مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال ششم، شماره ۳، پاییز ۱۳۹۷، ص ۶۴-۵۹

تحلیل رمز چرخشی روی CubeHash و Shabal

سید علی طباطبائی فیض‌آباد[۱]، احمد گائینی[۲*]، بهبد کشاورزی[۳]

۱- دانشجوی کارشناسی ارشد، ۲- استادیار گروه ریاضی و آمار، دانشگاه جامع امام حسین (ع) ۳- کارشناسی ارشد، دانشگاه شاهد

(دریافت: ۹۶/۰۵/۲۲، پذیرش: ۹۶/۱۰/۲۵)

چکیده

توابع چکیده‌ساز نقش بسیار مهمی در امنیت شبکه و مخابرات دارند. این توابع در خلاصه‌نمودن یک پیام نقش به‌سزایی دارند که در کاربردهای رمزنگاری مانند امضاء رقمی، الگوریتم‌های تولید اعداد تصادفی و پروتکل‌های احراز اصالت و غیره به‌طور گسترده استفاده می‌شوند. حمله چرخشی یک حمله نسبتا جدیدی است که جزء حملات عمومی بر توابع چکیده‌ساز محسوب می‌شود و بر روی الگوریتم‌هایی که در ساختار خود از سه عملگر چرخش، جمع پیمانه‌ای و یای انحصاری استفاده می‌کنند یعنی ساختاری ARX دارند، موثر است. در این مقاله برای اولین بار بر توابع چکیده‌ساز Shabal و CubeHash که کاندیداهای دور دوم مسابقه SHA-3 می‌باشند و در ساختار خود از خاصیت ARX بهره می‌برند تحلیل رمز چرخشی انجام می‌شود. تحلیل رمز چرخشی با درنظر گرفتن زنجیره مارکوف برای دنباله جمع‌های پیمانه‌ای به‌کار رفته‌شده در توابع چکیده‌ساز Shabal و CubeHash انجام می‌شود. تحلیل رمز چرخشی بر تابع چکیده‌ساز Shabal به پیچیدگی کل $2^{3393.58}$ برای ۱۶+۳- دور آن و پیچیدگی $2^{57.6}$ برای کل ۱۶- دور CubeHash منجر می‌شود. با توجه به نتایج به‌دست‌آمده مشاهده می‌شود که به‌علت وجود تعداد بیشتری از جمع‌های پیمانه‌ای که به‌صورت زنجیره مارکوف هستند، تابع چکیده‌ساز Shabal مقاومت بیشتری نسبت به تابع چکیده‌ساز CubeHash در برابر تحلیل رمز چرخشی از خود نشان می‌دهد و احتمال موفقیت کمتری دارد.

کلید واژه‌ها: توابع چکیده‌ساز، تحلیل رمز چرخشی، جمع پیمانه‌ای، زنجیره مارکوف.

۱- مقدمه

توابع چکیده‌ساز رمزنگاری در بسیاری از کاربردهای رمزنگاری مانند طرح‌های امضاء رقمی[۱] و پروتکل‌های احراز اصالت به‌کار می‌روند و از ابزارهای مهم در رمزنگاری مدرن هستند. یک تابع چکیده‌ساز، مانند تابع H، یک پیام با طول دلخواه را به‌عنوان ورودی گرفته و یک مقدار چکیده با اندازهٔ ثابت n تولید می‌کند. از الزامات امنیتی توابع چکیده‌ساز می‌توان به مقاومت آن در برابر برخورد[۲]، پیش‌تصویر دوم[۳] و پیش‌تصویر[۴] اشاره کرد [۱].

مؤسسه ملی استانداردها و فن‌آوری[۵] آمریکا کار استانداردسازی الگوریتم‌های چکیده‌ساز را در سال ۱۹۹۳ میلادی با انتشار الگوریتمSHA-0 [۲] شروع کرد. طولی نکشید که این الگوریتم به‌خاطر مشکل امنیتی آن با [۳] SHA-1 جایگزین شد [۴]. در ادامه، سال ۲۰۰۲ میلادی، NIST، توابع چکیده‌ساز خانواده SHA-2 [۵] را به مجموعه الگوریتم‌های چکیده‌ساز استاندارد خود اضافه کرد. در سال‌های ۲۰۰۴ و ۲۰۰۵ میلادی، پیشرفت‌هایی در رابطه با تحلیل توابع چکیده‌ساز پرکاربرد و استاندارد حاصل شد که یکی از این موارد مربوط به حمله موفقیت‌آمیز روی SHA-1 بود. با توجه به این امر، NIST اعلام کرد که لازم است در کاربردهای رمزنگاری از الگوریتم‌های خانواده SHA-2 استفاده شود (که در مقایسه با SHA-1 امنیت بالا، اما سرعت و کارآیی پایینی دارند). اگرچه تاکنون حمله موفقی روی توابع چکیده‌ساز خانواده SHA-2 ارایه نشده است، اما روشن است که یافتن یک برخورد (یا پیش‌تصویر دوم و یا پیش‌تصویر) در این خانواده منجر به حملات موفقیت‌آمیز روی کاربردهایی مانند امضاءهای رقمی و پروتکل‌های رمزنگاری خواهد شد. به همین دلیل، NIST برای یک تابع چکیده‌ساز استاندارد امن جدید، احساس نیاز کرد و در نوامبر ۲۰۰۷ میلادی، از برگزاری یک مسابقه عمومی برای انتخاب استاندارد چکیده‌ساز جدید و امن به‌نام SHA-3 خبر داد و یک سری الزامات اولیه برای نامزدهای این مسابقه مشخص کرد [۶].

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

1- Digital Signature
2- Collision
3- Secound Pre-Image
4- Pre-Image
5- NIST

تحلیل چرخشی[1] یک حمله نسبتاً جدید است که توسط Dmitry Khovratovich و Ivica Nikolic [۷] در تحلیل سیستم‌های ARX به‌کار رفته شده است. حمله چرخشی یک حمله احتمالی است که از سیر تکامل یک جفت چرخشی $(x, \vec{x})$ که یکی چرخش[2] دیگری به اندازه r-بیت است و از طریق دورهای یک تابع یا رمز انجام می‌شود، پیروی می‌کند. حمله چرخشی در برابر ساختن قالب‌ها از چندین تابع چکیده‌ساز[3] مثل...,Skein, Blake, Keccak راه‌اندازی شده است. محاسبه شانس موفقیت حمله‌های احتمالی به‌صورت یافتن احتمال ورودی‌ها و خروجی‌های متناظرش است که دارای یک خاصیت ویژه‌ای باشند که برای یک تابع یا جایگشت تصادفی، غیرمنتظره باشد. ایده اصلی تحلیل چرخشی این است که برخی تبدیل‌ها روی ورودی‌های چرخش‌یافته، خروجی‌های چرخش‌یافته تولید می‌کنند (در واقع دشمن انتشار روابط چرخشی را در سرتاسر تبدیل‌های الگوریتم بررسی می‌کند). Khovratovich و Nikolic [۷] مقاله قبلی خود را که فقط تعداد جمع‌های پیمانه‌ای را درنظر گرفته بودند و فرض مارکوف‌بودن در آن رعایت نشده بود را مورد بازبینی قرار دادند و یک احتمال جدید برای محاسبه پیچیدگی حمله چرخشی با توجه به مارکوف‌بودن آن ارایه کردند.

در این مقاله بر روی توابع چکیده‌ساز Shabal و CubeHash که کاندیداهای دور دوم مسابقه SHA-3 هستند و ساختاری ARX دارند حمله تحلیل رمز چرخشی انجام می‌شود. در بخش دوم این مقاله حمله تحلیل رمز چرخشی تشریح می‌شود و الزامات اجرای تحلیل رمز چرخشی مورد بررسی قرار می‌گیرد و در بخش سوم توابع چکیده‌ساز Shabal و CubeHash مختصراً معرفی می‌گردند و در بخش چهارم تحلیل رمز چرخشی بر توابع چکیده‌ساز اعمال می‌شود و در بخش آخر نتیجه بحث ارایه می‌گردد.

۲- تشریح تحلیل رمز چرخشی

در [۷] روش کلی برای تحلیل سیستم های ARX نشان داده شده است، ایده کلی فرض جفت کلمه‌ها است که یکی چرخش دیگری به اندازه r-بیت می‌باشد. که عملگرهای چرخشی به وسیله $\lll$ r یا $\ggg$ r و یا به طور معادل $\vec{x}$ و $\overleftarrow{x}$ تعریف می‌شوند که $\vec{x}$ چرخش x به اندازه r-بیت به سمت راست را نشان می‌دهد و $(x, \vec{x})$ را جفت چرخشی به اندازه r-بیت می‌نامیم. اثبات این‌که یک جفت چرخشی با هر تبدیل بیتی حفظ می‌شود آسان است مخصوصاً یای انحصاری[4] و چرخش که در رابطه (۱) نشان داده است [۷]:

$$\overrightarrow{x \oplus y} = \vec{x} \oplus \vec{y}, \vec{x} \ggg r' = \overrightarrow{x \ggg r'} \qquad (۱)$$

جمع پیمانه‌ای[5] را به مد 2^n درنظر می‌گیریم، احتمال این‌که جفت چرخشی از جمع پیمانه‌ای بیرون آید توسط لم ۱ محاسبه می‌شود.

لم ۱: احتمال چرخشی با درنظر گرفتن مقدار چرخشی r از رابطه (۲) محاسبه می‌گردد [۷]:

$$p_r(x \boxplus y \lll r = x \lll r \boxplus y \lll r) = \frac{1}{4}(1+2^{r-n}+2^{-r}+2^{-n}) \qquad (۲)$$

برای nهای بزرگ و r کوچک جدول (۱) را داریم:

جدول (۱): احتمال موفقیت حمله چرخشی به ازای مقادیر چرخشی متفاوت [۷]

r	P_r	$log_2 P_r$
۱	۰/۳۷۵	-۱/۴۱۵
۲	۰/۳۱۳	-۱/۶۷۶
۳	۰/۲۸۱	-۱/۸۳۱

برای $r = \frac{n}{2}$ احتمال نزدیک $\frac{1}{4}$ می‌باشد که این محاسبات برای چرخش به سمت راست نیز برقرار است. حال اگر یک طرح دلخواه $\mathcal{S}$ با چرخش و جمع پیمانه‌ای و xor بر n-بیت کلمه درنظر بگیریم قضیه زیر را تحت فرض استقلال داریم:

قضیه ۱: فرض کنید q تعداد عملگرهای جمع‌های پیمانه‌ای در یک طرح ARX باشد، فرض کنید $\vec{I}$ ورودی طرح $\mathcal{S}$ که به اندازه r-بیت به سمت راست چرخش داده شده، باشد آن‌گاه با احتمال P_r^q تساوی $\mathcal{S}(\vec{I}) = \overrightarrow{\mathcal{S}(I)}$ برقرار است [۷].

اثبات: به کمک استقرا بروی اندازه طرح در مرجع [۷].

به‌منظور اعمال تحلیل چرخشی، سعی می‌شود تا ورودی‌های طرح ARX تشکیل جفت چرخشی دهند. برای یک تابع تصادفی P که به z_2^t نگاشت می‌شود، احتمال این‌که $P(\vec{I}) = \overrightarrow{P(I)}$ باشد برای I تصادفی 2^{-t} است. بنابراین، می‌توانیم یک تابع غیرتصادفی بیابیم اگر تابع بتواند با q جمع پیمانه‌ای اجرا شود و نامساوی $P_r^q > 2^{-t}$ برقرار باشد [۷].

[۸] نشان می‌دهد که احتمال موفقیت حمله چرخشی ARX، تنها به تعداد جمع‌های پیمانه‌ای بستگی ندارد بلکه به طریقه اتصال آن‌ها بستگی دارد. احتمال چرخشی نمی‌تواند با ضرب احتمال تک‌تک جمع‌ها به‌دست آید. این بدین معنی است که فرض رمز مارکوف استفاده‌شده برای محاسبه ضمنی احتمال از این طریق امکان‌پذیر نیست.

1- Rotational Cryptanalysis
2- Rotation
3- Hash Function
4- Xor
5- Modular Addition

دنباله‌ای از متغییرهای تصادفی گسسته $v_0, \ldots, v_r$ یک دنباله مارکوف است اگر برای $0 < i < r$ رابطه (۳) برقرار باشد [۸]:

$$p_r = (v_{i+1} = \beta_{i+1} | v_i = \beta_i, v_{i-1} = \beta_{i-1}, \ldots, v_0 = \beta_0) = p_r(v_{i+1} = \beta_{i+1} | v_i = \beta_i) \quad (۳)$$

احتمال چرخشی ARX به سادگی با شمارش تعداد جمع محاسبه نمی‌شود و باید موقعیت جمع‌های پیمانه‌ای بررسی شوند، یعنی این‌که آیا جمع‌های پیمانه‌ای به‌صورت متوالی در الگوریتم آمده‌اند یا جدا جدا و در بین عملگرهای دیگر آمده‌اند. درحقیقت، زنجیره بزرگتر برای جمع‌های پیمانه‌ای احتمال چرخشی کمتری دارد. احتمال چرخشی جمع‌های پیمانه‌ای زنجیره‌ای در لم ۲ آمده است:

لم ۲: اگر $a_1, \ldots, a_k$ کلمه‌های n-بیتی تصادفی باشند و برای $0 < r < n$ که r یک عدد صحیح مثبت باشد، آن‌گاه احتمال چرخشی از رابطه (۴) به‌دست می‌آید [۸].

$$\begin{aligned} p_r &= ([(a_1 \boxplus a_2) \lll r = a_1 \lll r \boxplus a_2 \lll r] \\ &\wedge [(a_1 \boxplus a_2 \boxplus a_3) \lll r = a_1 \lll r \boxplus a_2 \lll r \boxplus a_3 \lll r] \\ &\wedge \ldots \wedge [(a_1 \boxplus \ldots \boxplus a_k) \lll r = a_1 \lll r \boxplus \ldots \boxplus a_k \lll r]) \\ &= \frac{1}{2^{nk}} \cdot \binom{k + 2^r - 1}{2^r - 1} \cdot \binom{k + 2^{n-r} - 1}{2^{n-r} - 1} \end{aligned} \quad (۴)$$

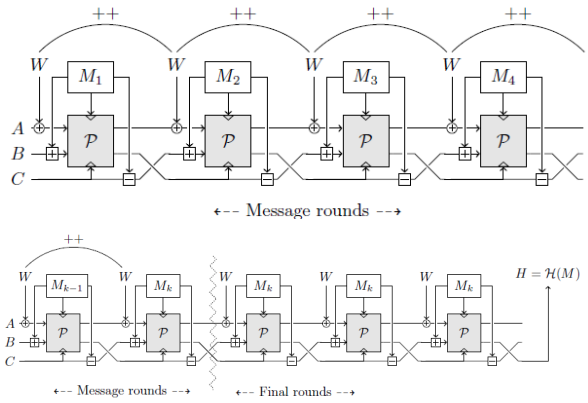
به طور خلاصه، احتمال چرخشی لزوماً برابر با حاصل‌ضرب تک‌تک احتمال موفقیت حمله چرخشی نیست. چنین میان‌بری در تخمین احتمال نه کران بالا نه کران پایین از احتمال واقعی را می‌دهد. بعد از تایید زنجیره مارکوف[1] می‌توان احتمال را تخمین زد در غیر این‌صورت، احتمال چرخشی باید اقتضایی محاسبه گردد.

۳- معرفی توابع چکیده‌ساز CubeHash, Shabal

این بخش به معرفی مختصری از توابع چکیده‌ساز Shabal و CubeHash می‌پردازد و آن‌ها را براساس الزامات تحلیل رمز چرخشی یعنی شمارش تعداد جمع‌های پیمانه‌ای به‌کار رفته‌شده در هر الگوریتم و بررسی این‌که آیا این جمع‌های پیمانه‌ای به‌صورت مارکوف هستند یا خیر، آنالیز می‌شود.

۳-۱- تابع چکیده‌ساز Shabal

Shabal یک تابع چکیده‌ساز مبتنی بر یک کلید جایگشتی $\mathcal{P}$ است. در شکل (۱) ساختار کلی Shabal را می‌بینیم که از k دور پیام و سه دور پایانی تشکیل شده است که مثلاً برای Shabal-512 ، k=16 می‌باشد [۹].



شکل (۱): ساختار کلی Shabal [۱۰]

ساختار تابع چکیده‌ساز Shabal از یک بافر[2] داخلی که طول فضای حالت داخلی آن ۱۴۰۸-بیت می‌باشد، استفاده می‌کند که به سه بخش $(A, B, C) \in \{0,1\}^{l_a} \times \{0,1\}^{l_m} \times \{0,1\}^{l_m}$ تقسیم می‌شود که در ابتدا مقادیر اولیه (A_0, B_0, C_0) را می‌گیرند. یک بافر کمکی $W \in \{0,1\}^{l_m}$ به‌عنوان شمارنده تعداد بلوک‌های پیام استفاده می‌شود. این ساختار از کلید جایگشتی $\mathcal{P}$ استفاده می‌کند که در رابطه (۵) نشان داده می‌شود [۱۰].

$$p = \{0,1\}^{l_m} \times \{0,1\}^{l_a} \times \{0,1\}^{l_m} \times \{0,1\}^{l_m} \rightarrow \{0,1\}^{l_a} \times \{0,1\}^{l_m} \quad (۵)$$

در شکل (۲) کد زیرکلید جایگشتی استفاده‌شده در Shabal در الگوریتم را نشان می‌دهد.

Input: M, A, B, C
Output: A, B

For i from 0 to 15, do:

- $B[i] \leftarrow B[i] \lll 17$

Next i

For j from 0 to $p-1$, do:

- For i from 0 to 15, do:
  - Compute

$$\begin{aligned} A[i+16j \bmod r] \leftarrow\ & \mathcal{U}(A[i+16j \bmod r] \oplus \mathcal{V}(A[i-1+16j \bmod r] \lll 15) \\ & \oplus C[8-i \bmod 16]) \\ & \oplus B[i+o_1 \bmod 16] \\ & \oplus (B[i+o_2 \bmod 16] \wedge \overline{B[i+o_3 \bmod 16]}) \\ & \oplus M[i] \end{aligned}$$

  where $(o_1, o_2, o_3) = (13, 9, 6)$
  - $B[i] \leftarrow (B[i] \lll 1) \oplus \overline{A[i+16j \bmod r]}$
- Next i

Next j

For j from 0 to 35, do:

- $A[j \bmod r] \leftarrow A[j \bmod r] \boxplus C[j+3 \bmod 16]$

Next j

شکل (۲): کد کلید جایگشتی الگوریتم CubeHash [۱۱]

1- Markov Chaining

2- Buffer

۳-۲- الگوریتم CubeHash

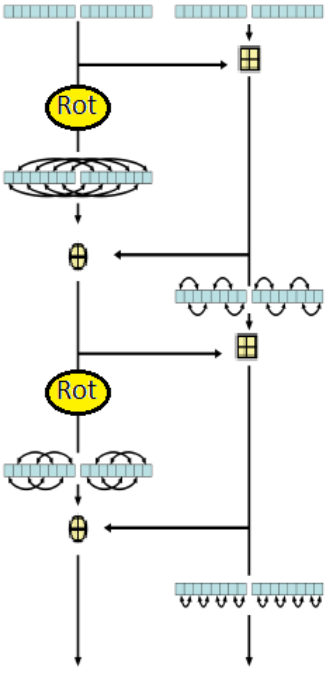
CubeHash r/b-h سه پارامتر دارد که r مشخص‌کننده تعداد دورهای تبدیل فضای حالت، b تعداد بیت‌ها در هر بلوک و h طول بیت‌های چکیده پیام می‌باشد. به غیر از این پارامترها، CubeHash یک فضای حالت داخلی ۱۰۲۴-بیتی دارد.

در اولین دور مسابقه NIST، پارامترهای r=8، b=1 و h={224,256,384,512} بود که در دومین دور مسابقه به r=16، b=32 تغییر داده شدند. الگوریتم CubeHash از یک ساختار اسفنجی استفاده می‌کند که یک ساختار تکراری است و برای داشتن خروجی دلخواه، از یک ورودی با طول متغییر و تبدیل آن به طول ثابت استفاده می‌شود [۱۲].

الگوریتم CubeHash از پنج گام اصلی زیر پیروی می‌کند:

۱) یک ۱۲۸- بایتی(۱۰۲۴- بیتی) را به‌صورت تابعی از (h,b,r) مقداردهی اولیه می‌شود.
۲) تبدیل پیام ورودی به پیام لایه‌گذاری‌شده، پیام لایه‌گذاری‌شده شامل یک یا چند بلوک b- بایتی است.
۳) xor کردن بلوک به اولین b- بایت‌های فضای حالت برای هر بلوک b-بایتی از پیام لایه‌گذاری شده و سپس از طریق r دور یکسان حالت معکوس را به دست می‌آوریم.
۴) به پایان‌رساندن فضای حالت
۵) خروجی‌گرفتن از اولین h/8 بایت‌ها از فضای حالت

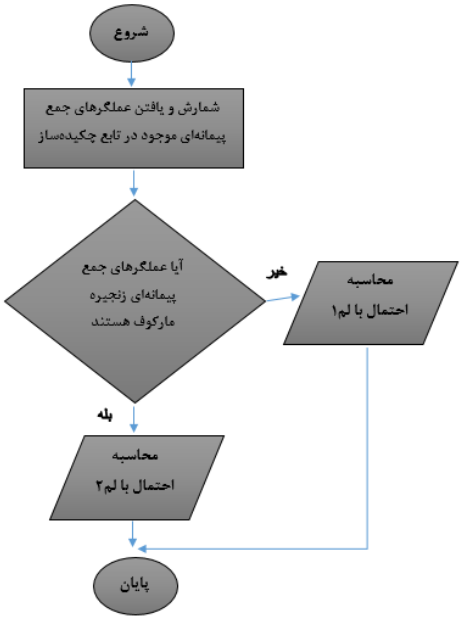
شکل (۳)، الگوریتم CubeHash را نشان می‌دهد:



شکل (۳): الگوریتم CubeHash [۱۱]

۴- اعمال تحلیل رمز چرخشی روی Shabal و CubeHash

در این بخش با توجه به الگوریتم‌های معرفی‌شده در بخش‌های ۳-۱ و ۳-۲ با رویکرد [۸- ۷]، تحلیل رمز چرخشی را بدین صورت که ابتدا تعداد جمع‌های پیمانه‌ای را در کل الگوریتم یافته و بررسی می‌شود که اگر جمع‌های پیمانه‌ای الگوریتم به صورت مارکوف بودند آن‌گاه با توجه به لم ۲ احتمال چرخشی را با درنظرگرفتن مقدار چرخشی r (در این‌جا تحلیل چرخشی با مقدار چرخشی $r = 1$ درنظر گرفته می‌شود) و صرف‌نظر کردن از ثابت‌ها (در صورت وجود) و n-بیت کلمه (با توجه به الگوریتم) محاسبه می‌شود و در غیر این‌صورت، از لم ۱ برای محاسبه احتمال چرخشی استفاده می‌شود. به‌عنوان مثال، برای تابع چکیده‌ساز Shabal-512 با k جمع پیمانه‌ای و n-بیت کلمه و مقدار چرخش r با توجه به نوع تابع چکیده‌ساز از لم‌های ۱ و۲ استفاده می‌شود. تمام محاسبات با استفاده از نرم‌افزار MAPLE-2016 انجام شده است. شکل (۴) مراحل حمله را نشان می‌دهد.



شکل (۴): فلوچارت تحلیل رمز چرخشی

۴-۱- تحلیل رمز چرخشی روی Shabal

با توجه به شکل (۱)، ۱۶ کلید جایگشتی برای دورهای پیام و ۳ کلید جایگشتی برای دور پایانی داریم که در مجموع ۱۹ کلید جایگشتی در تابع چکیده‌ساز Shabal-512 به‌کار رفته شده است [۱۳] که قبل از اولین کلید جایگشتی الگوریتم تنها یک جمع پیمانه‌ای وارد کلید جایگشتی شده است و در انتهای الگوریتم نیز یک تفریق پیمانه‌ای به‌صورت تکی داریم که عملگر تفریق و

جمع پیمانه‌ای در این‌جا احتمال چرخشی برابری دارند و با توجه به این‌که تا این‌جا این دو جمع پیمانه‌ای بررسی‌شده مارکوف نیستند پس بنا به لم ۱ با درنظرگرفتن $r = 1 , n = 32$ احتمال چرخشی هرکدام برابر با $2^{-1,415}$ می‌باشد که احتمال این دو برابر $2^{-1,415*2} = 2^{-2,83}$ می‌باشد. برای مابقی جمع‌های پیمانه‌ای همان‌طورکه در شکل(۱) می‌توان دید، هرکدام از جمع‌های پیمانه‌ای با عملگر تفریق به‌صورت مارکوف زنجیر شده‌اند که ۱۸ تا از این زنجیره‌ها داریم که هرکدام بنا به لم ۲ با درنظرگرفتن مقادیر $r = 1 , n = 32$ احتمال چرخشی برابر با $2^{-3,6}$ دارند که احتمال آن برابر $2^{-3,6*18} = 2^{-64,8}$ است. هم‌چنین، برای کلیدهای جایگشتی $\mathcal{P}$ بنا به شکل (۲) در قسمت انتهایی کد، ۳۶ جمع پیمانه‌ای به‌صورت مارکوف داریم که بنا به لم ۲، این ۳۶ زنجیره جمع پیمانه‌ای مارکوف دارای احتمال چرخشی $2^{-175,05}$ می‌باشد و چون ۱۹ تا کلید جایگشتی داریم احتمال آن برابر $2^{-175,05*19} = 2^{-3325,95}$ می‌باشد. پس احتمال کل $2^{-3393,58}$ می‌باشد. جدول (۲) این احتمال موفقیت حمله چرخشی را نشان می‌دهد.

جدول (۲): خلاصه تحلیل رمز چرخشی Shabal-512

احتمال کل دورها	احتمال تک دور	دورها	تابع چکیده‌ساز
$2^{-3393,58}$	–	۳+۱۶	Shabal-512

۴-۲- تحلیل رمز چرخشی بر روی CubeHash

با توجه به شکل (۳)، دو جمع پیمانه‌ای داریم که به‌صورت زنجیره مارکوف می‌باشند که بنا به لم ۲ و با درنظرگرفتن مقدار چرخش $r = 1$ و اندازه کلمه ۶۴-بیت برای CubeHash-512 احتمال چرخشی $2^{-3,6}$ را داریم که تابع چکیده‌ساز CubeHash دارای ۱۶ دور می‌باشد که هر دور آن شامل دو زنجیره جمع پیمانه‌ای به‌صورت مارکوف می‌باشد پس احتمال کل برای آن برابر $2^{-3,6*16} = 2^{-57,6}$ می‌باشد. جدول (۳) احتمال موفقیت حمله چرخشی CubeHash -512 را نشان می‌دهد.

جدول (۳): خلاصه تحلیل رمز چرخشی CubeHash -512

احتمال کل دورها	احتمال تک دور	دورها	تابع چکیده‌ساز
$2^{-57,6}$	$2^{-3,6}$	۱۶-دور	CubeHash-512

جدول (۴): نتایج تحلیل چرخشی بر توابع چکیده‌ساز Shabal-512 , CubeHash-512

احتمال کل	احتمال تک دور	تعداد دور	تابع چکیده‌ساز
$2^{-3393,58}$	–	۳+۱۶	Shabal-512
$2^{-57,6}$	$2^{-3,6}$	۱۶	CubeHash-512

۵- نتیجه‌گیری

در این مقاله برای اولین بار تحلیل رمز چرخشی بر توابع چکیده‌ساز Shabal-512 و CubeHash-512 انجام شد. از آن‌جایی که این توابع خاصیت ARX دارند پس یکی از بهترین حمله‌های شناخته‌شده‌ای که می‌توان برای این توابع چکیده‌ساز انجام داد، تحلیل رمز چرخشی می‌باشد. در این مقاله از یک ابزار قدرتمندی به‌نام فرض مارکوف استفاده شد که نقطه تمایز تحلیل چرخشی انجام‌شده بر توابع چکیده‌ساز CubeHash-512 و Shabal-512 می‌باشد. احتمال موفقیت حمله چرخشی با درنظرگرفتن فرض مارکوف محاسبه می‌شود که باعث کاهش احتمال چرخشی و افزایش پیچیدگی حمله می‌شود، پس طراح می‌تواند با افزایش تعداد جمع‌های پیمانه‌ای، به‌صورت زنجیره‌ای از جمع‌های پیمانه‌ای که خاصیت فرض مارکوف در آن رعایت شده باشد باعث افزایش پیچیدگی شود و حمله به الگوریتم را مشکل سازد. پس با توجه به نکاتی که ذکر شد، در بخش ۴ دیدیم تابع چکیده‌ساز CubeHash-512 احتمال موفقیت چرخشی $2^{-57,6}$ را دارد که در مقایسه با تابع چکیده‌ساز Shabal-512 احتمال موفقیت چرخشی کل آن $2^{-3393,58}$ می‌باشد. پس به‌دلیل نوع طراحی الگوریتم و محل قرارگرفتن جمع‌های پیمانه‌ای تابع چکیده‌ساز Shabal-512 مقاومت بیشتری نسبت به تابع چکیده‌ساز CubeHash-512 در برابر تحلیل رمز چرخشی دارد.

۶- منابع

[1] D. Stinson, “Cryptography Theory and Practice,” CRC, 2006 .

[2] F. Chabaud and A. Joux, “Differential Collisions in SHA-0,” CRYPTO '98, 1998 .

[3] M. Stevens, P. Karpman, and T. Peyrin, “Freestart Collision for Full SHA-1,” Eurocrypt 2016: Advances in Cryptology – Eurocrypt 2016, LNCS, vol. 9665, pp. 459-483, 2016 .

[4] S. Yu, L. Yang, W. Lei, S. Kazuo, and O. Kazuo, “Applications to ECHO and Grøstl,” In Proceedings of Asiacrypt, vol. LNCS 6477, pp. 38-55, 2010 .

[5] S. K. Sanadhya and P. Sarkar, “New Collision Attacks Against up To 24-step SHA-2,” IACR Cryptology, 2008 .

[6] T. Peyrin, "Improved Differential Attacks for ECHO and Grøstl," Cryptology 2010, 2010 .

[7] D. Khovratovich and I. Nikoli´c, "Rotational cryptanalysis of ARX," FSE 2010. LNCS, vol. 6147, pp. 333–346, 2010 .

[8] K. Dmitry, I. Nikolic, J. Pieprzyk, P. Sokolowski, and R. Steinfeld, "Rotational Cryptanalysis of ARX Revisited," IACR Cryptology, 2015 .

[9] D. Bernstein, "CubeHash specification," Department of Computer Science University of Illinois at Chicago Chicago, IL 60607–7045, 2009.

[10] A. Canteaut, T. Pornin, E. Bresson, and T. Icart, "Shabal, a Submission to NIST's Cryptographic Hash Algorithm Competition," Submission to NIST, 2008 .

[11] V. Jha, "Cryptanalysis of Cubehash," Aalto School of Science and Technology, 2010.

[12] E. Brier and T. Peyrin, "Cryptanalysis of CubeHash," ACNS 2009, vol. 5536, pp. 354-368, 2009.

[13] G. V. Assche, "A rotational distinguisher on Shabal's keyed permutation and its impact on the security proofs," 2010.

Journal of Electronical & Cyber Defence
Vol. 6, No. 3, 2018, Serial No. 23

Rotational Cryptanalysis on Shabal and CubeHash

S. A. Tabatabaei Feiz Abad, A. Gaini*, Behbod Keshavarzi

*Imam Hossein University

(Received: 13/08/2017, Accepted: 15/01/2018)

ABSTRACT

Hash functions have a very important role in network and telecommunication security. These functions play an important role in hashing a message which are widely used in cryptographic applications such as digital signatures, random number generator algorithms, authentication protocols, and so on. Rotational cryptanalysis is a relatively new attack that is part of a generic attack on hash functions and is effective on algorithms that have an ARX structure. In this paper, for the first time, we apply a rotational cryptanalysis and with the given assumption of the markov chain for the modular additions sequence employed in two algorithms Shabal and CubeHash, which are second-round candidates for the SHA-3 competition that use the ARX property in their structure. With the implementation of rotational cryptanalysis we arrived at the complexity of $2^{-3393.58}$ for the entire 16+3-rounds Shabal algorithm and the complexity of $2^{-57.6}$ for the entire 16-round CubeHash algorithm. According to the obtained results, it can be seen that due to the large number of modular additions with the given assumption of markov chain, the Shabal algorithm exhibits greater resistance to rotational cryptanalysis, compared to the CubeHash algorithm and is less likely to succeed.

Keywords: Hash Function, Rotational Cryptanalysis, Modular Addition, Markov Chaining

* Corresponding Author Email: againi@ihu.ac.irr