

تحلیل روش مصالحه زمان - حافظه با استفاده از گراف تصادفی

عبدالرسول میرقدری*^۱، علی دینی^۲، ناصر حسین غروی^۳، عباسعلی فتحی‌زاده^۴

۱- دانشیار، ۲- کارشناس ارشد، ۳- دانشجوی دکتری، ۴- کارشناس ارشد، دانشگاه جامع امام حسین (ع)

(دریافت: ۹۵/۰۶/۲۹، پذیرش: ۹۶/۰۱/۲۴)

چکیده

در این مقاله، روش مصالحه زمان - حافظه (TMTO)، برای تحلیل رمزهای قالبی و روش‌های منطبق با آن بررسی می‌شود. همچنین، موضوع‌های پوشش در زنجیره‌های هلمن، تصادم در این زنجیره‌ها، دورها و طوقه‌هایی که در یک تابع رمز قالبی ایجاد می‌شود مورد بحث قرار می‌گیرند. برای تحلیل روش هلمن از گراف تصادفی استفاده می‌شود. گراف تصادفی از روی تابع رمز قالبی ساخته شده و از آن برای استخراج زنجیره‌های بدون تصادم، دورها و طوقه‌ها استفاده می‌شود. با توجه به حالت‌ها و ویژگی‌های یکتای گراف ساخته شده، یک روش جدید برای استخراج دورها و طوقه‌ها در گراف تصادفی تحت عنوان "چابک‌سازی گراف" ارائه می‌شود. این روش به آسانی و با هزینه خیلی کم، دورها و طوقه‌های موجود در تابع رمز قالبی را استخراج می‌کند. دورها و طوقه‌های به‌دست آمده، برای تولید زنجیره‌های بدون تصادم در رمزهای قالبی مورد استفاده قرار گرفته و باعث پوشش کامل کلیدهای رمز قالبی در روش TMTO می‌شوند.

واژه‌های کلیدی: گراف جهت‌دار، گراف تصادفی، زنجیره بدون تصادم، روش مصالحه، رمز قالبی

۱- مقدمه

روش مصالحه حافظه- زمان (TMTO)^۱ در سال ۱۹۸۰ توسط هلمن ارائه شد [۱]. ایشان پیشنهاد کردند با ذخیره کردن داده‌های پیش‌پردازش شده در حافظه، می‌توان بین زمان و حافظه نوعی مصالحه برقرار کرد [۲]. ایده هلمن، در بررسی روش‌های تجزیه و تحلیل سیستم‌های رمز از جمله رمز قالبی که به مثابه "جعبه سیاه" می‌ماند، نیز کاربرد دارد [۳]. در این روش، توابع یک‌طرفه الگوریتم‌های رمز را طوری می‌نویسند که وارونگی داشته باشند. تابع یک‌طرفه رمز قالبی با نماد $f(x) = E_x(m)$ نوشته می‌شود که E، K و m به ترتیب الگوریتم رمز گذاری، کلید و متن اصلی (معلوم) هستند و مقادیر x و $f(x)$ ، از مجموعه $N = \{0, 1, \dots, N-1\}$ انتخاب می‌شوند [۴]. روش ساده تحلیل رمز قالبی، روش جستجوی کامل فضای کلید آن است که هر پیش‌تصویر $f(x)$ را با آزمودن تمام پیش‌تصویرهای ممکن x' به‌دست آورده و بررسی می‌شود که آیا $f(x') = f(x)$ است یا نه [۱]؟ با استفاده از تعداد اجراهای f، مقدار پیچیدگی زمان (T) محاسبه می‌شود که بدترین حالت در جستجوی کامل، N و بدترین حالت پیچیدگی فضای مقدار خیلی ناچیز M می‌شود [۴]. روش دیگر تحلیل رمز قالبی جستجوی لغت‌نامه است که همه

تصاویر و پیش‌تصاویر نظیر را به‌دست آورده و از پیش‌تصویرها و تصویرهای به‌دست آمده، هر کدام یکی را ذخیره می‌کنیم و در جدول خیلی بزرگ نگهداری می‌شود [۱]. این فرض مستلزم دو مرحله پیش‌پردازش و اجرا است که در مرحله پیش‌پردازش هم فضا و هم زمان، پیچیدگی را برابر با N در نظر گرفته و در مرحله اجرا، فضای پیچیدگی را برابر با M (تقریباً برابر با N) و پیچیدگی زمان را مقدار خیلی ناچیز T در نظر گرفته می‌شود [۲]. در روش هلمن، با فرض انجام مرحله پیش‌پردازش با استفاده از مصالحه زمان/ حافظه میان روش‌های جستجو به یک توافق رسیده و میان پیچیدگی‌های زمان، حافظه و داده در مرحله اجرا مصالحه‌ای ایجاد می‌شود [۳]. با توجه به ویژگی خاص الگوریتم رمز قالبی، در تولید زنجیره‌ها با طول و تعداد مشخص با تصادمی مواجه شده که حدود نیمی از کلیدهای رمز را پوشش می‌دهد [۱ و ۵]. از گراف تصادفی برای بررسی روش هلمن استفاده کرده و به بررسی تولید زنجیره‌های بدون تصادم و استخراج دورها پرداخته می‌شود که در سال‌های اخیر مورد توجه تحلیل‌گران حوزه رمزشناسی نیز قرار گرفته است [۶-۷]. با توجه به بررسی‌های اولیه انجام شده، بررسی حالت‌های گراف تصادفی جهت‌دار و استخراج دورها و بهبود اساسی حمله نیاز اصلی این تحقیق است [۴ و ۸]. برای تحقق این امر، از مدل توزیع توپ و ظرف استفاده کرده و با تشکیل روش مصالحه در رمز قالبی، حالت‌های ایجاد شده، استخراج می‌شوند [۹].

* رایانامه نویسنده مسئول: amrghdri@ihu.ac.ir

1- Time Memory Trade Off (TMTO)

2- Black-box

۲-۱- بیان مسئله

با در نظر گرفتن حالت اول مدل توزیع توپ‌ها در ظرف، فرض کنید r توپ در n ظرف متمایز با شماره‌های $1, 2, \dots, n$ توزیع می‌شوند. بر اساس شرایط متفاوت توپ‌ها و تعداد توپی که در هر ظرف قرار می‌گیرد، مدل مربوطه شش حالت متفاوت به خود می‌گیرد [۹]. در این مقاله، از حالت‌های مختلف مدل توپ و ظرف، حالتی که توپ‌ها متمایز هستند و از نظر قرار گرفتن تعداد توپ در هر ظرف محدودیتی وجود ندارد را مورد بررسی قرار می‌دهیم. توپ اول، n انتخاب ممکن برای ظرف دارد، توپ دوم هم n انتخاب، ... و توپ آخر نیز n انتخاب از میان ظرف‌ها دارد. پس بنا به اصل ضرب، تعداد حالات ممکن برابر با n^r می‌شود [۹]. در این مدل، تعداد توپ و ظرف را یکسان فرض کرده و توپ‌ها و ظرف‌ها را شماره‌دار و به شماره‌های $1, 2, \dots, n$ در نظر می‌گیریم. فرض می‌شود 2^n توپ را به‌طور یکنواخت در 2^n ظرف توزیع شده‌اند. برای یافتن مکان توپ‌ها در ظرف‌ها یا برای یافتن شماره توپ در ظرف‌ها نیاز به جستجوی کامل تمام 2^n حالت را داریم [۱۰]. برای یافتن یک روش جستجوی بهینه، از روش هلمن استفاده می‌شود. برای داشتن پوشش کامل در مرحله پیش‌پردازش و میزان موفقیت کامل در زمان اجرا به تحقیق و بررسی روش هلمن بر اساس گراف تصادفی پرداخته می‌شود.

۳- مفاهیم اساسی

در این بخش، مفاهیم اساسی مرتبط با گراف تصادفی و روش مصالحه هلمن معرفی می‌شوند.

۳-۱- مفهوم گراف تصادفی

گراف تصادفی را با یک پدیده شهودی و ساده احتمال یعنی با پرتاب سکه آغاز می‌کنیم. با این فرض که n نقطه در فضا در اختیار داریم، اگر احتمال رو آمدن سکه را p در نظر بگیریم، با همین احتمال p دو نقطه دلخواه از n نقطه در فضا را انتخاب نموده و به هم متصل می‌کنیم تا یک یال گراف مشخص شود. برای روشن شدن مطلب، حالت‌های خاص n, p در شکل‌های (۱) تا (۶) در زیر نشان داده شده‌اند [۱۲]:

▪ حالت اول: در حالتی که $n = 2$ و $p = 0$ است، دو نقطه تنها (ایزوله) به صورت شکل زیر داریم:



شکل (۱): رأس ایزوله در حالت $n = 2$ و $p = 0$

سپس با استفاده از حالت‌های به‌دست‌آمده، الگوریتم نحوه استخراج دور در این نوع گراف‌های تصادفی را ارائه می‌دهیم.

ساختار مقاله به این شرح است که ابتدا مفاهیم و تعاریف بیان شده و سپس در بخش دوم، کارهای مرتبط توضیح داده می‌شود. مفاهیم اساسی گراف در بخش سوم بیان می‌شوند. در بخش چهارم، حالت‌های گراف تصادفی در روش مصالحه را بر اساس مدل توزیع توپ و ظرف به‌دست‌آورده و در بخش پنجم، از روی این حالت‌ها یک الگوریتم جدید "روش چابک‌سازی گراف" برای استخراج دورها ارائه می‌شود. در نهایت، در بخش ششم به نتایج و پیشنهادات پرداخته می‌شود.

۲- کارهای مرتبط

در مقاله [۸]، دو بهبود اساسی بر روی حمله TMTO هلمن صورت گرفته است. بهبود اول روی کار هلمن در DES توسط ریوست^۱ با معرفی نقاط تمایز^۲ (DP) به منظور کاهش تعداد جداول جستجو در سال ۲۰۰۱ انجام شد. در ادامه، برست^۳ با معرفی احتمال موفقیت و پیچیدگی برای نقاط متمایز (DP) مبنی بر بالابودن احتمال موفقیت DP در کاربردهای عملی این روش را در سال ۲۰۰۲ بهبود داد. این بهبودها، برای ساخت و طراحی یک مصالحه واقع‌بینانه برای پیاده‌سازی رمز قالبی DES روی FPGA، با استفاده از توابع پوششی انجام گرفت.

اوکلین^۴ با معرفی جداول رین‌باو^۵ و پیشنهاد استفاده از توابع کاهنده متوالی در هر ستون زنجیره‌ها، روش هلمن در سال ۲۰۰۳ بهبود داد و یک بهبود اساسی دیگری نیز تحت عنوان مدل گراف تصادفی حالت‌پذیر روی حمله TMTO انجام گرفته است [۱۰ و ۸].

در نهایت، بهبودی جامع توسط بارکان^۶، بیهام^۷، شامیر^۸ با معرفی مدل گراف تصادفی حالت‌پذیر به منظور پوشش بهبودهای قبلی و هر طرح دیگر سازگار با این مدل در سال ۲۰۰۶ ارائه گردید [۶].

- 1- Rivest
- 2- Distinguished Points (DP)
- 3- Borest
- 4- Oechslin
- 5- RainBow
- 6- Barkan
- 7- Biham
- 8- Shamir

می‌شود. در این حالت، تعداد گراف‌هایی از این دست برابر با $4 \binom{n}{2}$ می‌باشد [۶]. حالت خاص n و p را برای گراف جهت‌دار نیز در شکل‌های زیر نشان داده شده است.

▪ حالت اول: در حالتی که $n = 2$ و $p = 0$ است، دو طوقه داریم.



شکل (۴): دو رأس طوقه‌دار در گراف تصادفی با حالت $p = 0$ و $n = 2$

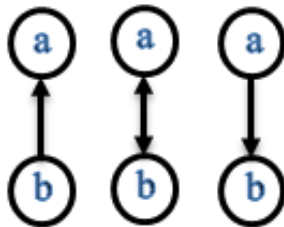
▪ حالت دوم: در حالتی که $n = 2$ و $p = \frac{1}{2}$ است، چهار حالت می‌تواند اتفاق بیفتد.

✓ دو طوقه



شکل (۵): دو رأس طوقه‌دار در گراف تصادفی با حالت $n = 2$ و $p = \frac{1}{2}$

✓ دو رأس مجاور با جهت‌های متفاوت



شکل (۶): دو رأس مجاور در گراف تصادفی جهت‌دار با حالت $n = 2$ و $p = \frac{1}{2}$

۳-۲- روش مصالحه هلمن

هلمن رمز قالبی DES را با روش $TMTO$ تحلیل کرد. با این روش، در هر سیستم رمزی که فضای کلید N عضوی دارد، می‌توان $N^{2/3}$ کلمه حافظه ساخت و با $N^{2/3}$ عملیات، کلید یک قالب متن رمز را جستجو و پیدا کرد [۵]. به‌طور معمول کلمات حافظه، بعد از انجام پیش‌پردازش، حاصل می‌شوند و عمل پیش‌پردازش مستلزم تعداد N عمل است. هلمن همچنین اظهار داشت که این روش با استفاده از یک تابع یک‌طرفه از طریق

▪ حالت دوم: در حالتی که $n = 2$ و $p = \frac{1}{2}$ است، دو حالت می‌تواند اتفاق بیفتد [۱۲]:

✓ حالت اول با احتمال $p = \frac{1}{2}$ دو نقطه تنها داریم.



شکل (۲): رأس ایزوله در حالت $n = 2$ و $p = \frac{1}{2}$

✓ حالت دوم با احتمال $p = \frac{1}{2}$ این دو رأس به هم متصل می‌شوند.



شکل (۳): دو رأس هم‌جوار در حالت $n = 2$ و $p = \frac{1}{2}$

چون با تغییر $0 \leq p \leq 1$ ، گراف‌هایی از نوع تهی تا کامل تولید می‌گردند. لذا، گراف‌های تصادفی تولید می‌شوند که برای n نقطه شماره‌دار، تعداد گراف‌های از این نوع برابر با $2 \binom{n}{2}$ می‌باشد. زیرا به تعداد $\binom{n}{2}$ طریق دو نقطه مذکور انتخاب شده و هر انتخاب می‌تواند دو حالت داشته باشد. یعنی دو رأس به هم متصل می‌شوند یا نمی‌شوند یا به‌عبارتی، دو رأس می‌توانند مجاور باشند یا نباشند. نکته قابل ذکر این است که در روند بالا، فرض شده است که گراف ساده است. اگر گراف جهت‌دار باشد، در این حالت تعداد گراف‌های از این دست برابر $4 \binom{n}{2}$ می‌شود زیرا در این حالت، بعد از انتخاب دو نقطه به تعداد $\binom{n}{2}$ طریق، سه حالت ممکن است به‌وجود آید.

(۱) دو رأس مجاور نباشند (یعنی یالی بین دو رأس انتخاب‌شده ایجاد نشود).

(۲) دو رأس مجاور بوده و جهت یک‌طرفه (یعنی فقط $u \rightarrow v$ یا $v \rightarrow u$ برقرار شود) باشد که این خود دو حالت را شامل می‌شود.

(۳) دو رأس مجاور بوده و جهت دوطرفه ($u \leftrightarrow v$) باشد. نکته‌ای که قابل ذکر است اگر جهت‌دار بودن یا نبودن نیز اختیاری باشد علاوه بر چهار حالت مذکور، یک حالت نیز به حالات ممکن افزوده

دارد به تعداد کلیدهای متمایزی که در مرحله پیش‌پردازش به دست آمده‌اند [۴].

۴- حالت‌های گراف تصادفی جهت‌دار براساس مدل توپ و ظرف

در این قسمت، با استفاده از مدل توزیع توپ در ظرف‌ها، روش مصالحه حافظه و زمان هلمن در رمزهای قالبی را براساس گراف تصادفی بیان می‌شود. روشی برای تولید زنجیره‌های بدون تصادم ارائه می‌شود. با توجه به این که بسیاری از مسائل آنالیز ترکیبی با مدل توزیع توپ‌ها در ظرف‌ها قابل بیان می‌باشند، لذا با گراف تصادفی جهت‌دار می‌توان از طریق این مدل، الگوریتم رمز را تحلیل کرد [۹]. به‌طور مثال، اگر $n = 16$ باشد و فرض کنیم که با احتمال یکنواخت توپ‌ها در ظرف‌ها توزیع شده‌اند، لذا مطابق جدول (۱) داریم:

جدول (۱): توزیع توپ در ظرف

۷	۶	۵	۴	۳	۲	۱	۰	توپ‌ها
9	A	8	B	7	5	2	9	ظرف‌ها
F	E	D	C	B	A	۹	8	توپ‌ها
0	5	8	7	3	A	1	2	ظرف‌ها

مطابق جدول می‌گوییم که، توپ شماره یک، دو، سه و الی آخر به ترتیب در ظرف‌هایی با شماره ۲، ۵، ۷ و الی آخر قرار می‌گیرند. حال می‌توان مجموعه فضای حالت توپ‌ها را A و مجموعه فضای حالت ظرف‌ها را B نامیده و یک تابع f به صورت $f: A \rightarrow B$ تعریف می‌کنیم.

با تعمیم مدل توپ و ظرف به گراف‌های تصادفی، توابع مصالحه و توابع رمزهای قالبی بدین ترتیب شکل می‌گیرند که در گراف‌های تصادفی، یال‌ها را توپ‌ها و رأس‌ها را ظرف‌ها در نظر می‌گیرند [۱۳]. در تابع رمزهای قالبی، کلیدها را توپ‌ها و قالب متن رمزی را ظرف‌ها فرض کرده و در توابع مصالحه کلیدها را توپ‌ها و قالب متن رمزی را ظرف‌ها فرض می‌کنیم.

مدل گراف تصادفی اردوش را برای تابع مصالحه در نظر می‌گیریم [۱۱]. از روی مدل گراف تصادفی اردوش گراف تصادفی $(V(D), A(D), \psi_D)$ را که در آن D یک گراف تصادفی جهت‌دار، V نشان‌دهنده رأس‌ها، A نشان‌دهنده یال‌ها و ψ نشان‌دهنده تابع $TMTO$ ی که رأس‌های متمایز را مجاور و رأس‌های غیرمتمایز را طوقه‌دار می‌کند، د نظر می‌گیریم [۱۳]. حال اگر

وارونگی^۱ قابل انجام است. روش $TMTO$ ، هلمن را به صورت زیر تشریح می‌کند [۱].

فرض کنید تابع زیر یک تابع رمزگذاری باشد:

$$E: k * p \rightarrow c$$

که در آن، $c \in \{0, 1\}^n$ ، $k \in \{0, 1\}^n$ ، $p \in \{0, 1\}^n$ به ترتیب معرف متن رمز، کلید مخفی و متن اصلی هستند. رمزگذاری یک قالب به صورت $c = E_x(p)$ یا $c = E(x, p)$ تعریف می‌شود.

رابطه $c = E(x, p)$ را در نظر می‌گیریم که در آن، p یک قالب متن اصلی ثابت و c متن رمز متناظر با آن است و هدف اصلی، بازیابی کلید $x \in K$ می‌باشد. با فرض این که $k = n$ است مراحل پیش‌پردازش و اجرا به شرح ذیل می‌باشند.

۳-۲-۱- مرحله پیش پردازش

در جدول هلمن، با شروع از یک نقطه تصادفی مانند x یک زنجیره به طول t به صورت $x_1 \rightarrow x_2 \rightarrow \dots \rightarrow x_t$ تولید می‌شود [۴].

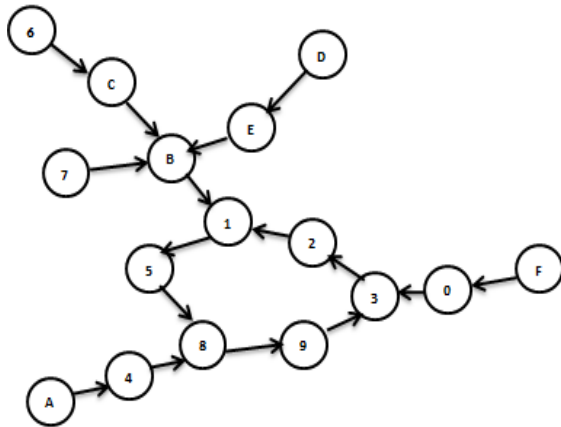
برای ساختن یک جدول هلمن در اندازه $m \times t$ ابتدا m نقطه تصادفی به عنوان نقاط شروع انتخاب می‌شوند که اولین عنصر در یک زنجیره را نقطه شروع و آخرین عنصر یک زنجیره را نقطه پایانی می‌نامند. با دانستن نقطه شروع، عناصر زنجیره پی‌درپی محاسبه می‌شوند [۳]. همچنین، به‌منظور بالا بردن سرعت جستجو در زمان اجرا، جداول نسبت به نقاط پایانی مرتب می‌شوند.

۳-۲-۲- مرحله زمان اجرا

در این مرحله، هدف یافتن پیش‌تصویر یک قالب متن رمز c است به شرطی که کلید استفاده‌شده برای تولید c در میان جداول تولیدشده، وجود داشته باشد. با اعمال مکرر f روی c به همراه عمل رمزگذاری، یک زنجیره توسط c تولید کرده و مقدار به دست آمده در هر بند از زنجیره را با نقاط پایانی همه جداول مقایسه می‌کنیم [۲]. اگر تطابقی پیدا شد، از روی نقطه آغازین، اقدام به تولید مجدد زنجیره متناظر کرده و کلید مورد نظر را با جستجوی کامل پیدا می‌کنیم. توجه داشته باشید که مواقعی پیش می‌آید که کلید مدنظر در نودهایی از زنجیره پیدا می‌شوند که با زنجیره‌های دیگر جداول تصادم دارند. لذا، در چنین مواقعی با خطا مواجه می‌شویم. بنابراین، میزان موفقیت حمله بستگی

❖ **گراف تصادفی جهت‌دار تک مولفه‌ای**

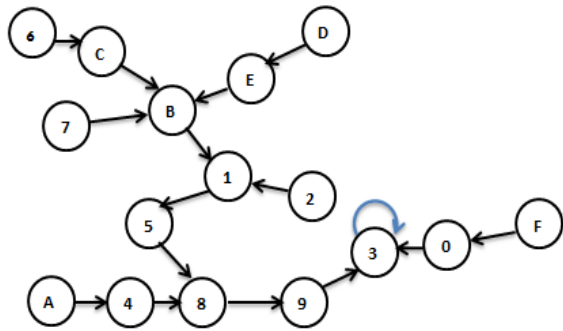
اگر در گراف تصادفی جهت‌دار جهت یال‌ها را برداریم لذا گراف به یک گراف همبند کامل تبدیل می‌شود. ممکن است چنین گراف تصادفی یکپارچه دارای دور و طوقه نیز باشد که در شکل زیر آن را مشاهده می‌کنید.



شکل (۷): گراف تصادفی جهت‌دار دوردار و بدون طوقه

دور گراف فوق عبارت است از: $1 \rightarrow 5 \rightarrow 8 \rightarrow 9 \rightarrow 3 \rightarrow 2 \rightarrow 1$

اگر گراف جهت‌دار را به صورت یکپارچه و طوقه‌دار نشان دهیم لذا گراف بالا به شکل زیر می‌باشد.



شکل (۸): گراف تصادفی دوردار و طوقه‌دار

طوقه در گراف فوق عبارت است از: $3 \rightarrow 3$

همان‌طور که در دو شکل (۷-۸) ملاحظه می‌کنید، دور و طوقه بر روی گراف فراگیر یکپارچه قرار دارند.

❖ **گراف تصادفی جهت‌دار چندمولفه‌ای**

در اشکال (۹-۱۰) در زیرگراف تصادفی جهت‌دار که شامل مولفه‌های یکپارچه و طوقه‌دار و دوردار هست، نشان داده شده است.

جدول (۱) در بالا را در نظر بگیریم، گراف تصادفی جهت‌داری می‌شود که ۱۶ رأس و ۱۴ یال ثابت دارد.

$$V(D) = \{0, 1, 2, \dots, C, D, E, F\}$$

$$A(D) = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9, e_A, e_B, e_C, e_D, e_E\}$$

و ψ_D برابر است با

$$\begin{aligned} \psi_D(e_1) &= E0, \psi_D(e_2) = 09, \psi_D(e_3) = 4B, \psi_H(e_4) = B3, \\ \psi_H(e_5) &= 37, \psi_H(e_6) = 79, \psi_H(e_7) = 91, \psi_H(e_8) = 12, \\ \psi_H(e_9) &= 25, \psi_H(e_A) = E5, \psi_H(e_B) = 58, \psi_H(e_C) = 8C, \\ \psi_H(e_D) &= 82 \end{aligned}$$

در مسئله انداختن m توپ در n ظرف به صورت یکنواخت و مستقل با سوالات زیر مواجه می‌شویم [۱۳]:

(الف) توزیع توپ‌ها چیست؟

(ب) چند تا ظرف خالی داریم؟

(ج) بیشترین تعداد توپ در یک ظرف چقدر است؟

اگر سوالات بالا را براساس گراف تصادفی جهت‌دار تفسیر کنید با مسئله قرارگرفتن m یال در n رأس به صورت یکنواخت و مستقل مواجه شده و باید به سوالات زیر پاسخ بدهید.

۱- توزیع یال‌ها چیست؟

۲- چند تا رأس درجه ورودی صفر داریم؟

۳- بیشترین تعداد یال‌ها در یک رأس چقدر است؟

برای پاسخ به این سوالات، به تحقیقاتی که در زمینه توزیع آماری نگاشت تصادفی انجام شده است، مراجعه کنید [۲ و ۳ و ۸]. که آقای هلمن نیز در تحقیقاتش از آن‌ها استفاده کرده است [۲]. با توجه به حالت گفته‌شده از مدل توپ و ظرف، گراف تصادفی به دست آمده در این تحقیق، از نظر پراکندگی فرق کرده و در کل دو حالت از گراف تصادفی جهت‌دار را پدید می‌آورد که دلیل به وجود آمدن این دو حالت عبارتند از:

- انداخته شدن همه توپ‌ها درون ظرف‌ها
- احتمال خالی ماندن بعضی ظرف‌ها
- قرارگرفتن بعضی توپ‌ها در ظرف‌های هم ترتیب و هم شماره

در زیر این دو حالت از گراف تصادفی جهت‌دار معرفی می‌شوند.

۵- الگوریتم یافتن دورها "روش چاپک‌سازی گراف"

در این تحقیق، روی حالت‌های مختلف گراف تصادفی حاصل شده در بخش چهارم بررسی‌هایی انجام شد که با حذف رأس‌های درجه صفر از گراف توانستیم به مولفه‌هایی از گراف برسیم که همگی دوره‌های توابع مصالحه هستند. لذا، این روش را "چاپک‌سازی گراف" نامیده و الگوریتمی برای آن ساخته‌ایم.

برای یافتن دورها در گراف روش‌ها و الگوریتم‌های مختلفی ارائه شده‌اند. الگوریتم‌های فلویید^۱، پولارد^۲، برنت^۳ و یائو^۴ [۶] برای یافتن دور مورد استفاده قرار می‌گیرند. نحوه کار همه این الگوریتم‌ها براساس یافتن دو نود هم‌نام در مسیری از گراف می‌باشد. هر الگوریتم این عمل را با روش خاص خود و متفاوت از دیگری انجام می‌دهد. نحوه یافتن دور در الگوریتم پیشنهادی متفاوت از این الگوریتم‌ها می‌باشد که در یافتن دوره‌های گراف‌های تصادفی جهت‌دار کارایی بهینه دارد. این روش را تحت عنوان الگوریتم "چاپک‌سازی گراف" ارائه داده و از آن در یافتن دورها استفاده می‌کنیم. الگوریتم پیشنهادی به شکل زیر می‌باشد:

1. while zero_indegree
 - a. zero_indegree=[indegree(node)==0]
 - b. remove_nodes(zero_indegree)
2. data=[nodes(indegree and outdegree==1)]

الگوریتم یافتن دورها در گراف تصادفی جهت‌دار را به شکل

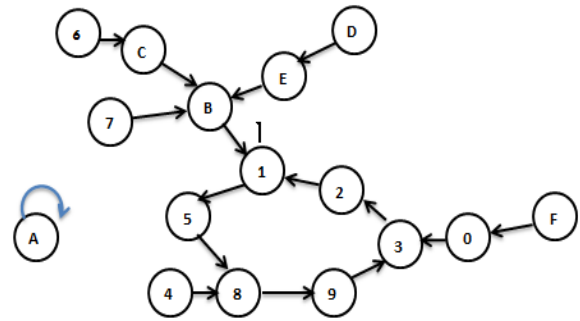
زیر شرح می‌دهیم:

- ۱- فرض می‌شود گراف تابع مصالحه تشکیل شده است.
- ۲- یک حلقه به نحوی تعریف می‌کنیم که همه رأس‌های با درجه صفر را پیمایش کرده و آن‌ها را از گراف حذف کند.
- ۳- حلقه را تا جایی که هیچ رأس با درجه ورودی صفر در گراف وجود نداشته باشد ادامه می‌دهیم.
- ۴- مولفه‌های مانده از گراف همگی دور یا طوقه هستند.

با در نظر گرفتن چند گراف فراگیر، دوره‌های آن‌ها را استخراج می‌کنیم.

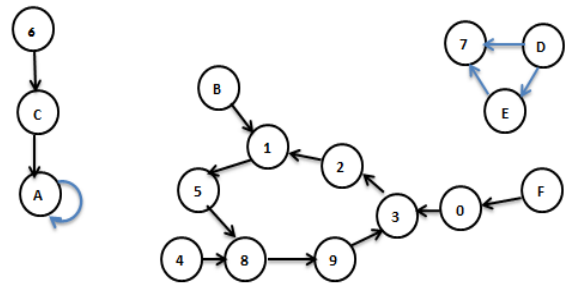
گراف اول مربوط به تابع مفروضی است که ۱۶ توپ را براساس آن در ۱۶ ظرف توزیع می‌کنیم. گراف فراگیر آن را در زیر شکل (۱۱) مشاهده می‌کنید.

تابع مفروض گراف فراگیر مقادیر عددی است که در جدول (۲)



شکل (۹): گراف تصادفی جهت‌دار با دو مولفه

همان‌طور که ملاحظه می‌شود گراف فراگیر شکل (۹) شامل یک مولفه یکپارچه و یک مولفه طوقه‌دار با طوقه $A \rightarrow A$ است. در شکل (۱۰) نیز یک گراف فراگیر شامل سه مولفه یکپارچه را نشان می‌دهد.



شکل (۱۰): گراف تصادفی با سه مولفه

دور در گراف فراگیر عبارت است از $D \rightarrow 7 \rightarrow E$.

در تحقیق حاضر، تنها با این دو حالت از گراف‌ها مواجه می‌شویم. آن‌ها گراف جهت‌دار تصادفی هستند که ویژگی‌های منحصر به فردی دارند. در مدل حاضر، ظرف‌هایی که هیچ توپی در خود جای ندادند و ظرف‌هایی که بیشتر از یک توپ در خود جای دادند، برای ما حائز اهمیت هستند. تناظر آن‌ها در گراف تصادفی رأس‌هایی هستند با درجه ورودی صفر و درجه خروجی بیشتر از یک. به عبارتی، رأس‌های با درجه ورودی صفر، ظرف‌های خالی هستند که هیچ توپی را در خود جای ندادند. رأس‌ها با درجه خروجی بیشتر از یک، ظرف‌هایی هستند که بیش از یک توپ در خود جای داده‌اند. با توجه به زنجیره‌های هلمن، بهترین نقاط برای شروع یک زنجیره نقطه‌ای است که پیش‌تصویر ندارد [۲]. تناظر این نقاط در گراف تصادفی جهت‌دار، رأس‌هایی هستند که درجه ورودی آنها صفر است. بنابراین، بهترین رأس برای شروع یک زنجیره رأسی است که درجه ورودی صفر دارد.

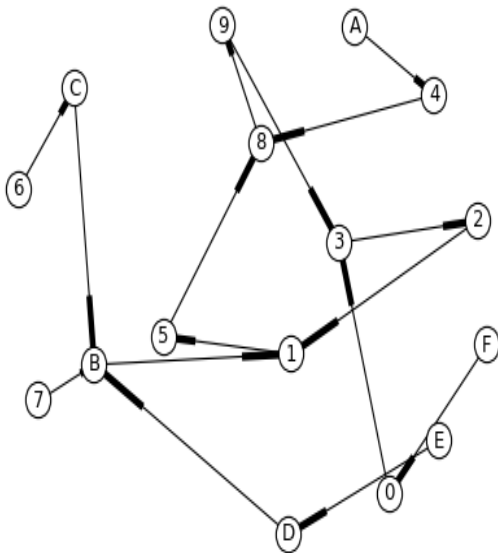
1- Floyd
2- Polard
3- Berent
4- Yao

گراف فراگیر دوم که از روی تابع مفروضی که ۱۶ توپ بر اساس آن در ۱۶ ظرف توزیع می‌شوند، ساخته شده در زیر مشاهده می‌شود. دوره‌های گراف با الگوریتم چابک‌سازی گراف پیدا شده‌اند که در شکل (۱۳) در زیر مشاهده می‌شوند.

مقادیر تابع مفروض گراف فراگیر دوم در جدول (۳) در زیر مشخص شده است:

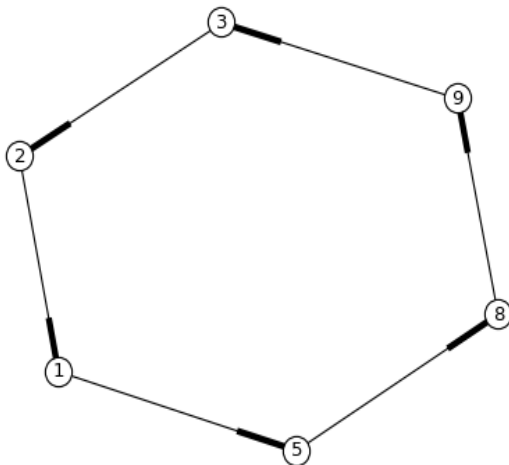
جدول (۳): توزیع ۱۶ توپ در ۱۶ ظرف

X	۰	۱	۲	۳	۴	۵	۶	۷
H(X)	۳	۵	۱	۲	۸	۸	C	B
X	۸	۹	A	B	C	D	E	F
H(X)	۹	۳	۴	۱	B	B	D	۰



شکل (۱۳): گراف فراگیر دوم

دوره‌های گراف فراگیر دوم عبارت است از شکل (۱۴):



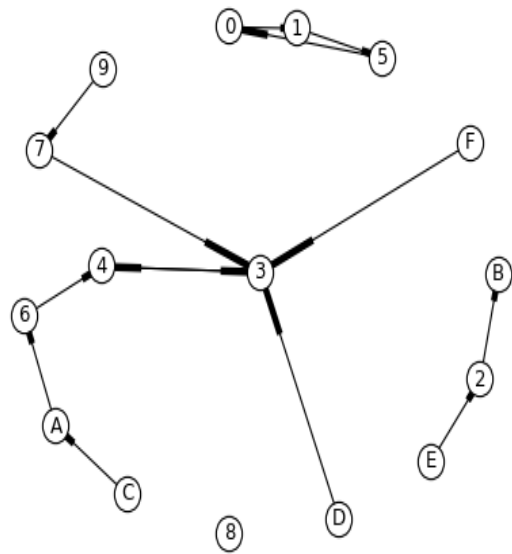
شکل (۱۴): دور در گراف فراگیر دوم

دیده می‌شود:

جدول (۲): توزیع ۱۶ توپ در ۱۶ ظرف

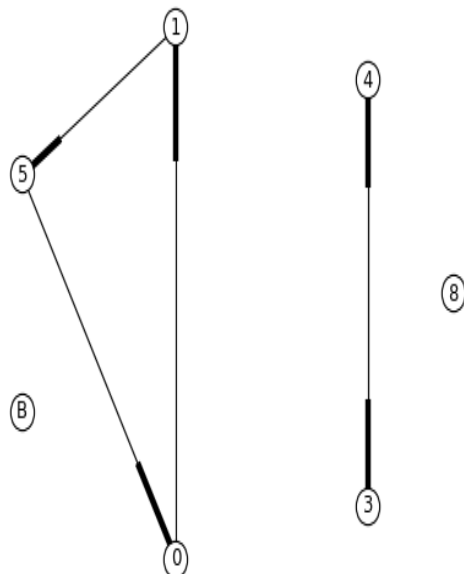
X	0	1	2	3	4	5	6	7
H(X)	1	5	B	4	3	0	4	3
X	8	9	A	B	C	D	E	F
H(X)	8	7	6	B	A	3	2	3

گراف فراگیر تابع مفروض بالا در شکل (۱۱) در زیر رسم شده است:



شکل (۱۱): گراف فراگیر اول

همان‌طور که ملاحظه می‌کنید چهار مولفه شامل دوره‌ها و طوقه‌ها استخراج شده که در شکل (۱۲) دیده می‌شود.



شکل (۱۲): دوره‌ها و طوقه‌های گراف فراگیر اول

۶- بحث و نتایج

در سال ۲۰۰۶ بارکان و همکارانش روش هلمن و تمام روش‌های منطبق با آن را با نظریه گراف بررسی کرده و نتیجه گرفتند که همه این روش‌ها ریشه در نظریه گراف دارد. آنها با استفاده از گراف تصادفی به ویژگی‌های یک تابع رمز قالبی پرداختند و مدلی را ارائه دادند که همه روش‌های طرح شده تا سال ۲۰۰۶ و یا هر مدل دیگر منطبق با این مدل را پوشش می‌دهد. ما برای بهبود روش هلمن بر اساس گراف تصادفی از مدل توزیع و توپ استفاده کرده و همه مدل‌هایی که این روش روی گراف تصادفی ایجاد می‌کند را استخراج کردیم. از روی این مدل‌ها و بررسی ویژگی آنها روشی جدید تحت عنوان "چابک سازی گراف" برای استخراج دورها و طوقه‌ها ارائه دادیم که با توجه به شکل‌ها و جداول فوق، دیده می‌شود با روش چابک‌سازی گراف تصادفی، دورها و طوقه‌ها در توابع مصالحه برای تولید زنجیره‌های بدون تصادم به‌سادگی و به نحو کارا مشخص می‌شوند. همچنین، گراف تصادفی ساخته شده در روش جدید، کل دامنه تابع رمز قالبی را پوشش می‌دهد. این روش در تولید زنجیره‌های بدون تصادم موثر بوده و در نحوه یافتن دورها و طوقه‌ها در تابع مصالحه نسبت به سایر روش‌های موجود متفاوت و بهتر عمل می‌کند. لذا این روش باعث افزایش پوشش کلید رمز قالبی هم در مرحله پیش‌پردازش و هم در مرحله اجرا می‌شود.

۷- نتیجه‌گیری

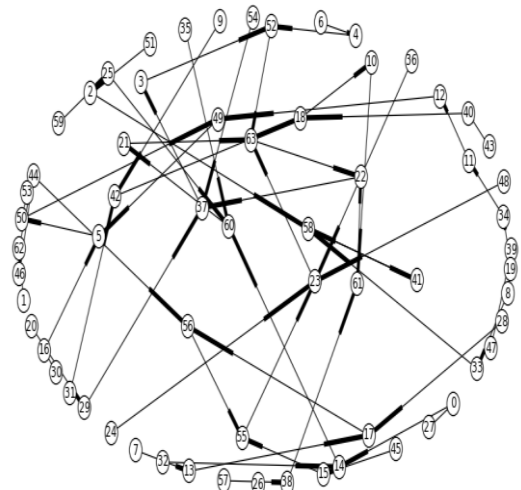
در این تحقیق روش مصالحه زمان-حافظه (TMTO) که اولین بار توسط هلمن برای تحلیل رمزهای قالبی استفاده شد، مورد بررسی قرار گرفت. هلمن از روی کلید و متن رمز زنجیره‌هایی ساخت و با ذخیره‌سازی نقاط شروع و نقاط پایانی زنجیره‌ها در حافظه، نوعی مصالحه میان زمان و حافظه برقرار کرد. اشکال این روش پوشش ندادن کل دامنه تابع رمز قالبی است. روش‌هایی که در توسعه و بهبود روش هلمن ارائه شدند همگی در کاهش حافظه ذخیره‌سازی و افزایش درصد پوشش کلید رمز قالبی نقش داشتند اما به تنهایی پوشش صد در صد نداشتند. ما برای بررسی مجدد و بهبود روش هلمن بر اساس گراف تصادفی از مدل توزیع و توپ استفاده کرده و همه مدل‌هایی که این روش روی گراف تصادفی ایجاد می‌کند را استخراج کردیم. از روی این مدل‌ها و بررسی ویژگی آنها روشی جدید تحت عنوان "چابک سازی گراف" برای استخراج دورها و طوقه‌ها ارائه شد. باید توجه داشت

گراف سوم مربوط می‌شود به تابع مفروضی که براساس آن ۶۴ توپ را در ۶۴ ظرف توزیع می‌کنیم. گراف فراگیر آن در جدول (۴) در زیر مشاهده می‌شود.

جدول (۴): توزیع ۶۴ توپ در ۶۴ ظرف

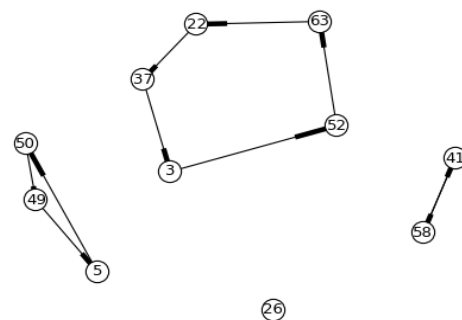
X	0	1	2	3	4	5	6	7
H(x)	14	62	58	52	52	50	4	13
X	16	17	18	19	20	21	22	23
H(X)	5	56	10	34	29	63	37	63
X	32	33	34	35	36	37	38	39
H(x)	14	58	11	60	23	3	61	8
X	48	49	50	51	52	53	54	55
H(x)	23	5	49	2	63	50	37	23
X	8	9	10	11	12	13	14	15
H(x)	33	42	61	12	49	17	60	55
X	24	25	26	27	28	29	30	31
H(X)	23	60	26	0	17	37	16	42
X	40	41	42	43	44	45	46	47
H(x)	18	58	18	40	56	15	44	39
X	56	57	58	59	60	61	62	63
H(x)	55	38	41	25	21	22	44	22

تابع مفروض گراف سوم عبارت است از:



شکل (۱۵): گراف فراگیر سوم

همان‌طور که ملاحظه می‌کنید، دورها و طوقه‌های حاصل شده از گراف فراگیر سوم به صورت زیر می‌باشند:



شکل (۱۶): دورها و طوقه در گراف فراگیر سوم

- [5] M. Sourav, "A study on time/memory trade off cryptanalysis," Applied Statistical Unit Indian Statistical 203, B. T. Road, Calcutta 700 108, INDIA, March 2006.
- [6] A. Shamir, "Random Graph in Security and Privacy," The Weizmann Institute, Hifa, June 2010.
- [7] A. Shamir, "Random Graph in Cryptography," The Weizmann Institute L..., Haifa, May 2007.
- [8] A. Doganakosy and S. Nurdan, "Variant Constructions for TMTO based on Random Mapping Statistics," in 3rd Information Security & Cryptology Conferece With International Participation, Ankara, December 2008.
- [9] A. Gaini, "Introduction for probability thory," The Publishing Center of Imam Hussein, Tehran, 1979.
- [10] S. Haridi and P. Roy, "Concepts, Techniques and Models of Computer Programing," Universit'e catholique de Louvain (at Louvain-la-Neuve), 2003.
- [11] A. Renyi and P. Erdos, "On Random Graph," Publication Mathematicas 6, pp. 290-297, Nov. 1958.
- [12] H. A. Zakerzade, H. Bigdeli, and M. A. Iranmanesh, "The concept of random graphs and models," The Student publication Statistics (Neda), Tehran, vol. 7, no. 2, pp. 30-34, 2010.
- [13] E. Upfal and M. Mitzenmacher, "Balls, Bins, Random Graphs (Balls-and-Bins Model)," Probability and Computing, published by Cambridge University Press, 2005.

که گراف تصادفی ساخته شده در روش جدید کل دامنه تابع رمز قالبی را پوشش می دهد. روش چابک سازی گراف در تولید زنجیره های بدون تصادم مورد استفاده موثر بوده و در نحوه یافتن دورها و طوقه ها در تابع مصالحه نسبت به سایر روش های موجود متفاوت عمل کرده و باعث افزایش پوشش کلید رمز قالبی هم در مرحله پیش پردازش و هم در مرحله اجرا می شود.

۸- مراجع

- [1] M. Helman, "A cryptanalytic time-memory trade off," IEEE Transactions on Information Theory, vol. 26, no. 4, pp. 401-406, 1980.
- [2] E. Barkan, E. Biham, and A. Shamir, "Rigorous Bounds on Cryptanalytic Time/Memory Trade Offs," Lecture note in computer science, pp. 1-21, 2006.
- [3] E. Barkan, E. Biham, and A. Shamir, "Rigorous Bounds on Cryptanalytic Time/Memory," Proceedings of Crypto 2006, LNCS 4117, pp. 1-21, 2006.
- [4] N. A. Saran, "Time memory trade off attack on symmetric ciphers," Applied Mathematics of Middle East Technical University, Feb. 2009.

TMTO Method Analysis for Block Ciphers Using a Random Graph

A. R. Mirghadri*, A. Dini, N. H. Gharavi, A. A. Fathizadeh

*Imam Hossein University

(Received: 19/09/2016, Accepted: 13/04/2017)

ABSTRACT

In this paper, we consider the Time-Memory-Trade-Off (TMTO) method for analysis of block ciphers and related methods. Also, we discuss some subjects including coverage in the Hellman chains, collision in chains, cycles and rings that create a block cipher function. Hellman method is analyzed by a random graph. The random graph is made of a function block cipher, which is applied to extract non-collision chains, cycles and rings. According to the unique modes and features available in the random graph, a new method for extraction of cycles and rings in the random graph entitled 'Agility of graph' is offered. This method extracts the cycles and rings of the lock cipher function as easily and at a very low cost. The obtained cycles and rings are used for generating non-collision chains in the block ciphers that they make a complete coverage of block ciphers in the TMTO method .

Keywords: Directed Graph, Random Graph, Non-Collision Chains, Trade-Off Method, Block Cipher.

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