می‌کند. هلمن برای مقابله با پدیده ادغام زنجیره‌ها پیشنهاد می‌کند به جای یک جدول،t جدول ساخته شود و خروجی تابع f در هر جدول با یک مقدار دلخواه ولی متفاوت (مثل شماره جدول)ترکیب (*xor*) شود. به این مقدار دلخواه، حالت پنهان[1] گفته می‌شود [۲]. علت این نام گذاری آن است که بیشترین زمان اجرای فاز حمله، صرف کشف مقدار صحیح حالت پنهان می‌شود. با به‌کارگیری حالت پنهان، اگر دو زنجیره در دو جدول مختلف با یکدیگر تصادم پیدا کنند، در یکدیگر ادغام نخواهند شد. بدین صورت مشکل تا حدودی رفع می‌شود ولی همچنان در هر جدول به تنهایی، این مشکلات وجود دارد و در مجموع نیز احتمال موفقیت روش هلمن چندان بالا نیست.

بارزترین کارهای انجام شده در ادامه‌ی کار هلمن برای بهبود آن، عبارتند از: روش نقاط تمایز ریوست[2] که در سال ۱۹۸۹ ارائه و به حمله DP مشهور شد. حمله DP با به‌کارگیری نقاط تمایز، فضای موردنیاز و زمان جستجو را از طریق کاهش نیاز به دسترسی به حافظه‌ی سخت، کاهش می‌دهد [۳]. مهمترین بهبود ارائه‌شده روی جداول هلمن، توسط اُکلین[3] در سال ۲۰۰۳ انجام شد [۴]. اُکلین با به‌کارگیری جداول رنگین کمانی[4] و استفاده از توابع پوشانه متفاوت روی ستون‌های جدول هلمن، سعی کرد به مقابله با رفتارهای نامطلوب زنجیره‌ها (ادغام و دوری شدن) بپردازد. نسخه‌های دیگری از حمله اُکلین، با نام حمله رنگین کمانی نازک[5] و رنگین کمانی فازی[6] توسط بارکان، بیهام و شامیر[7] در سال ۲۰۰۶ ارائه شد[۵]. یک نسخه ترکیبی از حملات TMTO نیز در سال ۲۰۱۰ ارائه شد که با ترکیب حمله DP و جداول رنگین کمانی، روی الگوریتم رمز A5/1 اجراء شده و توانست آن را بشکند. این حمله جدید، روش کراکن نام گرفت [۶-۷]. در مجموع هر چند این تحقیقات و سایر کارهای انجام شده اخیر، منجر به بهبودهایی به لحاظ حافظه و سرعت روی حمله هلمن گردیدند، اما هیچ یک نتوانستند سطح پوشش جداول و در نتیجه احتمال موفقیت حمله را افزایش چندانی بدهند. لذا در این مقاله هدف ما آن است که با تمرکز بر مرحله اول حمله هلمن، به تحلیل رفتاری زنجیره‌های رمز پرداخته و علت پایین بودن سطح پوشش جداول را بررسی کنیم. از آنجایی که زنجیره‌های هلمن در واقع مسیرهایی دلخواه با نقاط شروع و پایان معین روی گراف تابع و در جهت حرکت آن می‌باشند که از قوانین و رفتارهای گراف توابع تبعیت می‌کنند، تحلیل ما بر مبنای گراف توابع تصادفی خواهد بود. نتایج عملی تحلیل فوق را روی یک نسخه کوچک شده از الگوریتم رمز استاندارد AES به نام mAES پیاده سازی و مقایسه کرده‌ایم. mAES الگوریتمی است که برای مقاصد آموزشی و آزمایشی با مبانی الگوریتم AES ولی در مقیاس کوچک، با طول کلید و قالب ۱۶ بیت، ایجاد شده است [۹ - ۸]. کد منبع این الگوریتم به زبان برنامه سازی C، با استفاده از مرجع [۹] نوشته شده است. بقیه ساختار مقاله، به ترتیب شامل مباحث زیر می‌باشد: در بخش ۲، مفاهیم اساسی مورد استفاده معرفی شده‌اند. در بخش ۳ تحلیل رفتاری زنجیره-های رمز هلمن را در چهار زیربخش مشتمل بر تحلیل رئوس پایانه‌ای و حالات پنهان و تحلیل احتمالاتی دور و ادغام زنجیره-ها، ارائه خواهیم نمود. بخش چهارم و پایانی مقاله به نتیجه‌گیری اختصاص دارد.

۲- مفاهیم اساسی

برخی مفاهیم اساسی مورد نیاز را شرح می‌دهیم.

۲-۱- توابع تصادفی

مجموعه A را مجموعه تمام رشته بیت‌های0 و 1 به طول n در نظر گرفته می شود. بنا به اصل ضرب، تعداد اعضای مجموعه A برابر 2^n است که از این به بعد قرار می‌دهیم $N = 2^n$. همچنین مجموعه همه توابع از مجموعه A به A را با $S=\{f \mid f:A\rightarrow A\}$ نشان داده که بنا به اصل ضرب تعداد اعضای S برابر N^N است. یک تابع تصادفی روی A متغیری تصادفی است که هر یک از اعضای S را با احتمال مساوی $\frac{1}{N^N}$ انتخاب می‌کند. صورت معادل دیگر برای تابع تصادفی این است که بگوییم، تابعی است که هر رشته بیت از مجموعه A را با احتمال مساوی $\frac{1}{N}$ به رشته بیت دیگری در A می‌نگارد. یا این‌که تابعی است که هر بیت iام، $1 \le i \le n$، یک رشته بیت از A را با احتمال $\frac{1}{2}$ به 0 و با همان احتمال به 1، در رشته بیت تصویر شده، می‌نگارد. می‌توان نشان داد که صورت‌های ذکر شده در بالا برای یک تابع تصادفی معادل هم هستند.

۲-۲- گراف توابع تصادفی

فرض کنید f یک تابع تصادفی روی مجموعه A باشد. گراف تابع f یک گراف جهت‌دار است که مجموعه رئوس آن A و یال‌های آن زوج مرتب‌های $(x, f(x))$ هستند که $x \in A$. گراف یک تابع ممکن است دارای چندین مؤلفه همبندی[8] (زیرگراف

1-Hidden State
2-Rivest
3- Ochshelin
4- Rainbow Table
5-Thin-Rainbow
6-Fuzzy-Rainbow
7- Barkan, Biham, Shamir

8- Connected Component

همبند ماکزیمال) باشد. هر مؤلفه همبندی دارای تنها یک دور جهت‌دار و چندین درخت جهت‌دار است که به این دور متصل شده‌اند. دنباله نقاط $x_0, x_1, x_2, \ldots$ را در نظر بگیرید که در آن $x_0 = x$ و $x_i = f(x_{i-1})$ برای هر i. در گراف یک تابع، این دنباله بخشی از یکی از مؤلفه‌های همبندی را نمایش می‌دهد. در حقیقت این دنباله یک مسیر جهت‌دار از گراف است که به یک دور جهت‌دار متصل می‌شود. تعاریف زیر در ادامه این مقاله مورد نیاز خواهد بود [۱۰].

۱) طول مسیر(تعداد یال‌ها) با شروع از رأس x به اولین رأس روی دور مؤلفه همبندی وابسته به x را طول دم[1] x می‌نامند و آن را با $\lambda(x)$ نمایش می‌دهند.

۲) طول مسیر دور جهت‌دار وابسته به رأس x (که با تعداد یال‌ها و یا رئوس اندازه‌گیری می‌شود) را طول دور[2] x می‌نامند و با $\mu(x)$ نمایش می‌دهند.

۳) طول مسیر بدون تکرار در دنباله بالا را طول ρ برای x می‌نامند و آن را با $\rho(x)$ نمایش می‌دهند. به پارامتر ρ، غالباً Rho-length هم گفته می‌شود. توجه نمائید که $\rho(x) = \lambda(x) + \mu(x)$.

۴) تعداد یال‌ها در مؤلفه همبندی شامل رأس x را اندازه مؤلفه[3] x می‌نامند.

۵) رأس x را دوری می‌نامند، اگر متعلق به یک دور باشد.

۶) رأس x را پایانه (ترمینال) گویند هرگاه $f^{-1}(x)$ تهی باشد (پیش تصویر نداشته باشد و خودش تصویر یک رأس دیگر باشد). در حقیقت یک رأس پایانه‌ای رأسی است که اولاً تنها نباشد و ثانیاً هیچ ورودی نداشته باشد.

۲-۳- پارامترهای گراف توابع تصادفی

گراف توابع تصادفی دارای ویژگی‌های خاصی هستند که این ویژگی‌ها در خصوص مفهوم کلی گراف‌ها مصداق ندارد. مهمترین این ویژگی‌ها عبارتند از: جهت‌دار بودن گراف، وجود یک یا چند مؤلفه همبندی در گراف، وجود یک و تنها یک دور در هر مؤلفه همبندی و این‌که هر رأس می‌تواند فاقد ورودی باشد (ترمینال نودها)، می‌تواند دارای یک و یا چند ورودی باشد، ولی حتماً یک و فقط یک خروجی دارد. بر اساس این ویژگی‌ها، پارامترهایی برای بررسی رفتار گراف توابع تعریف شده است. در مراجع [۱۱ -۱۰] این پارامترها به دو دسته (پارامترهای مستقیم[4] و تجمعی[5]) تقسیم‌بندی شده و مقدار آنها به اثبات رسیده است که ما به لحاظ اهمیت، مهم‌ترین این پارامترها را در جدول‌های (۲- ۱) نشان داده‌ایم.

جدول (۱). پارامترهای مستقیم یک گراف تصادفی [۱۰]

نام پارامتر	مقدار پارامتر
تعداد مؤلفه‌ها (*# Components*)	$\frac{1}{2}\log N$
تعداد نقاط حلقوی (*# Cyclic nodes*)	$\sqrt{\pi N/2}$
تعداد نقاط پایانه‌ای (*#Terminal nodes*)	$e^{-1}N$

جدول (۲). پارامترهای تجمعی یک گراف تصادفی [۱۱]

نام پارامتر	**مقدار پارامتر**
طول دم (*Tail length*)	$\lambda = \sqrt{\pi N/8}$
طول حلقه (*Cyclic length*)	$\mu = \sqrt{\pi N/8}$
طول مسیر بدون تکرار (*Rho-length*)	$\rho = \sqrt{\pi N/2}$ $(\rho = \lambda + \mu)$
اندازه مؤلفه (*Component size*)	$2N/3$

۳- تحلیل رفتاری زنجیره‌های رمز هلمن

همان‌طور که دیده شد زنجیره‌های هلمن با طول معین t با شروع از یک نقطه تصادفی و به تعداد m ساخته می‌شوند. این بدین معنی است که به‌طور تصادفی m رأس روی تعدادی از مؤلفه‌های همبندی گراف تابع انتخاب کرده‌ایم و از هر رأس به تعداد معین t یال پیش رفته‌ایم. تعداد رئوس متمایزی که بدین ترتیب به دست می‌آید (سطح پوشش جدول)، همان تعداد یال‌های متمایز طی شده روی گراف تابع خواهد بود که به‌طور مستقیم بستگی دارد به پارامترهای گراف تابع که در بخش (۲-۳) معرفی شد. در ادامه با توجه به نقش این پارامترها به تحلیل رفتاری زنجیره‌های هلمن بر اساس این مسیرها روی گراف تابع تصادفی خواهیم پرداخت.

۱-۳- نقش رئوس پایانه‌ای

رأس دلخواه x را در نظر بگیرید. هر رأس با احتمال $\frac{1}{N}$ به x نگاشته می‌شود و با احتمال $1 - \frac{1}{N}$ به آن نگاشته نمی‌شود. پس در کل با احتمال $\left(1 - \frac{1}{N}\right)^N$ هیچ رأسی به x نگاشته نمی‌شود و

1-Tail length
2-Cycle length
3-Component size
4-Direct Parameters
5-Cumulative Parameters

لذا با همین احتمال یک رأس پایانه‌ای است. از طرفی می‌دانیم که $\lim_{N\to\infty}\left(1-\frac{1}{N}\right)^N = e^{-1}$. بنابراین طبق قضیه حد مرکزی، با احتمال زیاد تعداد رئوسی که هیچ رأسی به آن‌ها نگاشته نشده است (رئوس پایانه‌ای) برابر است با $e^{-1}N$. این مطلب که در جدول (۱) نیز نشان داده شده است، بدان معناست که حدود $\frac{100}{e} \approx 37\%$ از کل رئوس (N)، پایانه‌ای هستند. به عبارت دیگر این رئوس روی هر مسیر دلخواهرویگراف تابع، هرگز رخ نمی‌دهند، مگر آن‌که رأس آغازین آن مسیر باشند. ما این مطلب را روی تابع رمز mAES پیاده‌سازی نموده‌ایم. نتیجه به‌دست‌آمده برابر ۳۶٫۵۹٪ است که به خوبی این موضوع راتأیید می‌کند. در روش هلمن، برای ساخت یک زنجیره، امکان توجه به این نکته وجود نداشته و به طور ناخواسته به همین مقدار از میزان پوشش هر جدول کاسته خواهد شد.

۳-۲- تأثیر تغییرات مقدار حالت پنهان

در روش هلمن، جداول مختلف با تغییرات مقدار حالت پنهان ساخته می‌شوند. واضح است که تغییر حالت پنهان موجب تغییر گراف تابع، که زنجیره‌های رمز منتج از آن هستند، می‌گردد. یک سؤال اساسی در اینجا مطرح خواهد شد که چه رابطه‌ای بین پارامترهای گراف یک تابع تصادفی با پارامترهای گراف توابع حالات پنهان آن وجود دارد؟ ممکن است در حالت کلی چنین رابطه‌ای برای همه پارامترها وجود داشته و یا نداشته باشد. به نظر می‌رسد پاسخ کامل به این سؤال دشوار بوده و خود می‌تواند موضوع یک تحقیق جداگانه و مستقل باشد. اما آنچه که ما در اینجا بررسی نموده‌ایم حول دو محور است: اول نشان می‌دهیم که تعداد رئوس پایانه‌ای تغییر نمی‌کند و هرکدام از دیگری قابل محاسبه است و دوم این‌که، علیرغم آن‌که گراف هر تابع مفروض دارای مشخصات معینی است (مانند طول مسیر بدون تکرار، تعداد حلقه‌ها یا مولفه‌ها و غیره)، اما با اعمال حالت پنهان، هرچند که تعداد رئوس پایانه‌ای ثابت می‌مانند، سایر پارامترهای گرافبه لحاظ کیفی و کمی تغییر می‌کند. لذا مستقل از آنکه بتوانیم رابطه‌ای بین پارامترهای گراف تابع و حالات پنهان آن پیدا کنیم یا خیر، تغییر حالت پنهان، به‌لحاظ ساخت زنجیره‌های رمز، می‌تواند تأثیر مثبت و یا تأثیر منفی داشته باشد. دلیل این امر آن است که رئوس پایانه‌ای هیچ پیش تصویری ندارند، بنابراین، با تغییر حالت پنهان فقط مقدار آنها تغییر می‌کند، ولی موقعیت آنها به عنوان رأس پایانه‌ای تغییری نمی‌کند. اما سایر رئوس که در واقع خروجی‌های تابع در موقعیت‌های مختلف هستند، با تغییر حالت پنهان هم از لحاظ مقدار و هم موقعیت، هر دو تغییر می‌کنند و در کل این تغییرات به نحوی است که از روی گراف یک تابع، می‌توان گراف حالات پنهان آن و به ویژه رئوس پایانه‌ای را به‌دست آورد. در خصوص محور اول بحث، گفته شد که با داشتن رئوس پایانه‌ای یک تابع مفروض، رئوس پایانه‌ای حالات پنهان آن نیز به‌دست می‌آید. این مطلب در قضیه (**۱**) در زیر ثابت شده است.

قضیه (۱). فرض کنید مجموعه

$$\tau = \{v_j | f^{-1}(v_j) = \emptyset, j = 1, \dots, k\}$$

و f شامل تمام رئوس پایانه‌ای تابع

$$\{F_i(x) = f(x) \oplus i, \mid i \in \mathrm{S}, F_0 = f\}$$

مجموعه تمام توابع تصادفی قابل استفاده در جداول هلمن با فضای حالت پنهان S باشند. آنگاه مجموعه

$$\tau_i = \{v_j \oplus i \,|F_i^{-1}(v_j \oplus i) = \emptyset, j = 1, \dots, k\}$$

شامل تمام رئوس پایانه‌ای تابع F_i برای هر $i \in \mathrm{S}$ است.

اثبات:

برای اثبات ابتدا نشان می‌دهیم که هر رأس به فرم $v_j \oplus i$ در F_i ، هیچ پیش تصویری نمی‌تواند داشته باشد. این شرط لازم است اما کافی نیست، زیرا ممکن است رئوس دیگری هم وجود داشته باشند که پیش تصویر نداشته باشند. لذا به عنوان شرط کافی نشان می‌دهیم هر رأسی که پیش تصویر نداشته باشد، حتما به فرم $v_j \oplus i$ خواهد بود.

۱) ابتدا فرض کنید $F_i(x) = v_j \oplus i$. نشان می‌دهیم چنینxی وجود ندارد. فرض کنید وجود داشته باشد، پس با توجه به تعریف F_i داریم $F_i(x) = f(x) \oplus i = v_j \oplus i$. این زمانی اتفاق می‌افتد که $f(x) = v_j$ شود. اما این با تعریف v_j (که پیش تصویر ندارد) در تناقض است. بنابراین چنین x ی وجود ندارد یعنی $v_j \oplus i$ دارای پیش تصویری توسط تابع F_i نمی‌باشد. بنابراین مجموعه‌ی$\{v_j \oplus i \mid j = 1, \dots, k\}$ زیر مجموعه تمام رئوس پایانه‌ای تابع F_i می‌باشد.

۲) حال فرض کنید x یک رأس پایانه‌ای تابع F_i باشد، یعنی$F_i^{-1}(x) = \emptyset$. نشان خواهیم داد که به ازای یک i و j خاص$x = v_j \oplus i$ خواهد بود. $F_i^{-1}(x) = \emptyset$ یعنی هیچ y وجود ندارد که $F_i(y) = x$ شود یا به عبارتیyی وجود ندارد که $f(y) \oplus i = x$. بنابراین به ازای هر y: $f(y) \neq x \oplus i$. اما این یعنی $x \oplus i$ یک رأس پایانه‌ای برای f است. در نتیجه به ازای یک j ، $v_j = x \oplus i$ خواهد شد. از این‌رو $x = v_j \oplus i$ و نتیجه خواهد شد که مجموعه تمام رئوس پایانه‌ای تابع F_i زیرمجموعه $\{v_j \oplus i \mid j = 1, \dots, k\}$ می‌باشد.

در خصوص محور دوم این بحث، گفته شد که تغییرات حالت پنهان باعث تغییر گراف حالت پنهان تابع نیز می‌گردد و این

تغییرات به لحاظ مسئله ساخت زنجیره‌ها، می‌توانند در جهت مثبت و یا در جهت منفی باشد. یعنی با انتخاب حالات پنهان مناسب، می‌توان زنجیره‌های خوبی (با پوشش بالا) ساخت و یا با انتخاب مقادیر نامناسب می‌توان زنجیره‌های بد (با پوشش اندک) ساخت. در حالت کلی می‌توان گفت که هرچه گراف تابع دارای مؤلفه‌های همبندی کمتری بوده و طول مسیر بدون تکرار و طول حلقه‌ی آن بزرگتر باشد، این وضعیت برای ساخت زنجیره‌ها مطلوب‌تر خواهد بود. ما بررسی کاملی به روی این موضوع انجام داده‌ایم. برای سادگی و روشن شدن مطلب، تابع f را به‌صورت زیر درنظر بگیرید. در انتخاب این تابع سعی شده رفتار غیرخطی توابع رمز، از طریق به‌کارگیری یک جعبه جانشینی[1]، در مقیاس کوچک، شبیه‌سازی شود.

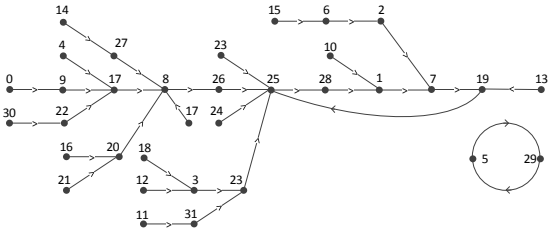
$$f(x) = x^2 + Sbox[x] \ (mod\ 32);$$

که

$$Sbox[x] = \{9,12,3,14,1,4,30,2,26,0,29,6,19,10,23,5,\\ 20,7,31,16,24,27,13\ \ 8,25,11,21,15,17,28,18,22\}$$

این یک تابع ۵ بیتی و با $N = 2^5 = 32$ است یعنی $f: \{0,1,\dots,31\} \mapsto \{0,1,\dots,31\}$. گراف این تابع را در شکل (۱) نشان داده‌ایم. چنانچه ملاحظه می‌شود این گراف دارای دو مؤلفه با حلقه‌هایی به طول ۲ و ۵ می‌باشد. حداکثر طول مسیر بدون تکرار در این گراف مربوط به نقاط پایانه‌ای ۰ و ۳۰ می‌باشد:

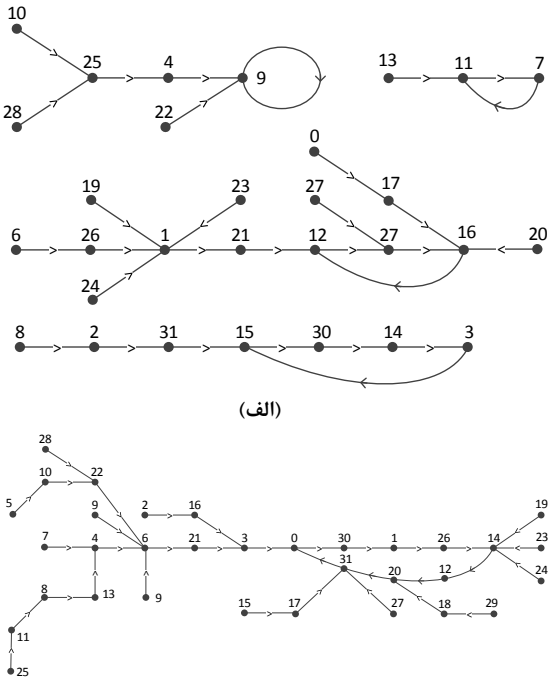
$$\rho(0) = \rho(30) = \rho_{max} = 10.$$



شکل (۱). گراف تابع تصادفی

$$f(x) = x^2 + Sbox[x] \ (mod\ 32)$$

روشن است که فضای حالات پنهان، در روش هلمن، برای این تابع برابر $S = \{0,1,\dots,31\}$ خواهد بود. مجموعه‌ی تمام توابع تصادفی قابل به‌کارگیری در جدول‌های هلمن، با توجه به حالات پنهان، را با F_i نشان می‌دهیم که: $F_i = f \oplus i, \forall i \in S$. ما مقادیر تمام توابع F_i و همچنین مقادیر نقاط پایانه‌ای هریک را به طور جداگانه (با پیاده‌سازی نرم‌افزاری)، به‌دست آورده‌ایم. اکنون به کمک این اطلاعات، گراف تمام توابع تصادفی F_i را نیز رسم می‌نمائیم. نتیجه بررسی این گراف‌ها نشان می‌دهد که الگوهای مختلفی در گراف توابع F_i وجود دارد. فرض کنید $\rho_{i,min}$ و $\rho_{i,max}$ به ترتیب نشان دهنده حداقل و حداکثر طول مسیر بدون تکرار در گراف تابع F_i باشد. دو حالت حدی را در شکل (۲) نشان داده‌ایم. شکل (۲- الف) نشان دهنده گراف حالت پنهان با حداقل طول مسیر بدون تکرار در کل فضا برابر $\rho(6)_{24,min} = 7$ و شکل (۲- ب) نشان دهنده گراف حالت پنهان با حداکثر طول مسیر بدون تکرار در کل فضا برابر $\rho(25)_{23,max} = 16$ می‌باشد. گراف شکل (۲- الف) دارای چهار مؤلفه است، درحالیکه گراف شکل (۲- ب) دارای یک مؤلفه است. در بهترین حالت با گراف شکل (۲- الف) می‌توان زنجیره‌ای به طول هفت ساخت، در حالی که با گراف شکل (۲- ب) در بهترین حالت می‌توان زنجیره‌ای با پوشش نیمی از فضا ساخت، به علاوه احتمال گرفتار شدن در حلقه‌های کوچک در گراف (۲- الف) بسیار بیشتر است. این مثال به خوبی تفاوت نقش حالت پنهان را در ساخت زنجیره‌ها، در روش هلمن نشان می‌دهد. در واقع نزدیک به نیمی از حالات پنهان دلخواه به‌کار رفته در روش هلمن، به لحاظ تحلیل گراف، حالت‌های مناسبی نبوده و نمی‌توانند آن طور که انتظار می‌رود، به سطح پوشش جدول‌ها اضافه کنند.



(الف)

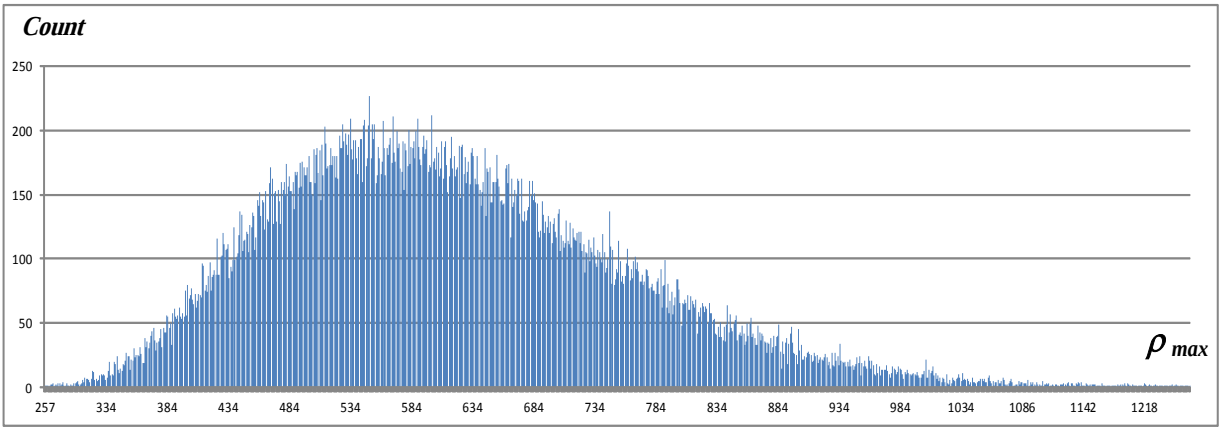
(ب)

شکل (۲). گراف تابع تصادفی f با دو حالت پنهان مختلف
الف) F_{24} با حداقل طول مسیر بدون تکرار در کل فضا
ب) F_{23} با حداکثر طول مسیر بدون تکرار در کل فضا

نتیجه این بررسی روی الگوریتم mAES پیاده شد. به علت بزرگی فضا، امکان نمایش گراف این الگوریتم وجود ندارد. لذا با محاسبات نرم‌افزاری، داده‌های گراف الگوریتم و گراف تمام

1-Substitution-box (S-box)

حالت‌های پنهان آن را به‌صورت مجموعه‌ای از نقاط رئوس و یال‌ها و پارامترهای مستقیم هر گراف را به‌طور جداگانه به‌دست‌آورده و داده‌های خروجی تحلیل شده‌اند. این تحلیل مبتنی بر اندازه‌گیری مهمترین پارامتر مؤثر گراف در ساخت زنجیره‌ها، یعنی طول بزرگترین مسیر بدون تکرار (ρ_{max}) می‌باشد. سپس با استفاده از این اطلاعات نمودار فراوانی و تغییرات ρ_{max} رسم شده و در شکل (۳) نشان داده شده است. در این نمودار محور افقی نشان‌دهنده مقادیر ρ_{max} و محور عمودی نشان‌دهنده فراوانی آن در کل فضای حالات پنهان می‌باشد. این نمودار نشان دهنده یک توزیع نزدیک به نرمال است که مقادیر آن هرچه به سمت راست قرار داشته باشند، برای ساخت زنجیره‌ها مطلوب‌تر و هرچه به سمت چپ باشند، نامطلوب‌تر هستند. واضح است که برای Nهای بزرگتر، شکل این منحنی به حالت نرمال خود نزدیک‌تر شده و از همین قانون تبعیت خواهد کرد. بنابراین نتیجه‌بحث این است‌که انتخاب مقدار حالت پنهان تاثیر به‌سزایی در کارایی و سطح پوشش جدول‌های تولید شده دارد. در روش هلمن به انتخاب حالت پنهان مناسب، توجهی نمی‌شود، لذا با احتمال تقریباً یکسان امکان انتخاب حالت مناسب و یا نامناسب وجود دارد و حالات نامناسب منجر به تولید جدول-هایی با سطح پوشش پایین خواهند شد.



شکل (۳). نمودار تغییرات ρ_{max} گراف الگوریتم mAES و حالات پنهان آن

۳-۳- احتمال ساخت مسیر بدون تکرار با طول بیشتر از یک مقدار ثابت (تحلیل دوری)

در این بخش می‌خواهیم با بررسی طول مسیر بدون تکرار (Rho-length) در گراف توابع تصادفی و تعمیم آن به زنجیره‌های هلمن، کارآیی این زنجیره‌ها را از این جنبه تحلیل کنیم. در مرجع [۱۱] نشان داده شده که

$$\Pr\{\rho \geq t\} = \frac{N-1}{N}\frac{N-2}{N}\dots\frac{N-t}{N}. \qquad (۱)$$

است. از آنجایی که محاسبه احتمال فوق برای Nهای بزرگ[۱] کار دشوار و حتی غیرممکن است، در ادامه این بخش تقریب مناسبی برای محاسبه آسان‌تر رابطه (۱) ارایه می‌دهیم.

قضیه (۲). فرض کنید مقدار N بسیار بزرگ و $t \leq \sqrt{N}$ باشد. همچنین فرض کنید تحت یک تابع تصادفی تعریف‌شده روی مجموعه‌ای متشکل از N رأس، با شروع از رأس دلخواه x زنجیره را می‌سازیم. در این صورت احتمال این که Rho-length بزرگتر یا مساوی عدد طبیعی t باشد را می‌توان به‌صورت $\Pr\{\rho \geq t\} \cong e^{-\frac{t^2}{2N}}$ تقریب زد.

اثبات:

ابتدا رابطه (۱) را به شکل زیر بازنویسی می‌کنیم:

$$\Pr\{\rho \geq t\} = \frac{(N-1)!}{N^t(N-t-1)!} = \frac{N!(N-t)}{N^t(N-t)!N}. \qquad (۲)$$

بسط تیلور تابع لگاریتم به ازای هر $0 < x < 1$، به‌صورت $\ln(1-x) = -x - \frac{x^2}{2} - \frac{x^3}{3} - \cdots$ می‌باشد. چون $x\sqrt{N} < N$ بنابراین نامساوی $0 < \frac{x}{\sqrt{N}} < 1$ برقرار است و با جاگذاری داریم: $\ln\left(1-\frac{x}{\sqrt{N}}\right) = -\frac{x}{\sqrt{N}} - \frac{x^2}{2N} - \frac{x^3}{3N\sqrt{N}} - \cdots$. حال با استفاده از این بسط داریم:

$$\left(1-\frac{x}{\sqrt{N}}\right)^N = e^{\ln\left(1-\frac{x}{\sqrt{N}}\right)^N}$$
$$= e^{N\left(-\frac{x}{\sqrt{N}}-\frac{x^2}{2N}-\frac{x^3}{3N\sqrt{N}}-\cdots\right)} = e^{-\sqrt{N}x-\frac{1}{2}x^2-\frac{1}{3\sqrt{N}}x^3-\cdots}.$$

وقتی که N به بی‌نهایت میل می‌کند، جملات سوم به بعد در نما، به صفر میل می‌کنند و لذا می‌توان نوشت:

$$\left(1-\frac{x}{\sqrt{N}}\right)^N \cong e^{-\sqrt{N}x-\frac{1}{2}x^2}.$$

۱- بزرگ بودن N یک امر نسبی است که با توان پردازشی قابل دسترس، معنا می‌شود.

همچنین به روش مشابه می‌توان نتیجه گرفت:

$$\left(1-\frac{x}{\sqrt{N}}\right)^{-\sqrt{N}x} \cong e^{x^2}.$$

اکنون با استفاده از تقریب استرلینگ برای محاسبه فاکتوریل اعداد بزرگ[۱] و با توجه به تقریب‌های بالا داریم:

$$\Pr\{\rho \geq t\} = \frac{N!(N-t)}{N^t(N-t)!N} \cong \frac{\left(\frac{N}{e}\right)^N \sqrt{2\pi N}(N-t)}{N^t\left(\frac{N-t}{e}\right)^{N-t}\sqrt{2\pi(N-t)}N}.$$

حال فرض کنید عدد c به گونه‌ای انتخاب شده باشد که، $t = c\sqrt{N}$ در این صورت داریم:

$$\Pr\{\rho \geq t\} = \frac{e^{-c\sqrt{N}}\sqrt{N}\left(N-c\sqrt{N}\right)}{\left(1-\frac{c}{\sqrt{N}}\right)^{N-c\sqrt{N}}\sqrt{N-c\sqrt{N}}N}$$

$$= \frac{e^{-c\sqrt{N}}\sqrt{N-c\sqrt{N}}}{\left(1-\frac{c}{\sqrt{N}}\right)^{N}\left(1-\frac{c}{\sqrt{N}}\right)^{-c\sqrt{N}}\sqrt{N}}$$

$$= \frac{e^{-c\sqrt{N}}\sqrt{N-c\sqrt{N}}}{e^{-c\sqrt{N}-\frac{1}{2}c^2}e^{c^2}\sqrt{N}}$$

$$= \frac{\sqrt{N-c\sqrt{N}}}{e^{\frac{1}{2}c^2}\sqrt{N}}$$

که چون $c = O(1)$، لذا می‌توان نوشت:

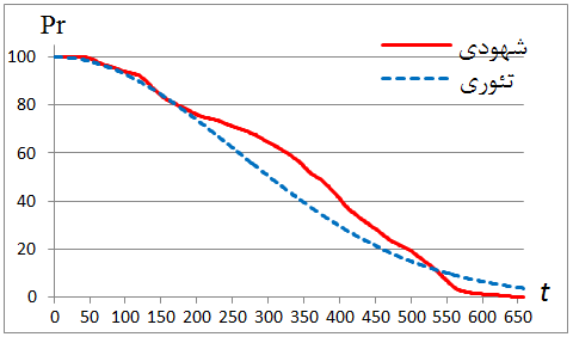
$$\Pr\{\rho \geq t\} \cong \frac{1}{e^{\frac{1}{2}c^2}} = e^{-\frac{1}{2}c^2}$$

که

$$\Pr\{\rho \geq t\} \cong e^{-\frac{t^2}{2N}}$$

■

این رابطه به ما نشان می‌دهد که اگر از یک نقطه تصادفی شروع به ساخت یک زنجیره رمز نمائیم، مانند آن است که از یک رأس دلخواه روی گراف یک تابع تصادفی شروع به حرکت کنیم و طول مسیر طی شده، قبل از آنکه به اولین تکرار برسیم، با احتمال $e^{-\frac{t^2}{2N}}$ ، بزرگتر یا مساوی عدد طبیعی t خواهد بود. به عبارت دیگر در ساخت زنجیره‌های هلمن، توجه به احتمال فوق جهت انتخاب پارامتر t ، ما را از ساخت زنجیره‌های دوری که در واقع هدر دادن منابع است، باز خواهد داشت و در مقابل عدم توجه به آن موجب ساخت زنجیره‌های دوری و کاهش سطح پوشش جداول می‌گردد. برای N معین، نتیجه این احتمال، با مشاهدات شهودی روی الگوریتم رمز mAES در نمودار شکل (۴) مقایسه شده است.



شکل (۴). نمودار احتمالی ساخت یک زنجیره با $\rho \geq t$ در دو حالت نظری و عملی روی الگوریتم mAES

۳-۴- تحلیل ادغام

در این بخش می‌خواهیم از یک رأس تصادفی شروع کرده و زنجیره‌ای بدون تداخل و تقاطع بسازیم. هدف ما محاسبه احتمال این که زنجیره تا طول حداقل t در حلقه نیفتد و با زنجیره‌های قبلی هم ادغام نشود است . البته فرمولی که برای محاسبه این احتمال ارائه می‌کنیم، با این فرض است که قبلا r زنجیره بدون حلقه ساخته شده‌اند که با همدیگر ادغام نمی‌شوند. اگر مجموعه D_i نشان دهنده رئوس زنجیره i اُم باشد، مجموعه D را

به صورت $D = D_1 \cup D_2 \cup \cdots \cup D_r$ در نظر می‌گیریم و قرار می‌دهیم $|D| = d$. حال می‌خواهیم با شروع از رأس تصادفی x زنجیره $r+1$ اُم را بسازیم. چون ادغام زنجیره جدید با زنجیره‌های قبلی نامطلوب می‌باشد، لذا می‌خواهیم که تمامی اعضای این زنجیره از D^c (مکمل مجموعه D)، که تعداد اعضای آن به وضوح برابر $N-d$ است، انتخاب شوند. حال برای نقطه x مفهوم ρ_D را به این صورت تعریف می‌کنیم که برابر طول زنجیره بدون تکرار ساخته شده از x باشد که اعضای آن در D نباشند. در این صورت با استفاده از رابطه (۱)، احتمال اینکه ρ_D از عدد مفروض t بزرگتر باشد، به صورت زیر محاسبه می‌شود:

$$\Pr\{\rho_D \geq t\} = \frac{N-d}{N}\frac{N-d-1}{N}\frac{N-d-2}{N}\cdots\frac{N-d-t}{N}.$$

این رابطه را می‌توان به شکل زیر نیز بازنویسی کرد:

$$\Pr\{\rho_D \geq t\} = \frac{(N-d)!}{N^{t+1}(N-d-t-1)!}.$$

و یا:

$$\Pr\{\rho_D \geq t\} = \frac{(N-d)!(N-d-t)}{N^t(N-d-t)!N} \qquad (۳)$$

۲- تقریب استرلینگ: $N! \approx \left(\frac{N}{e}\right)^N \sqrt{2\pi N}$

در حقیقت رابطه (۳) تعمیم رابطه (۲) است. بدین معنی که اگر قرار دهیم $d=0$، مفهوم ρ_D تبدیل به ρ می‌شود و همان رابطه به دست می‌آید. حال می‌خواهیم احتمالی که با رابطه (۳) قابل محاسبه است را برای Nهای بزرگ تقریب بزنیم. این موضوع را به صورت قضیه زیر بیان می‌کنیم.

قضیه (۳). فرض کنید D زیرمجموعه‌ای d عضوی از مجموعه شامل N رأس که $d \le \sqrt{N}$ باشد. اگر x یک رأس تصادفی از مجموعه تمام رئوس انتخاب شود و تحت تابعی تصادفی از رأس x شروع به ساخت زنجیره کنیم آن‌گاه احتمال این که زنجیره دارای طول بزرگتر یا مساوی t بوده (که $t=O(\sqrt{N})$) و با D اشتراک نداشته باشد برابر است با

$$\Pr\{\rho_D \ge t\} = \frac{(N-d)!\,(N-d-t)}{N^t (N-d-t)!\,N}.$$

اثبات :

لذا با استفاده از تقریب استرلینگ نتیجه می‌شود:

$$\Pr\{\rho_D \ge t\} \cong \frac{\left(\frac{N-d}{e}\right)^{N-d}\sqrt{2\pi(N-d)}(N-d-t)}{N^t\left(\frac{N-d-t}{e}\right)^{N-d-t}\sqrt{2\pi(N-d-t)}N}$$

$$= \frac{\left(\frac{N-d}{N}\right)^{N-d} e^{-t}\sqrt{N-d}\,(N-d-t)}{\left(\frac{N-d-t}{N}\right)^{N-d-t}\sqrt{N-d-t}N}$$

حال با قرار دادن $t=p\sqrt{N}$ و $d=q\sqrt{N}$ نتیجه می‌شود:

$$Pr\{\rho_D \ge t\}$$
$$\cong \frac{\left(1-\frac{q}{\sqrt{N}}\right)^{N-q\sqrt{N}} e^{-p\sqrt{N}}\sqrt{N-q\sqrt{N}}\left(N-(p+q)\sqrt{N}\right)}{\left(1-\frac{p+q}{\sqrt{N}}\right)^{N-(p+q)\sqrt{N}}\sqrt{N-(p+q)\sqrt{N}}\,N}$$
$$= \frac{\left(1-\frac{q}{\sqrt{N}}\right)^{N}\left(1-\frac{q}{\sqrt{N}}\right)^{-q\sqrt{N}} e^{-p\sqrt{N}}\sqrt{N-q\sqrt{N}}\left(N-(p+q)\sqrt{N}\right)}{\left(1-\frac{p+q}{\sqrt{N}}\right)^{N}\left(1-\frac{p+q}{\sqrt{N}}\right)^{-(p+q)\sqrt{N}}\sqrt{N-(p+q)\sqrt{N}}\,N}$$

چون N به بی‌نهایت میل می‌کند و $p=O(1)$ و $q=O(1)$، لذا داریم:

$$\Pr\{\rho_D \ge k\} \cong \frac{\left(1-\frac{q}{\sqrt{N}}\right)^{N}\left(1-\frac{q}{\sqrt{N}}\right)^{-q\sqrt{N}} e^{-p\sqrt{N}}}{\left(1-\frac{p+q}{\sqrt{N}}\right)^{N}\left(1-\frac{p+q}{\sqrt{N}}\right)^{-(p+q)\sqrt{N}}}$$

در اینجا به‌طور مشابه، با استفاده از تقریب‌های به‌کار رفته در قضیه (۲) داریم:

$$\Pr\{\rho_D \ge t\} \cong \frac{e^{-q\sqrt{N}-\frac{1}{2}q^2} e^{q^2} e^{-p\sqrt{N}}}{e^{-(p+q)\sqrt{N}-\frac{1}{2}(p+q)^2} e^{(p+q)^2}}$$

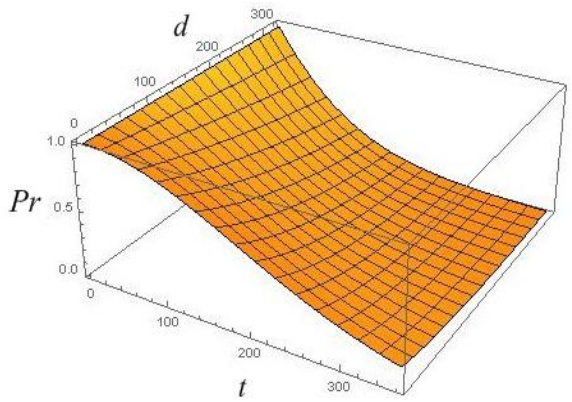
$$= \frac{e^{-q\sqrt{N}} e^{\frac{1}{2}q^2} e^{-p\sqrt{N}}}{e^{-(p+q)\sqrt{N}} e^{\frac{1}{2}(p+q)^2}}$$
$$= \frac{e^{\frac{1}{2}q^2}}{e^{\frac{1}{2}(p+q)^2}}$$
$$= e^{-\frac{1}{2}p^2-pq}$$
$$= e^{-\frac{1}{2}\left(\frac{t}{\sqrt{N}}\right)^2-\frac{td}{N}}$$
$$= e^{-\frac{t^2+2td}{2N}}.$$

در نتیجه داریم:

$$\Pr\{\rho_D \ge t\} \cong e^{-\frac{t^2+2td}{2N}}.$$

■

بنابراین، طراح حمله پس از ساخت هر زنجیره، به کمک این احتمال، می‌تواند تصمیم به ساختن یا نساختن زنجیره بعدی بگیرد. یعنی در واقع این فرمول به او می‌گوید که آیا احتمال معقولی برای ساخت یک زنجیره بعدی که با قبلی‌ها ادغام نشود و در حلقه هم نیفتد، وجود دارد یا خیر؟ در ساخت زنجیره‌های هلمن توجهی به این احتمال نمی‌شود و در حالی یک زنجیره جدید ساخته می‌شود، که احتمال ادغام آن با یکی از زنجیره‌های از قبل ساخته شده به شدت افزایش پیدا کرده و این کار به همین‌صورت تا m زنجیره ادامه پیدا می‌کند. بدیهی است که بعد از ساخت چند زنجیره‌ی ابتدایی، زنجیره‌های بعدی با احتمال زیاد در یکدیگر ادغام شده و آن‌طور که انتظار می‌رود، سطح پوشش جدول را بالا نخواهند برد. نمودار سه بعدی این احتمال برحسب مقادیر مختلف t و d برای مقدار معین $N=2^{16}$ در شکل (۵) نشان داده شده است. همان طوری که در شکل واضح است، این نمودار برای $d=0$ همان نمودار شکل (۴)، در حالت نظری است.



شکل (۵). نمودار احتمالی عدم ادغام زنجیره‌ها برحسب پارامترهای d و t

۴- نتیجه‌گیری

در این مقاله به تحلیل رفتاری زنجیره‌های رمز هلمن و روش‌های مشابه آن، بر اساس گراف توابع تصادفی پرداخته و دیدیم که در مجموع می‌توان چند دلیل مهم برای رفتار نامطلوب این زنجیره‌ها (ادغام و حلقوی شدن) و در نتیجه پایین بودن سطح پوشش جداول هلمن ذکر کرد: ۱) وجود رئوس پایانه‌ای که امکان رخداد آن‌ها به‌جز در رأس آغازین یک زنجیره وجود ندارد، به‌طور کاملاً طبیعی باعث پایین آمدن سطح پوشش جدول‌ها می‌شود. ۲) جدول‌های هلمن با تغییر مقدار حالت پنهان ساخته می‌شوند که این تغییر باعث تغییر گراف تابع و در نتیجه تغییر رفتار آن به لحاظ ساخت زنجیره‌های رمز می‌شود. این تغییر می‌تواند به طور تقریباً یکسان (براساس یک توزیع نرمال) به افزایش احتمال ساخت یک زنجیره‌ی خوب و یاافزایش احتمال ساخت یک زنجیره بدرفتار منجر گردد. در ساخت زنجیره‌های هلمن به این مسئله توجهی نمی‌شود و حالات پنهان به‌طور تصادفی انتخاب می‌شوند. بدیهی است که انتخاب یک حالت پنهان نامناسب منجر به ساخت جدولی با سطح پوشش پایین می‌گردد. احتمال ساخت یک زنجیره غیردوری با طول حداقل t را به‌دست آوردیم. اگر برای انتخاب پارامتر t در ساخت زنجیره هلمن به این احتمال توجهی نشود، زنجیره‌های ساخته شده با احتمال زیاد در یک دور گرفتار شده و سطح پوشش آنها افزایش نخواهد یافت. همچنین احتمال ادغام زنجیره‌ها را به‌دست آورده و دیده شد که با افزایش طول و تعداد زنجیره‌ها این احتمال به طور نمایی بیشتر می‌شود. در ساخت زنجیره‌های هلمن به این احتمال توجهی نمی‌شود و بدیهی است که پس از ساخت چند زنجیره اول، افزایش پوشش جدول به سرعت به سمت صفر میل می‌کند و ساخت زنجیره‌های بعدی در عمل کار تقریباً بیهوده‌ای است و به حد مورد انتظار به افزایش سطح پوشش جدول منجر نمی‌شود. روش خود را به طور عملی روی الگوریتم رمز mAES پیاده‌سازی نموده و در هر قسمت دیدیم که نتایج نظری و عملی تاییدی بر یکدیگر هستند.

۵- مراجع

[1] M. E. Hellman, "A Cryptanalytic Time-Memory Trade Off," IEEE Transactions on Information Theory, vol. IT-26, no.4, JULY 1980.

[2] E. P. Barkan, "Cryptanalysis of Ciphers and Protocols," Research Thesis for the Degree of Doctor of Philosophy, Submitted to the Senate of the Technion-Computer Science Department, Ph.D. Thesis, 2006.

[3] D. E. Denning, "Cryptography and Data Security," p. 100, Addison-Wesley, Publishing Company, Boston, 1st edition, 1982.

[4] P. Oechslin, "Making a F. Aster Cryptanalytic Time-Memory Trade-Off," in Advances in Cryptology-CRYPTO 2003, vol. 2729 of Lecture Notes in Computer Science, pp. 617-630, Springer 2003.

[5] E. Barkan, E. Biham, and A. Shamir, "Rigorous bounds on cryptanalytic time/memory tradeoff," S. Inc. Dwork, editor, CRYPTO, vol. 4117 of Lecture Notes in Computer Science, pp. 1–21, Springer 2006.

[6] K. Nohl and C. Paget, "GSM-SRSLY," Congress slides during CCC 2009, retrieved from http:/events.ccc.de/congress/2009/F. Ahrplan/attachments/1519_26C3, Karsten. Nohl. GSM. Pdf, December 2009.

[7] K. Nohl, "Attacking phone privacy," Convention slides during Black Hat USA 2010, retrieved from https://media.blackhat.com/bh-us-10/whitepapers/Nohl/BlackHat-USA-2010-Nohl-Attacking- Phone.Privacy-wp.pdf, 2010.

[8] R. Chung-Wei Phan, "Mini Advanced Encryption Standard (Mini-AES): A Testbed for Cryptanalysis Students," Published in Cryptologia, XXVI (4), 2002.

[9] C. Cid, S. Murphy, and M. J. B. Robshaw, "Small Scale Variants of the AES," Information Security Group, Royal Holloway, University of London, Egham, Surrey, TW20 0EX, U.K, 2005.

[10] P. Flajolet and A. M. Odlyzko, "Random Mapping Statistics", in Advances in Cryptology- Eurocrypt'89, LNCS 434, pp. 329-354, 1990, Springer-Verlag Berlin Heidelberg 1990.

[11] R. Sedgewick and P. Flajolet, "An Introduction to the Analysis of Algorithms," Second Edition, Princeton University, INRIA Rocquencourt, Addison-Wesley, Library of Congress Control Number: 2012955493, 2013.

Journal Of Electronical & Cyber Defence
Vol. 4, No. 1, 2016, Serial No.13

Hellman Chains Analysis Base on Graph of Random Function

A. Mirghadri*, N. H. Gharavi, M. Abdollahi Azgomi, H. Soltani

*Imam Hossein University

(Received: 25/10/2015, Accepted: 03/05/2016)

ABSTRACT

Despite several studies and attempts, in time-memory trade-off attacks on cryptographic algorithms, the coverage of Hellman tables and similar methods are practically much less than half and their probability of success is low. In fact, Hellman chains are paths with given starting and end vertices on a functional graph. In this paper, behavior of these chains is investigated with this approach. In the beginning of the paper, parameters of the functional graph for a random mapping are defined and based on these parameters, Hellman chains are analyzed. Our results show that the coverage of such tables can't be high, for the following reasons: First, there exist some remarkable terminal vertices (37%) on the functional graph such that the possible occurrence of these vertices on chains (except in the starting vertices) is zero. Secondly, appropriate parameters for constructing chains exist in graph for about half of all hidden states of cipher function. Thirdly, for construction of noncyclic chains and collision of chains, we must pay attention to the obtained probabilities in this note.Practically, above reasons show that after some point the coverage of a Hellman table tends to zero quickly, and so construction of them will be ineffective. Our results are implemented on mAES algorithm where validate our theatrical results .

Keywords: Trade-off Attacks, Cipher Chains, RainbowTables, Random Functional Graph, Terminal Vertices, Hidden State.

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