توبع چکیده‌ساز

زهرا ذوالفقهی و نصر باقری
دانشگاه مهندسی برق دانشگاه تربیت مدرس شیراز، تهران، ایران
z.zolfaghari71@gmail.com
nbagheri@arttu.com

چکیده
در این مقاله به معرفی حمله TMTO و نحوه پیدا کردن نزدیک‌برخوردگی در یک تابع چکیده‌ساز پرداخته شده است. با دنستراتوکن مهاسات چکیده‌ساز، محاسبه یک حد پایین برای پیچیدگی گورمیکالی در یک چکیده‌ساز به وسیله ارائه یک الگوریتم بهینه‌سازی می‌تواند این الگوریت توانایی کشف این حالت‌ها را داشته باشد. این الگوریتم زیر استفاده از حافظه‌های دارای دو حافظه دارد. با استفاده از الگوریتم متعدد برای دادن به حافظه‌ها یک حالت که بهترین حافظه‌ها را می‌تواند کشف کند، که این الگوریتم و همچنین دیگر چکیده‌سازی‌ها همین‌طور که سپس نشان داده می‌شود.

و از گوناگون تابع چکیده‌ساز، نزدیک‌برخوردگی، بدی‌بستان زمان‌حافظه

۱- مقدمه

حمله پیش‌تصویر دوم Zamani که x نام داده شده است، بیان می‌کند که x یکی از مسائل متداول در رمزگذاری کلید خصوصی مسئله پیدا کردن برخورد است. اغلب توان نه در پیدا کردن برخورد برای توابع چکیده‌ساز بکه در مسائل دیگر رمزگذاری نیز مطرح است. طی چندین دهه، پیدا کردن برخورد به‌طور گسترده‌تر مطالعاتی گرفته است. خلاصه این مسئله و همراه با پیدا کردن نیازمندی‌های مستند به دست آمده است. با توجه به مسئله بالای یک حمله بروز و دو جایی که حمله‌های پیش‌تصویر x یک حجم حمله‌های پیش‌تصویر x نمی‌باشد که Zamani که x نام داده شده است. خلاصه این مسئله و همراه با پیدا کردن نیازمندی‌های مستند به دست آمده است.

۱ Second-priemage attack
۲ Collision attack
۳ Prieimag attack

توبع چکیده‌ساز، از تختی‌های رمزگذاری یک بنیادی مورد استفاده بسیاری از ساختارهای و بروز و یک تابع

هنگامی که در زمینه رمزگذاری استفاده می‌شود، یک

حمله برخوردگی Zamani که x نام داده شده است، بیان می‌کند که x یک حجم حمله‌های پیش‌تصویر x نمی‌باشد که Zamani که x نام داده شده است.

۱Collision attack
۲ Prieimag attack
۳ Noised attack

سال ۱۳۹۶، جلد ۱۱، شماره ۲
دو فصل نامه علمی ترویجی متدی امنیت فضای تولید و تبادل اطلاعات (افتا)

می‌کند. به‌طور کلی، انتظار می‌رود که یک تابع چیک‌ساز مانند یک تابع تصادفی و رفتار دارد. این شرط بطور دقیق نمی‌تواند به‌طور کامل مشاهده شود و در این حالت، پیشرفت‌های جزئی و اصلاحاتی معنی‌داری به داشته که کیکی نمی‌تواند آن‌ها گزارش نماید توسط میان‌برنگی و سینگلر [6] پیش‌گیری شده است. این گزارش را حاصل می‌کند زمانی که هر یک از اندولاهاهای GDP راه حلی برای صعود و چندین حمله در این مورد پیشنهاد شده است.

کوچک‌ترین حمله در این مقاله استفاده شده است:

1. انتخاب یک کریپتوگرافی برای پیچیدگی حمله‌های

    زندگی در برابر چیک‌ساز (دستکم 2a2/√Bw(n))/2 به‌طور کلی ارزیابی تابع چیک‌ساز نیاز دارد. این حال تا زمان‌اداره باید یک رمز انتخاب شده باشد تا به‌طور مؤثر مورد توان‌پذیری‌های جدید به داشته که با مقدار حذف و مشاهده حذف و با توجه به مثالی مورد استفاده برای اجزای از این موشک‌های بزرگ GPU و/یا با استفاده از ابزارهای داده‌های پیشرفته‌های کمترین شرکت می‌باشد.

2. مزایای مطالبه‌مرتب

در اینجا ابتدا به بحث در مورد حمله تلفن‌های بپندازد برخوردار کامپیوترکه در ادامه نیز تلفن‌های بپندازد برخوردار شرکت می‌باشد.

3. تجربیات گروهی جستجوی جامعه

ارزیابی به‌طور کلی پیام‌های رمزگذاری f(m)=m' یک همبسته ژن‌ریزشی در m زبان f که در m' زبان می‌باشد. هدف محاسبه باید در آن کار، می‌تواند یک تابع چیک‌ساز ساز، رمز قابل رمز جنگی باشد. در یک تابع چیک‌ساز می‌تواند حذف دهند همین وروی است. یک کار محیطی می‌تواند انجام دهد انجام جستجوی جامعه. همه می‌تواند انجام کند و بیندی که آیا از خروجی در m' فرمودار، به‌طور مثال در نتیجه می‌باشد. به‌طور کلی پیام‌های رمزگذاری یک همبسته ژن‌ریزشی در m' زبان f که در m' زبان می‌باشد. هدف محاسبه باید در آن کار، می‌تواند یک تابع چیک‌ساز ساز، رمز قابل رمز جنگی باشد. در یک تابع چیک‌ساز می‌تواند حذف دهند همین وروی است. یک کار محیطی می‌تواند انجام دهد انجام جستجوی جامعه. همه می‌تواند انجام کند و بیندی که آیا از خروجی در m' فرمودار، به‌طور مثال در نتیجه می‌باشد. به‌طور کلی پیام‌های رمزگذاری یک همبسته ژن‌ریزشی در می‌باشد. به‌طور کلی پیام‌های رمزگذاری یک همبسته ژن‌ریزشی در m' زبان f که در m' زبان می‌باشد. هدف محاسبه باید در آن کار، می‌تواند یک تابع چیک‌ساز ساز، رمز قابل رمز جنگی باشد. در یک تابع چیک‌ساز می‌تواند حذف دهند همین وروی است. یک کار محیطی می‌تواند انجام دهد انجام جستجوی جامعه. همه می‌تواند انجام کند و بیندی که آیا از خروجی در m' فرمودار، به‌طور مثال در نتیجه می‌باشد. به‌طور کلی پیام‌های R

3. Stream cipher

2 Block cipher

1 Lamberger
2 - نکات متمایز

بعدا، رویت2 به‌وهیچ‌یافته روش هر م بدون را پیشنهاد کرد که هدف آن کاهش تعداد سختی به حافظه و نپایین سرعت بخشیدن جستجوی جامع است. در هر که سختی به حافظه پرورده می‌باشد، زمان بیشتری از محدودات را صرف می‌کند. این روش، شرط خامه‌های زنجیره‌ی ریسید به یک نقطه پایانی دارد به معنای نمایه‌ی خاصی به صورت خودکار می‌شود. نقاط پایانی دیری بیشتر

\[ \text{ضریب } K \text{ بین نقطه صفر می‌شوند.} \]

از آنجا که ممکن است، مدت زمان‌ها را یا حتی برای همیشه در مورد گیرفته به‌ره دیگر تابث به معنی بعضی از طول زنجیره، در زمان‌های کم و متوسط بیش از سری‌های نپایین می‌شوند. این‌ها بکار می‌رود تا در تکرار تعداد نیاز داشته‌باشند. 

3- جداول رنگ‌کمان

برای یک مدت طولانی، روش رویت‌ها به‌جهت هر مهیل تابع نتیجه‌گیری است. این‌ها به‌معنی بعضی از طول زنجیره، در زمان‌های کم و متوسط بیش از سری‌های همیشه در با برای به‌ویژه در اگه که پروفایل‌ها به‌جهت هر مهیل تابع نتیجه‌گیری است. این‌ها به‌معنی بعضی از طول زنجیره، در زمان‌های کم و متوسط 

\[ f_k(x_k) \rightarrow f_0(x_0) \rightarrow f_1(x_1) \rightarrow f_2(x_2) \rightarrow \cdots \rightarrow f_n(x_n) \] 

در مرحله‌ی پرخطر مهیلی، f_0 را برای به‌ویژه زمان‌ها برای روز متن‌راتی که خودش داده است، تکرار و مرحله پرخطر مهیلی، f_0 را برای به‌ویژه زمان‌ها برای روز متن‌راتی که خودش داده است، تکرار و مرحله پرخطر مهیلی، f_0 را برای به‌ویژه زمان‌ها برای روز متن‌راتی که خودش داده است، تکرار و مرحله پرخطر مهیلی، f_0 را برای به‌ویژه زمان‌ها برای روز متن‌راتی که خودش داده است، تکرار و مرحله

2 Distinguished points
3 Rivest
4 Rainbow tables
5 Oechslin

1 Hellman

مسر نصیر حمیدی (ترجمه‌ی: حافظه) بوسیله توابع (TMTO) در بالای چکیده‌ساز

برای تاریخ دهم فروردین 1396 (جلد 11، شماره 1) 17
دو فصل نامه علمی ترویجی منادی امنیت فضای تویید و تبادل اطلاعات (افتا)

ماتریس‌های متغیر محاسبه شوند. تنا ناقص نخست و آخر
به زنجیره ذخیره می‌شوند [7].

\[ x_0 \rightarrow f_0(x_0) \rightarrow f_1(f_0(x_0)) \rightarrow \cdots \rightarrow \]
\[ f_{n-1}(\cdots f_0(x_0)\cdots) \]

به 1- بهبود بدیهستان زمان-حفظه

در برنامه‌های کاربردی، بطور معمول عناصر فرست \( L \)
خروجی‌های اولیه می‌باشند؛ در نتیجه بطور زیر فرموله می‌شود:

\[ x_0, x_1, \ldots, x_k \in \{0,1\}^n \rightarrow [0,1]^n, n' \geq n \]

\[ f_1(y_1) \oplus f_2(y_2) \oplus \ldots \oplus f_k(y_k) = 0 \]

به 2- مدل‌ها به دست آمده در اینجا هر یک از این مدل‌ها خود در دسترس داده‌ها می‌باشد. مدل‌های تا دقت کافی فرست خروجی به دست می‌آید. 

\[ \text{مقدار} = \text{مقدار} \]

\[ 0 \]

به 3- مدل‌ها به دست آمده در اینجا هر یک از این مدل‌ها خود در دسترس داده‌ها می‌باشد. مدل‌های تا دقت کافی فرست خروجی به دست می‌آید.

\[ \text{مقدار} = \text{مقدار} \]

\[ 0 \]

به 4- مدل‌ها به دست آمده در اینجا هر یک از این مدل‌ها خود در دسترس داده‌ها می‌باشد. مدل‌های تا دقت کافی فرست خروجی به دست می‌آید.

\[ \text{مقدار} = \text{مقدار} \]

\[ 0 \]

به 5- مدل‌ها به دست آمده در اینجا هر یک از این مدل‌ها خود در دسترس داده‌ها می‌باشد. مدل‌های تا دقت کافی فرست خروجی به دست می‌آید.

\[ \text{مقدار} = \text{مقدار} \]

\[ 0 \]

به 6- مدل‌ها به دست آمده در اینجا هر یک از این مدل‌ها خود در دسترس داده‌ها می‌باشد. مدل‌های تا دقت کافی فرست خروجی به دست می‌آید.

\[ \text{مقدار} = \text{مقدار} \]

\[ 0 \]

به 7- مدل‌ها به دست آمده در اینجا هر یک از این مدل‌ها خود در دسترس داده‌ها می‌باشد. مدل‌های تا دقت کافی فرست خروجی به دست می‌آید.

\[ \text{مقدار} = \text{مقدار} \]

\[ 0 \]
معمولی $\frac{M}{2}$ را می‌تواند چنین $f$ برخوردی مقدار $M$ داشته باشد. هنگامی که آنها $\frac{n}{2}$ همه $i$ را برای مقدار $M$ می‌تواند، جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول همین نشته $\frac{m}{2}$ هر یک از $M$ مقدار به همراه با جدول ها
دو فصل نامه علمی ترویجی متادی امینیت فضای تولید و تبادل اطلاعات (افتا)

3- ارزیابی پیچیدگی

پیچیدگی برای تولید MX، حافظه است Tpre می‌توان زمان MX و حافظه است. همان‌طور که در بالا ذکر شد، سطح یک نیاز به 2-1\(\frac{N}{M^2}X\) تنها را در مدل 2\(\frac{N}{M^2}X\) می‌تواند را به سطح D در انجام می‌دهد. برای پیدا کردن راه‌حل مورد نظر پس از رسیدن به سطح D در سطح دیگر ارتجاع به بیت بیشتر L ایجاد شده عناصر می‌باشد. بنابراین

\[ M^2 = 2-\frac{1}{2}\left(\frac{N}{M^2}X\right)^2 \]

درخست (d-1)m به عنوان مثال \(m = d - 1\) است. این کمیت از (d-1)m به سطح D به صورت م cq دیگر، به‌طوری‌که در حالت کلی از این سطح به سطح S می‌تواند کاهش یابد. در جدول 4، میزان‌های قبیل ارائه شده در (5) با این میزان‌های جدید برای \(k = 4\) و \(l = 2\) مقدار حافظه خاص می‌باشد. به‌طوری‌که، پیچیدگی زمان‌گیر کردن برای همین مقدار حافظه وجود


4- پیدا کردن برخورد های کامل

روش اساسی پیدا کردن برخورد های یا نزدیکترین برخورد در روش عمومی محاسبه نزدیکترین برخورد با تعداد زیادی از ورودی تصادفی است. ابتدا از محاسبه تعداد (i) می‌تواند کاهش دهند به طور دقیقی تعداد محاسبه

\[ O(2^n) \]

به‌طور کلی، تعداد محاسبه مورد نظر 2\(\frac{n}{2}m\) است.

جدول 2: مقایسه مداوم‌ها برای سادگی، ضرب تابع برای N نادیده گرفته شده است. [9]

<table>
<thead>
<tr>
<th>ایستهای #</th>
<th>بیت‌های محصول</th>
<th>کردن کننده</th>
<th>ارائه‌شده</th>
</tr>
</thead>
<tbody>
<tr>
<td>سطح 1</td>
<td>m</td>
<td></td>
<td></td>
</tr>
<tr>
<td>سطح 2</td>
<td>(l )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>سطح 3</td>
<td>(l + (i - 1)m)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(d + 1)m</td>
<td>(l + dm)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

جدول 1: مقایسه تعداد بیت‌های محصول بین K-درخت و algoritme ارائه‌شده. [9]

روش | M | T | پارامترها | دیگر
---|---|---|------------|---
یکشش و همکاران (\(T, M^2 = N\)) | \(\frac{n}{2}\) | \(\frac{n}{2}\) | – |
الگوریتم پیش‌بندی | \(\frac{n}{2}\) | \(\frac{n}{2}\) | – |

\[ X = \frac{n}{2}, \quad \frac{\frac{n}{2}}{2} \]

از وضعیت \(M = d + dm\) و پارامترها \(M\) و \(K\) کاهشی را برای جدول همین می‌توان تبعیض کرد. زنگی به‌طوری‌که در حال ایجاد را با دیگر مقادیر نگست و آخر از هر زنگی را به‌طوری‌که در جدول همین موسوم به \(T_{pre}\) هنگامی که ساختمان شده، یک برخورد جزئی بیتی را با \(T_{pre}\)
تشخیص داد (این روش ها متعلق به تحلیل واحدهای مواد در)، در این کار بررسی توانایی تحلیل ذهنی، به عضو مؤثر می‌شود. همچنین بر روی واکنش‌ها با پیچیدگی تصادف دایره‌ای بوده است. پیچیدگی به ویژه در برشود با استفاده از تحلیل ذهنی کشف می‌شود. توصیف و تحلیل قرار گرفت.  کام اصلی کاربردهای از تکرار، با شروع از یک نقطه تصادفی و توقف زمانی که یک نقطه ممکن با ویژگی‌های قابل مشاهده است. در این کاربرد از یک جدول برای ذهنی زنجیره M (معنی‌دار اعداد نقطه شروع و پایان) استفاده می‌شود و همچنین که نقطه شروع به دیده شود، با احتمال زیاد یک برخورد به سمت ادامه است. تجربه و تحلیل این ارتقاء و تبلیغات مختلف را (بسته به تعیین برخوردها مورد اندازه‌گیری) در نظر می‌گیرد. یک پارامتر مهم در تجربه و تحلیل نسبت نقطه مشخص شده است.

\[ i \propto M \]

به عنوان مثال

اگر با دانش کافی حالت بازی ذهنی تمام زنجیره‌ها موجود باشد، یک کرون i برخورد بر از یک حجم کار از \[ \frac{1}{\sqrt{2\pi n}} \] را به اندازه که \( n = 0 \) جفت نقطه را پوشانده‌است. پیچیدگی داده‌شده توسط اورشال و تحلیل نسبت نقطه

\[ C_{\text{smallest}} = \sqrt{\frac{\pi}{2}} \sqrt{2n!}, \]

یک عامل تسریع از \( \sqrt{\pi} \) است بی‌پایاگردن i برخورد به طور مستقل وجود دارد.

\[ \text{(9)} \]

\[ \text{Van Oorschot} \]

\[ \text{1 Memory-less algorithms} \]

\[ \text{2 Pollard} \]

\[ \text{3 Floyd's algorithm} \]

\[ \text{4 Brent's algorithm} \]
دو فصل نامه علمی ترویجی متادان امنیت فضای تولید و تبادل اطلاعات (افتا)

3-4 پیداکردن تعداد زیادی از برخورد

به معنی مال

در این مورد، حافظه یا داده‌ها آرامش‌ها [15] نشان میدهند زمانی که حافظه بر است، پیچیده‌ی برخورد به طبقه‌ی ماتریسی باید برای (2) بررسی شود. برای این پیچیده به کمیته است. به‌طور دقیق‌تر، در نواحی آرامش‌ها برای تعیین تأثیر

حقیقی انجام داده و پیچیده‌ی زیر حاصل شده است:

\[ C = 5 \frac{\sqrt{n}}{M} \cdot \]

هنگام که \( \sqrt{n} \approx 2.25 \sqrt{M} \theta \)

است. یک عملیه ترتیبی از \( \sqrt{\frac{M}{n}} \) نسبت به پیداکردن یا برخورد به طور مستقیم و داراد.

حد جهانی. به‌طور کلی، یک کران بالا برای پیچیده‌ی که در هر دو شرایط کار می‌کند، با جمع دو برای می‌توان

بیان کرد:

\[ C \leq \sqrt{\frac{\sqrt{2}}{M}} \cdot \]

الگوریتم حافظه-کمال

در این الگوریتم تعداد محاسبات موردی دارای پیداکردن یک تجدیدبرخورد \( B_w(n) \) است. همچنین حد پایین تعداد ارزیابی چگیمه موردی دارای هر الگوریتم \( B_w(n) \) ندیده‌ی برخورد درس کم محاسبه چهت

دستیابی به \( w \) تجدیدبرخورد با احتمال ناجی است.

با این حال، لازم است ناپایین به \( B_w(n) \) است. حافظه قابلیت استرس جدول به انتصاده \( \Omega \left( \sqrt{2}, B_w(n) \right) \) در مقدار حمل برخورد بین الگوریسمی، جدول

چگیمه و یا زنجیره تکرار نمی‌توان کاهش داد. در این مورد، اجرای عملی ضعف حساب می‌شود [10].

5- کامپیوتربرخورد

\( h(x) = x \) به‌صورت \( x \), \( x^2 \) به‌صورت \( h(x) = x \)

و \( \| w \| \leq \| \| \) است. به‌طور کلی \( \| h(x) \| \leq \| \| ) است. ابتدا برخی از نتایج در آن‌ها با قابلیت معنی‌داری می‌توان و تعریف ۱. انتخاب یک نب در همه‌ی همان برش \( w \) و تعریف ۱. انتخاب یک نب در همه‌ی همان برش

\[ \sum_{i=0}^{\lfloor w/2 \rfloor} c_i \] \( w \) که \( c_i \) هر جفت \( x \) و \( x^2 \) کامپیوتربرخورد نتیجه دهم برابر است با:

\[ B_w(n)/2^n \]

1. Memory-full algorithm
مقدار حافظه می‌تواند به‌طور قابل توجهی توسط $M \approx \frac{\sqrt{M}}{\sqrt{4 \pi}}$ در صورتی که $M$ یک عدد باشد که به معنای لغزش که در شرح ۴ شرح داده شد باشد، کاهش یابد. در اینجا نمونه و مثال‌های مقادیر بهره $\beta$ و پیچیدگی حانه به شکل نشان داده می‌شود. در پیش‌بازیزی عملی یک حانه نزدیک به‌جواره و فریز می‌شود که مقداری از حانه و دسترس است، که به‌طور قابل توجهی منجر به حمله‌های بی‌پره می‌شود.

3-1 پیچیدگی

مطلق با شکل (۲) بیت از تابع $J$ که به‌طور یک‌نواختی با توجه به بروز باقی‌مانده جستجو می‌کند. برای هر بروز باقی‌مانده $n$، بیش از ۳ بیت از منابع الکترومغناطیسی می‌شود. در نتیجه پیداکردن یک نزدیک به‌جواره پس از آزمایش (۳) به‌طور $B_{\beta}(\beta)$ برخورد امکان‌پذیر است.

مقدار $B_{\beta}(\beta)$ به‌طور یک‌نواختی با توجه به $M = \frac{\sqrt{M}}{\sqrt{4 \pi}}$ در صورتی که $M$ یک عدد باشد که به معنای لغزش که در شرح ۴ شرح داده شد باشد، کاهش یابد.

6-4 تغییر در حافظه با روش

کوتاماسازی

نخستین کوتاماسازی تعیین ساده روش مبتنی بر کوتاماسازی در بخش ۵ است. مثالی از شکل (۴) بیت با $2w > 1$ برخورد. این است که یک برخورد در نتیجه $n$ که به‌طور یک‌نواختی با توجه به $M$ به‌طور یک‌نواختی با توجه به $n$ باید به‌طور یک‌نواختی با توجه به $n$ قطعیت نیاز به تعداد کمی از برخورد است. اما پیداکردن برخورد با مدلی ثابت زیر به‌طور به‌طور یک‌نواختی با توجه به $n$ ویژه از این ناحیه دیده از پیچیدگی این کوتاماسازی است که به‌طور مقداری از جزئی و تحلیل ول اورشیت (۱۵) که در بخش ۴ بیان‌آوری شد استفاده شده است.
دو فصل نامه علمی ترموئی‌مندی امنیت فضای تولید و تبدیل اطلاعات (افتا)

برای این اندک‌زه، پیچیدگی بهصورت زیر است:

\[ C \approx \frac{2^{n/2}}{\sqrt{B_w(\tau)}} \]  \hspace{1cm} (20)

که این پیچیدگی بیشتر از پیچیدگی بهینه می‌گردد.

امد توسط کورنلیک حالت‌های کامل از بیان ۲\(^{n/2}/\sqrt{B_w(\tau)} \) (که این پیچیدگی بیشتر از حد بی‌بودن برای این کورنلیک مربوط می‌شود) بهتر است.

به‌پایه درعمل، برای \( m \) و \( n \) داده شده، تخمین

\[ C \leq C_{small} + C_{lg} = \left( \frac{1}{2} + \sqrt{\frac{2^{n/2}/B_w(n)}{M}} \right)^{n/2}/B_w(n) \]  \hspace{1cm} (21)

برای کدورت‌های کیت بی‌بودن خوب، این حد را برای تمام مقادیر محاسبه و از حد از کورنلیک که پایین‌ترین حد را داشته، استفاده کردند. در مقاله [10] نمونه‌های این حمله بر 5 نشان داده است.

- نتایج

در این مقاله، حمله TMTO و روش‌های بهبود این حمله عمومی راه‌های درمانی، معرفی و همچنین، کورنلیک عمومی جهت کپیراک در نزدیک‌ترین شش آماری معرفی شد که هر دو کورنلیک بهینه می‌تواند بر کاهش‌های و متنی بر کاهش یک‌پاره بهینه را تعیین می‌دهد. بر علی‌کاریته بیشتر، هدف این کورنلیک مطالعه بوده است و در عمل TMTO قابل بهبودی است. لازم به ذکر است که با استفاده از کورنلیک عکس‌هایی از صد افتاده و در عمل کورنلیک مشابه که با حالت‌های میان‌شکلی و سه‌گانه که با حالت‌های کم در زمان مشابه کمتر از 4، به‌بودن را می‌توان پیدا کرد.

\[ C_{large} = \frac{5/2 - m/2}{B_w(\tau)} \leq \frac{5/2 - m/2}{B_w(\tau)} \]  \hspace{1cm} (17)

\[ C_{large} = \frac{5/2 - m/2}{B_w(\tau)} \leq \frac{5/2 - m/2}{B_w(\tau)} \]  \hspace{1cm} (18)

\[ C_{large} = \frac{5/2 - m/2}{B_w(\tau)} \leq \frac{5/2 - m/2}{B_w(\tau)} \]  \hspace{1cm} (19)

\[ C_{large} = \frac{5/2 - m/2}{B_w(\tau)} \leq \frac{5/2 - m/2}{B_w(\tau)} \]  \hspace{1cm} (20)

\[ C_{large} = \frac{5/2 - m/2}{B_w(\tau)} \leq \frac{5/2 - m/2}{B_w(\tau)} \]  \hspace{1cm} (21)

نصور باقری، دانشیار دانشگاه تربیت دیپر شهید رجایی، کارشناسی خود را در دانشگاه مارنارن و دوره کارشناسی ارشد و دکتری را در دانشگاه علم و صنعت ایران در مهندسی الکترونیک به پایان رساند. مقالات متعددی در زمینه رمزگشایی توسط ایشان، در مجلات و همایش‌های ملی و بین‌المللی، ارائه شده است. در حال حاضر زمینه پژوهشی وی رمزگاری و امنیت اطلاعات است.


