

تحلیل رمز چرخشی روی Shabal و CubeHash

سید علی طباطبائی فیض آباد^۱، احمد گائینی^{۲*}

۱ - استادیار گروه ریاضی و آمار، دانشگاه جامع امام حسین (ع) دانشجوی کارشناسی ارشد،
(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 نسبتاً 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 در نظر 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 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 به علت 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

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 کارایی پایینی دارند). اگرچه تاکنون حمله موفق 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].

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 اندازه 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 الگوریتم SHA-0 [۲] شروع کرد. طولی نکشید که این الگوریتم به‌خاطر مشکل امنیتی آن با [۳] SHA-1 جایگزین شد [۴].

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

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

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

جمع پیمانه‌ای^۵ را به مد 2^n در نظر می‌گیریم، احتمال این‌که جفت چرخشی از جمع پیمانه‌ای بیرون آید توسط لم ۱ محاسبه می‌شود.

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

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

برای n های 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 δ با چرخش و جمع پیمانه‌ای و xor بر n -بیت کلمه در نظر 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 δ که به اندازه r -بیت به سمت راست چرخش داده شده، باشد آن‌گاه با احتمال P_r^q تساوی $\vec{\delta(\vec{I})} = \vec{\delta(\vec{I})}$ برقرار است [۷].

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

به منظور اعمال تحلیل چرخشی، سعی می‌شود تا ورودی‌های طرح ARX تشکیل جفت چرخشی دهند. برای یک تابع تصادفی P که به Z_t^2 نگاشت می‌شود، احتمال این‌که $P(\vec{I}) = \vec{P(\vec{I})}$ باشد برای I تصادفی 2^{-t} است. بنابراین، می‌توانیم یک تابع غیر تصادفی 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 به دست آید. این بدین معنی است که فرض رمز مارکوف استفاده شده برای محاسبه ضمنی احتمال از این طریق امکان‌پذیر نیست.

تحلیل چرخشی^۱ یک حمله نسبتاً جدید است که توسط Ivica Nikolic و Dmitry Khovratovich [۷] در تحلیل سیستم‌های ARX به کار رفته شده است. حمله چرخشی یک حمله احتمالی است که از سیر تکامل یک جفت چرخشی $(x, \vec{x})$ که یکی چرخش^۲ دیگری به اندازه 2^r -بیت است و از طریق دوره‌های یک تابع یا رمز انجام می‌شود، پیروی می‌کند. حمله چرخشی در برابر ساختن قالب‌ها از چندین تابع چکیده‌ساز^۳ مثل Skein, Blake, Keccak,... راه‌اندازی شده است. محاسبه شانس موفقیت حمله‌های احتمالی به صورت یافتن احتمال ورودی‌ها و خروجی‌های متناظرش است که دارای یک خاصیت ویژه‌ای باشند که برای یک تابع یا جایگزشت 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). Nikolic و Khovratovich [۷] مقاله قبلی خود را که فقط تعداد جمع‌های پیمانه‌ای را در نظر گرفته بودند و فرض مارکوف بودن در آن رعایت نشده بود را مورد بازبینی قرار دادند و یک احتمال جدید برای محاسبه پیچیدگی حمله چرخشی با توجه به مارکوف بودن آن ارائه 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 ارائه می‌گردد.

۲- تشریح تحلیل رمز چرخشی

در [۷] روش کلی برای تحلیل سیستم‌های ARX نشان داده شده است، ایده کلی فرض جفت کلمه‌ها است که یکی چرخش دیگری به اندازه 2^r -بیت می‌باشد. که عملگرهای چرخشی به وسیله $r \lll r$ یا $r \gg r$ و یا به طور معادل $\vec{x}$ و $\vec{x}$ تعریف می‌شوند که $\vec{x}$ چرخش x به اندازه 2^r -بیت به سمت راست را نشان می‌دهد و $(x, \vec{x})$ را جفت چرخشی به اندازه 2^r -بیت می‌نامیم. اثبات این‌که یک جفت چرخشی با هر تبدیل بیتی حفظ می‌شود آسان است مخصوصاً یای انحصاری^۴ و چرخش که در رابطه (۱) نشان داده است [۷]:

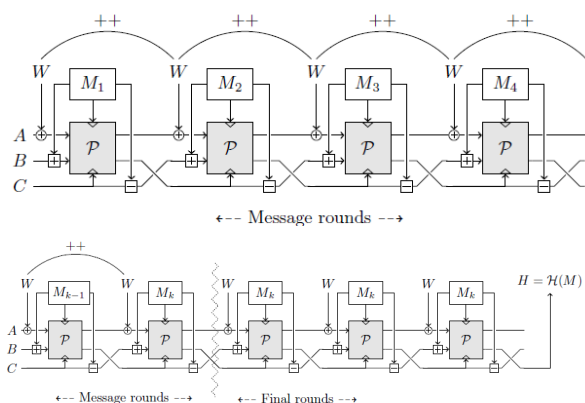
1- Rotational Cryptanalysis

2- Rotation

3- Hash Function

4- Xor

5- Modular Addition



شکل (۱): ساختار کلی Shabal [۱۰]

ساختار تابع چکیده ساز Shabal از یک بافر^۲ داخلی که طول فضای حالت داخلی آن ۱۴۰۸ بیت می باشد، استفاده می کند که به سه بخش $(A, B, C) \in \{0,1\}^{l_a} \times \{0,1\}^{l_m} \times \{0,1\}^{l_m}$ تقسیم می شود که در ابتدا مقادیر اولیه (A_0, B_0, C_0) را می گیرند. یک بافر کمکی $W \in \{0,1\}^{l_m}$ به عنوان شمارنده تعداد بلوک های پیام استفاده می شود. این ساختار از کلید جایگشتی $\mathcal{P}$ استفاده می کند که در رابطه (۵) نشان داده می شود [۱۰].

$$p = \{0,1\}^{l_m} \times \{0,1\}^{l_a} \times \{0,1\}^{l_m} \times \{0,1\}^{l_m} \rightarrow \{0,1\}^{l_a} \times \{0,1\}^{l_m} \quad (5)$$

در شکل (۲) کد زیرکلید جایگشتی استفاده شده در Shabal در الگوریتم را نشان می دهد.

```

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

For i from 0 to 15, do:
    • B[i] ← B[i] ≪ 17
Next i

For j from 0 to p - 1, do:
    • For i from 0 to 15, do:
        - Compute
          A[i + 16j mod r] ← U(A[i + 16j mod r] ⊕ V(A[i - 1 + 16j mod r] ≪ 15)
                               ⊕ C[8 - i mod 16])
                               ⊕ B[i + o1 mod 16]
                               ⊕ (B[i + o2 mod 16] ∧ B[i + o3 mod 16])
                               ⊕ M[i]
          where (o1, o2, o3) = (13, 9, 6)
          - B[i] ← (B[i] ≪ 1) ⊕ A[i + 16j mod r]
    • Next i
Next j

For j from 0 to 35, do:
    • A[j mod r] ← A[j mod r] ⊕ C[j + 3 mod 16]
Next j
    
```

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

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

$$p_r = (v_{i+1} = \beta_{i+1} | v_i = \beta_i, v_{i-1} = \beta_{i-1}, \dots, v_0 = \beta_0) \quad (3)$$

$$= p_r(v_{i+1} = \beta_{i+1} | v_i = \beta_i)$$

احتمال چرخشی ARX به سادگی با شمارش تعداد جمع محاسبه نمی شود و باید موقعیت جمع های پیمانه ای بررسی شوند، یعنی این که آیا جمع های پیمانه ای به صورت متوالی در الگوریتم آمده اند یا جدا جدا و در بین عملگرهای دیگر آمده اند. درحقیقت، زنجیره بزرگتر برای جمع های پیمانه ای احتمال چرخشی کمتری دارد. احتمال چرخشی جمع های پیمانه ای زنجیره ای در لم ۲ آمده است:

لم ۲: اگر $a_1, \dots, a_k$ کلمه های n -بیتی تصادفی باشند و برای $0 < r < n$ که یک عدد صحیح مثبت باشد، آن گاه احتمال چرخشی از رابطه (۴) به دست می آید [۸].

$$p_r = ((a_1 \boxplus a_2) \lll r = a_1 \lll r \boxplus a_2 \lll r) \wedge [(a_1 \boxplus a_2 \boxplus a_3) \lll r = a_1 \lll r \boxplus a_2 \lll r \boxplus a_3 \lll r] \wedge \dots \wedge [(a_1 \boxplus \dots \boxplus a_k) \lll r = a_1 \lll r \boxplus \dots \boxplus a_k \lll r]$$

$$= \frac{1}{2^{nk}} \cdot \binom{k + 2^r - 1}{2^r - 1} \cdot \binom{k + 2^{n-r} - 1}{2^{n-r} - 1} \quad (4)$$

به طور خلاصه، احتمال چرخشی لزوماً برابر با حاصل ضرب تک تک احتمال موفقیت حمله چرخشی نیست. چنین میان بری در تخمین احتمال نه کران بالا نه کران پایین از احتمال واقعی را می دهد. بعد از تایید زنجیره مارکوف^۱ می توان احتمال را تخمین زد در غیر این صورت، احتمال چرخشی باید اقتضایی محاسبه گردد.

۳- معرفی توابع چکیده ساز CubeHash, Shabal

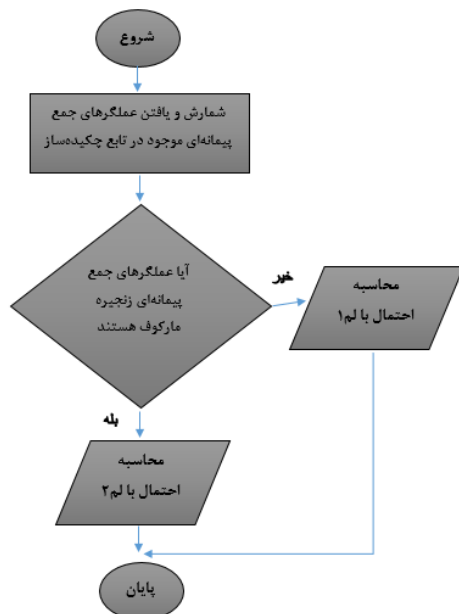
این بخش به معرفی مختصری از توابع چکیده ساز Shabal و CubeHash می پردازد و آن ها را براساس الزامات تحلیل رمز چرخشی یعنی شمارش تعداد جمع های پیمانه ای به کار رفته شده در هر الگوریتم و بررسی این که آیا این جمع های پیمانه ای به صورت مارکوف هستند یا خیر، آنالیز می شود.

۳-۱- تابع چکیده ساز Shabal

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

۴- اعمال تحلیل رمز چرخشی روی Shabal و CubeHash

در این بخش با توجه به الگوریتم‌های معرفی شده در بخش‌های ۱-۳ و ۲-۳ با رویکرد [۷-۸]، 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 در نظر گرفتن مقدار چرخشی r (در این جا تحلیل چرخشی با مقدار چرخشی $r = 1$ در نظر گرفته می‌شود) و صرف نظر کردن از ثابت‌ها (در صورت وجود) و n -بیت کلمه (با توجه به الگوریتم) محاسبه می‌شود و در غیر این صورت، از لم ۱ برای محاسبه احتمال چرخشی استفاده می‌شود. به عنوان مثال، برای تابع چکیده ساز Shabal-512 با k جمع پیمانه‌ای و n -بیت کلمه و مقدار چرخش r با توجه به نوع تابع چکیده ساز از لم‌های ۱ و ۲ استفاده می‌شود. تمام محاسبات با استفاده از نرم افزار 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 چکیده ساز Shabal-512 به کار 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 به صورت تکی داریم که عملگر تفریق و

۲-۳- الگوریتم CubeHash

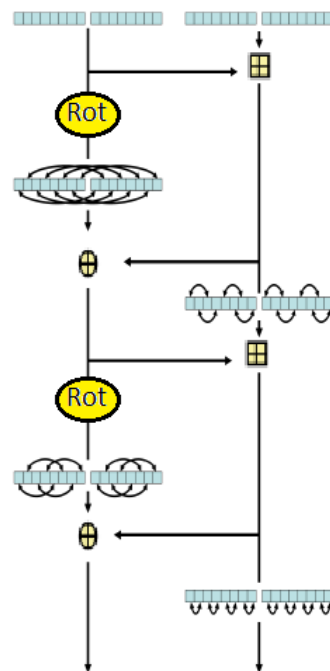
CubeHash $r/b-h$ سه پارامتر دارد که r مشخص کننده تعداد دورهای تبدیل فضای حالت، b تعداد بیت‌ها در هر بلوک و h طول بیت‌های چکیده پیام می‌باشد. به غیر از این پارامترها، CubeHash یک فضای حالت داخلی ۱۰۲۴-بیتی دارد.

در اولین دور مسابقه NIST، پارامترهای $b=1$ ، $r=8$ 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-بیتی (۱۰۲۴-بیتی) را به صورت تابعی از (h, b, r) مقداردهی اولیه می‌شود.
- (۲) تبدیل پیام ورودی به پیام لایه گذاری شده، پیام لایه گذاری شده شامل یک یا چند بلوک b -بیتی است.
- (۳) xor کردن بلوک به اولین b -بیت‌های فضای حالت برای هر بلوک b -بیتی از پیام لایه گذاری شده و سپس از طریق r دور یکسان حالت معکوس را به دست می‌آوریم.
- (۴) به پایان رساندن فضای حالت
- (۵) خروجی گرفتن از اولین $h/8$ بیت‌ها از فضای حالت

شکل (۳)، الگوریتم CubeHash را نشان می‌دهد:



شکل (۳): الگوریتم CubeHash [۱۱]

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 به نام فرض مارکوف استفاده شد که نقطه تمایز تحلیل چرخشی انجام‌شده بر توابع چکیده‌ساز CubeHash-512 و Shabal-512 می‌باشد. احتمال موفقیت حمله چرخشی با در نظر گرفتن فرض مارکوف محاسبه می‌شود که باعث کاهش احتمال چرخشی و افزایش پیچیدگی حمله می‌شود، پس طراح می‌تواند با افزایش تعداد جمع‌های پیمانه‌ای، به صورت 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 به دلیل نوع طراحی الگوریتم و محل قرار گرفتن 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 Asiaticrypt, 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.

جمع پیمانه‌ای در این جا احتمال چرخشی برابری دارند و با توجه به این که تا این جا این دو جمع پیمانه‌ای بررسی شده مارکوف نیستند پس بنا به لم ۱ با در نظر گرفتن $r = 1, n = 32$ احتمال چرخشی هر کدام برابر با $2^{-1,415}$ می‌باشد که احتمال این دو برابر $2^{-2,83} = 2^{-1,415 \times 2}$ می‌باشد. برای مابقی جمع‌های پیمانه‌ای همان‌طور که در شکل (۱) می‌توان دید، هر کدام از جمع‌های پیمانه‌ای با عملگر تفریق به صورت مارکوف زنجیر شده‌اند که ۱۸ تا از این زنجیره‌ها داریم که هر کدام بنا به لم ۲ با در نظر گرفتن مقادیر $r = 1, n = 32$ احتمال چرخشی برابر با $2^{-3,6}$ دارند که احتمال آن برابر $2^{-64,8} = 2^{-3,6 \times 18}$ است. همچنین، برای کلیدهای جایگشتی P بنا به شکل (۲) در قسمت انتهایی کد، ۳۶ جمع پیمانه‌ای به صورت 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 $2^{-3325,95} = 2^{-175,05 \times 19}$ 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

۲-۴- تحلیل رمز چرخشی بر روی CubeHash

با توجه به شکل (۳)، دو جمع پیمانه‌ای داریم که به صورت زنجیره مارکوف می‌باشند که بنا به لم ۲ و با در نظر گرفتن 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 به صورت مارکوف می‌باشد پس احتمال کل برای آن برابر $2^{-57,6} = 2^{-3,6 \times 16}$ 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

- [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.
- [6] T. Peyrin, "Improved Differential Attacks for ECHO and Grøstl," Cryptology 2010, 2010 .
- [7] D. Khovratovich and I. Nikolić, "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.

Rotational Cryptanalysis on Shabal and CubeHash

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

*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 $2^{33.58}$ 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.ir