Journal of Electronical & Cyber Defence
Vol. 9, No. 1, 2021, Serial No. 33

Improvement of Rotational Cryptanalysis of Shabal and Cubehash Hash Functions

M. Aboei Mehrizi, J. alizadeh*

*Imam Hossein Comprehensive University

(Received: 12/04/2020, Accepted: 05/08/2020)

ABSTRACT

A cryptographic hash function maps an arbitrary length input to a fixed length output. These functions are used in many cryptographic applications such as digital signatures. They must be secure against collision, preimage and 2-preimage attacks. Rotational cryptanalysis is an approach to the analysis of ARX ciphers. The Hash functions Shabal and Cubehash, which are two candidates of the second round of the SHA-3 competition, have an ARX structure. They have been analyzed with respect to rotational cryptanalysis by Tabatabaei et al. In this paper we consider their analysis and present some observations. Our observations show that the results of Tabatabaei et al.'s cryptanalysis are not accurate. Then we present some new results about rotational cryptanalysis of Shabal and Cubehash. Thereafter we present some new results and show that rotational cryptanalysis is effective on a smaller number of rounds on Shabal and Cubehash Hash functions.

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

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

نشریه علمی "پدافند الکترونیکی و سایبری"
سال نهم، شماره ۱، بهار ۱۴۰۰، ص ۱۰۰-۹۱

علمی – پژوهشی

بهبود تحلیل چرخشی توابع چکیده‌ساز Cubehash و Shabal

مجید ابوئی مهریزی[۱]، جواد علیزاده[۲*]

۱- کارشناس ارشد، و ۲- استادیار، گروه رمز و امنیت، دانشگاه جامع امام حسین(ع)

(دریافت:.۱۳۹۹/۰۱/۲۴، پذیرش: ۱۳۹۹/۰۵/۱۵)

چکیده

یک تابع چکیده‌ساز رمزنگاری، ورودی‌های با طول دلخواه را به یک مقدار چکیده با اندازه ثابت تبدیل می‌کند. توابع چکیده‌ساز در بسیاری از کاربردهای رمزنگاری مانند امضای رقمی به کار می‌روند و می‌بایست در برابر برخورد، پیش تصویر و پیش تصویر دوم مقاوم باشند. تحلیل چرخشی به‌عنوان یک روش تحلیل رمز برای تحلیل الگوریتم‌هایی که در ساختارشان از سه عملگر چرخش، جمع پیمانه‌ای و XOR استفاده می‌کنند، یعنی سامانه‌های ARX معرفی شده است. توابع چکیده‌ساز Shabal و Cubehash که از نامزدهای دور دوم مسابقه SHA-3 هستند، جزو ساختارهای ARX دسته‌بندی می‌شوند. این توابع توسط طباطبایی و همکاران با استفاده از تحلیل چرخشی مورد ارزیابی قرار گرفته‌اند. با بررسی‌های صورت گرفته مشخص شد این تحلیل‌ها تحلیل‌های دقیقی نیستند. در این مقاله تحلیل چرخشی روی توابع چکیده‌ساز ذکرشده با دقت بیشتری مورد مطالعه و بررسی قرار می‌گیرد. این کار با توجه به برخی نتایج جدید در حوزه تحلیل چرخشی انجام می‌شود و نشان داده می‌شود که در مقایسه با کار طباطبایی و همکاران، تحلیل چرخشی روی تعداد دور کمتری از توابع چکیده‌ساز Shabal و Cubehash مؤثر است.

کلیدواژه‌ها: تابع چکیده‌ساز، تحلیل چرخشی، جمع پیمانه‌ای، زنجیره مارکوف.

۱- مقدمه

توابع چکیده‌ساز رمزنگاری، در بسیاری از کاربردهای رمزنگاری، مانند طرح‌های امضای رقمی و پروتکل‌های احراز اصالت به‌کار می‌روند و از ابزارهای مهم در رمزنگاری مدرن هستند. یک تابع چکیده‌ساز، مانند 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، پیش تصویر دوم و پیش تصویر اشاره کرد [۱].

مؤسسهٔ ملّی استانداردها و فناوری آمریکا[1] (NIST) کار استانداردسازی الگوریتم‌های چکیده‌ساز را در سال ۱۹۹۳، با انتشار الگوریتم SHA-0 [۲] شروع کرد. طولی نکشید که این الگوریتم، به‌خاطر مشکل امنیتی آن، با SHA-1 [۳] جایگزین شد. در ادامه، در سال ۲۰۰۲، این موسسه، توابع چکیده‌ساز خانوادهٔ SHA-2 [۴] را به مجموعه الگوریتم‌های چکیده‌ساز استاندارد خود اضافه کرد. در سال‌های ۲۰۰۴ و ۲۰۰۵، پیشرفت‌هایی در رابطه با تحلیل توابع چکیده‌ساز پرکاربرد و استاندارد حاصل شد [۵، ۶] که یکی از این موارد مربوط به حمله موفقیّت‌آمیز روی SHA-1 بود. به همین دلیل NIST برای یک تابع چکیده‌ساز استاندارد امن جدید احساس نیاز کرد و در نوامبر ۲۰۰۷، از برگزاری یک مسابقهٔ عمومی برای انتخاب استاندارد چکیده‌ساز جدید و امن به نام SHA-3 [۷] خبر داد و یک سری الزامات اوّلیه برای نامزدهای این مسابقه مشخص کرد [۸]. در ابتدا ۵۱ نامزد به دور اول مسابقه ارسال شدند که از این ۵۱ طرح، ۱۴ طرح به مرحله دوم راه پیدا کردند. در نهایت ۵ نامزد نهایی معرفی شدند و از میان این نامزدها، تابع Keccak به‌عنوان برنده مسابقه و استاندارد SHA-3 معرفی شد.

تحلیل چرخشی روشی مؤثر به‌منظور تحلیل ساختارهای رمزنگاری متقارن ARX (که در آنها از سه عمل اصلی جمع پیمانه‌ای، چرخش بیتی و XOR استفاده می‌شود) است که نخستین بار توسط دیمیتری خوراتویچ و ایویکا نیکولیچ در سال ۲۰۱۰ مطرح شد [۹]. در این روش انتشار زوج‌های چرخشی در توابع به‌کاررفته در یک ساختار ARX مورد مطالعه و بررسی قرار می‌گیرد. این روش تحلیل در مدل حمله متن آشکار انتخابی انجام می‌شود. در سال ۲۰۱۵ ادعایی مطرح شد مبنی بر اینکه زمانی که زنجیره‌ای از عملگرهای جمع پیمانه‌ای در ساختار وجود

* رایانامه نویسنده پاسخگو: jaalizadeh@ihu.ac.ir

[1] National Institute of Standards and Technologies (NIST)

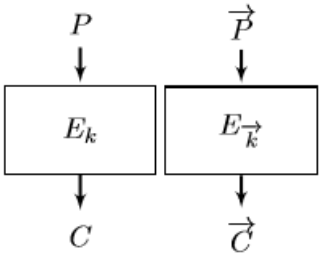
داشته باشد، دیگر نمی‌توان بر اساس استدلال ارائه‌شده در [۹] عمل کرد و احتمال حفظ ویژگی چرخشی به‌مراتب پایین‌تر خواهد بود. بر همین اساس خوراتویچ و همکاران در [۱۰]، تحلیل چرخشی ساختارهای Blake2 و Skein را با این دیدگاه که در آن‌ها زنجیره‌ای از عملگرهای جمع پیمانه‌ای وجود دارد، مورد بازبینی قرار دادند. یکی از مسائلی که تحلیل چرخشی ساختارهای ARX را با محدودیت مواجه می‌کند، حضور ثابت‌های دوری در چنین ساختارهایی می‌باشد. در سال ۲۰۱۶ محققان در [۱۱] مفهومی تحت عنوان RX-تفاضل را مطرح کردند که می‌توانست این محدودیت را رفع کند. در سال ۲۰۱۷ آن‌ها روش خود را خودکارسازی کردند [۱۲] و با استفاده از این روش خودکار، نسخه‌های مختلف رمز قالبی Speck را مورد ارزیابی قرار دادند [۱۲].

در سال ۲۰۱۸ طباطبایی و همکاران از روش تحلیل چرخشی استفاده کرده و دو تابع چکیده‌ساز Shabal و Cubehash، از نامزدهای دور دوم مسابقه SHA-3 را مورد ارزیابی قرار دادند. آنها برای ۱۹ دور Shabal و نیز ۱۶ دور Cubehash تمایزگرهایی با پیچیدگی به ترتیب $2^{3393.58}$ و $2^{57.6}$ ارائه کردند [۱۳]. در این مقاله تحلیل چرخشی روی دو تابع چکیده-ساز ذکرشده مورد بازنگری قرار می‌گیرد و نشان داده می‌شود که نتایج تحلیل ارائه‌شده توسط طباطبایی و همکاران از دقت لازم برخوردار نیستند. با توجه به نتایج این مقاله می‌توان گفت که با استفاده از تحلیل چرخشی می‌توان حداکثر برای ۵ دور Shabal و نیز ۷ دور Cubehash، به ترتیب با پیچیدگی $2^{1282.27}$ و یک تمایزگر از نوع چرخشی به‌دست آورد.

ادامه مطالب این مقاله به این صورت سازمان‌دهی شده است که در بخش ۲، تحلیل چرخشی روی رمزهای متقارن ARX تشریح می‌شود. در بخش ۳، روش تحلیل طباطبایی و همکاران روی دو تابع Shabal و Cubehash تشریح می‌شود. در بخش ۴، تحلیل چرخشی دو تابع ذکرشده مورد بازبینی قرار داده‌شده و نشان داده می‌شود که نتایج ذکرشده در بخش ۳ از دقت کافی برخوردار نیستند. در نهایت نتیجه‌گیری مقاله در بخش ۵ ارائه می‌شود.

۲- تشریح تحلیل چرخشی

تحلیل چرخشی یک حمله از نوع ساختاری آماری است که در آن انتشار یک زوج چرخشی از طریق تابع رمزنگاری مورد مطالعه و بررسی قرار می‌گیرد. از این ویژگی در وهله اول برای تمایز رمز از یک تابع تصادفی و در وهله دوم برای حمله کشف کلید روی آن استفاده می‌شود. ایده اصلی حمله این است که یک زوج از کلمات در نظر گرفته شود که یکی از کلمات چرخش یافته کلمه دیگر است. سپس بررسی می‌شود که خروجی تابعی که ورودی آن کلمه چرخش یافته بوده است، چه مقدار به خروجی چرخش یافته تابعی که ورودی آن کلمه اصلی بوده است، نزدیک می‌باشد. این توضیحات در شکل (۱) نشان داده شده است.



شکل (۱): زوج‌های چرخشی ورودی و خروجی در الگوریتم رمزنگاری E [۱۲].

عمل چرخش درون کلمه‌ای با r ⋙ و یا r ⋙ نشان داده می‌شود. متغیر چرخش یافته نیز با $\vec{X}$ و یا $\bar{X}$ نشان داده می‌شود. اکنون اگر فرض شود $\vec{X}$ چرخش یافته Xبه اندازه r بیت به سمت راست باشد، زوج (Xو$\vec{X}$) یک زوج چرخشی نامیده می‌شود(با چرخش به اندازه r بیت). می‌توان بررسی کرد که عملگرهای XOR و چرخش ویژگی چرخشی را با احتمال ۱ حفظ می‌کنند [۹]. یعنی

$$\overrightarrow{X \oplus Y} = \vec{X} \oplus \vec{Y}\,.\quad \vec{X} \ggg r' = \overrightarrow{X \ggg r'} \qquad (۱)$$

همچنین احتمال حفظ ویژگی چرخشی برای یک زوج چرخشی توسط عملگر جمع پیمانه‌ای توسط رابطه زیر بیان می‌شود [۹]:

$$\mathrm{P}(\overrightarrow{x+y} \quad \vec{x}+\vec{y}) \quad -(1 \qquad) \qquad (۲)$$

با توجه به رابطه (۲)، برای n بزرگ و r کوچک، احتمال حفظ ویژگی چرخشی، مطابق جدول (۱) به‌دست می‌آید [۹]:

جدول (۱): احتمال حفظ ویژگی چرخشی در عمل جمع پیمانه‌ای [۹].

R		(p_r)
1	0.375	-1.415
2	0.313	-1.676
3	0.281	-1.831

برای $r = \frac{n}{2}$ این احتمال نزدیک به $\frac{1}{4}$ است. روابط فوق برای چرخش به چپ هم صادق است. حال اگر یک طرح دلخواه مانند

S شامل جمع پیمانه‌ای و چرخش و XOR روی کلمات n بیتی در نظر گرفته شود،آنگاه قضیه زیر اثبات می‌شود:

قضیه ۱ [۹]. فرض کنید S یک سیستم ARX بوده و تعداد عملیات جمع پیمانه‌ای در s برابر با q باشد و $\vec{I}$ چرخش یافته I به سمت راست به میزان r باشد که به سیستم S وارد می‌شود. در این صورت با احتمال $(p_r)^q$،خواهیم داشت $S(\vec{I}) = \overrightarrow{S(I)}$، که در آن p_r احتمال این است که یک جمع پیمانه‌ای بتواند ویژگی چرخش را حفظ کند.

درنتیجه برای یک تابع تصادفی مانند S که طول خروجی آن t بیت است، احتمال اینکه $p(\vec{I}) = \overrightarrow{p(I)}$ باشد، برابر با 2^{-t} است. بنابراین اگر یک تابع با تعداد q جمع پیمانه‌ای به‌گونه‌ای بتواند پیاده‌سازی شود که $(p_r)^q > 2^{-t}$ باشد، در این صورت از این ویژگی می‌توان برای تشخیص عدم تصادفی بودن تابع استفاده کرد. به‌عنوان مثال زمانی که $r = 1$ باشد، هر طرح ARXای که در ساختار خود تعداد کمتر از $\frac{t}{1.415}$ جمع پیمانه‌ای داشته باشد در برابر تحلیل چرخشی آسیب‌پذیر خواهد بود.

در روابط فوق اعتقاد بر این است که احتمال موفقیت تحلیل چرخشی روی رمزها و توابع مبتنی بر ARX تنها به تعداد جمع‌های پیمانه‌ای به‌کاررفته در ساختار بستگی دارد. در [۱۰] خوراتویچ و همکاران نشان دادند که احتمال حفظ ویژگی چرخشی، علاوه بر تعداد عملگرهای جمع پیمانه‌ای به‌کاررفته در ساختار، به موقعیت قرارگیری آن‌ها نیز بستگی دارد. روابط فوق تا زمانی صحیح است که عملگرهای جمع پیمانه‌ای به‌کاررفته در ساختار یک زنجیره (به عبارت دیگر زنجیره مارکف) را تشکیل ندهند. درصورتی‌که بیشتر عملگرهای جمع‌های پیمانه‌ای در طراحی رمزهای ARX به‌صورت زنجیر هستند و یا به عبارت دیگر خروجی جمع پیمانه‌ای قبلی ورودی جمع پیمانه‌ای بعدی است که این باعث می‌شود احتمال چرخشی به‌مراتب کمتر شود [۱۰]. برای بهبود احتمال حفظ ویژگی چرخشی توسط جمع‌های پیمانه‌ای در حضور زنجیره عملگرهای جمع پیمانه‌ای، قضیه زیر مطرح می‌شود [۱۰].

قضیه ۲ [۱۰]. فرض کنید $a_1' \dots' a_k$ کلمات n بیتی هستند که به‌صورت تصادفی انتخاب شده‌اند و r یک عدد صحیح مثبت باشد به‌طوری که $0 < r < n$. آنگاه

$$\Pr([(a_1 + a_2) \lll r = a_1 \lll r + a_2 \lll r] \wedge [(a_1 + a_2 + a_3) \lll r = a_1 \lll r + a_2 \lll r + a_3 \lll r] \wedge \dots \wedge [(a_1 + \dots + a_k) \lll r = a_1 \lll r + \dots + a_k \lll r]) = \frac{1}{2^{nk}} \binom{k+2^r-1}{2^r-1} \binom{k+2^{n-r}-1}{2^{n-r}-1} \quad (۳)$$

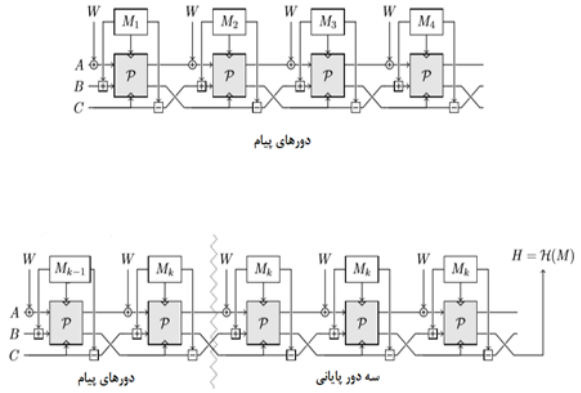
۳- تحلیل چرخشی توابع چکیده‌ساز Cubehash و Shabal توسط طباطبائی و همکاران

در این بخش، ابتدا توابع چکیده‌ساز Cubehash و Shabal به‌طور مختصر معرفی می‌شوند. سپس تحلیل چرخشی روی آنها که توسط طباطبائی و همکاران ارائه‌شده است، بررسی شده و مشاهداتی در رابطه با این تحلیل‌ها گزارش می‌شود.

۳-۱- معرفی تابع چکیده‌ساز Shabal

تابع چکیده‌ساز Shabal مبتنی بر استفاده از جایگشت P است و بر اساس بلوک‌های پیام ۵۱۲ بیتی کار می‌کند. Shabal از خروجی‌های به طول $L_h = \{192,224,256,384,512\}$ پشتیبانی می‌کند. حالت داخلی Shabal شامل سه بافر A، B و C است که A، ۱۲ کلمه ۳۲ بیتی و B و C، ۱۶ کلمه ۳۲ بیتی می‌باشند (بنابراین طول فضای حالت داخلی Shabal ۱۴۰۸ بیت است). مقادیر اولیه این بافرها A_0، B_0 و C_0 است که بسته به طول خروجی، مقادیر متفاوتی را به خود می‌گیرند [۱۵].

Shabal از یک بافر کمکی $(W \in Z_2^{64})$ به‌منظور شمارش تعداد بلوک‌های پیام استفاده می‌کند. با توجه به نقش W، این شمارنده را نمی‌توان به‌عنوان بخشی از حالت داخلی به شمار آورد. Shabal متشکل از k دور برای پوشش دادن بلوک‌های پیام و ۳ دور پایانی است. به عبارت دیگر پس از اینکه تمامی بلوک‌های پیام توسط k دور پوشش داده شدند، ساختار ۳ دور دیگر برای آخرین بلوک پیام تکرار می‌شود [۱۵]. در شکل (۲) ساختار تابع چکیده‌ساز Shabal آورده شده است.



شکل (۲): ساختار تابع درهم‌ساز Shabal [۱۵].

در هر دور Shabal عملیات زیر انجام می‌شود [۱۵]:

- XOR شدن بافر A با شمارنده بلوک پیام (W)
- اضافه شدن بلوک پیام (M) از طریق جمع پیمانه‌ای به بافر B

- استفاده از جایگشت P به‌منظور تولید A و B جدید
- کم کردن بلوک پیام (M) از بافر C
- جابه‌جا کردن B و C با یکدیگر

جایگشت P در Shabal شامل سه گام است. در گام اول تنها کلمات بافر B تغییر پیدا می‌کند. در گام دوم کلمات بافرهای A و B به‌صورت هم‌زمان تغییر پیدا می‌کنند و در گام سوم تنها کلمات بافر A تغییر پیدا می‌کند [۱۶]. در جایگشت کلید Shabal عملگرهای جمع پیمانه‌ای، XOR، AND، چرخش و همچنین U (به معنای ضرب در ۳ به پیمانه 2^{32})، V (به معنای ضرب در ۵ به پیمانه 2^{32}) و $\overline{a}$ (به معنای متمم مقدار a) استفاده می‌شود.

گام‌های جایگشت Shabal به شرح زیر است [۱۶]:

۱. $B = B \lll 17$) هر یک از ۱۶ کلمه ۳۲ بیتی بافر B به مقدار ۱۷ بیت به سمت چپ چرخش داده می‌شوند).

۲. در این گام کلمات بافرهای A و B هم‌زمان به‌صورت زیر تغییر پیدا می‌کنند.

```
for i=0 to 2 do
    for j = 0 to 15 do
        A[j + 16i  mod 12]
                ← u(A[j + 16i  mod 12] ⊕
        v(A[j − 1 + 16i  mod 12] ⋘ 15) ⊕
        C[8 − j  mod 16]) ⊕
        B[j + 13  mod 16] ⊕
        (B[j + 9  mod 16] ∧ ¬B[j + 6  mod 16])
        ⊕ M[j]
        B[j] ← (B[j] ⋘ 1) ⊕ A[j
                + 16i  mod 12]
    end for
end for
```

۳. در این گام تنها کلمات بافرهای A تغییر پیدا می‌کنند.

```
for j = 0 to 35 do    A[j  mod 12]
                ← A[j  mod 12] + C[j + 3  mod 16]
```

۳-۲- تحلیل چرخشی تابع چکیده‌ساز Shabal توسط طباطبائی و همکاران

با توجه به شکل (۲) در کل برای ۱۹ دور از ساختار Shabal، ۱۹ جایگشت P به‌کار برده می‌شود که قبل از اولین جایگشت تنها یک جمع پیمانه‌ای و در انتهای ساختار نیز یک تفریق پیمانه‌ای به‌کار برده می‌شود. عملگر تفریق و جمع پیمانه‌ای، احتمال حفظ ویژگی چرخشی برابری دارند و با توجه به اینکه این دو عملگر مارکف نیستند، بنا به رابطه (۲) و با در نظر گرفتن مقدار چرخش $r = 1$ و اندازه کلمه ۳۲ بیت، احتمال حفظ ویژگی چرخشی هر کدام برابر $2^{-1.415}$ و درنتیجه احتمال مجموع این دو عملگر $2^{-1.415\times 2} = 2^{-2.83}$ می‌شود. برای ما بقی جمع‌های پیمانه‌ای همان‌طور که در شکل (۲) مشخص است، هرکدام از جمع‌های پیمانه‌ای با عملگر تفریق پیمانه‌ای به‌صورت زنجیره مارکف هستند که برای ۱۹ دور، ۱۸ تا از چنین زنجیره‌هایی وجود دارد. بر اساس رابطه (۳) و همچنین با در نظر گرفتن مقدار چرخش $r = 1$، احتمال حفظ ویژگی چرخشی برای هر کدام از این زنجیره‌ها $2^{-3.585}$ و برای ۱۸ زنجیره احتمالی برابر $2^{-3.585\times 18} = 2^{-64.53}$ دارد. همچنین برای جایگشت P با توجه به سومین گام، یک زنجیره ۳۶ تایی از عملگرهای جمع پیمانه‌ای وجود دارد که به‌صورت مارکف هستند. با توجه به رابطه (۳) احتمال حفظ ویژگی چرخشی این زنجیره ۳۶ تایی $2^{-175.05}$ است و برای ۱۹ دور این احتمال $= 2^{-175.05\times 19}$ $2^{-3325.95}$ می‌باشد. پس احتمال حفظ ویژگی چرخشی برای ۱۹ دور از ساختار Shabal، $2^{-3393.31}$ خواهد بود.

۳-۳- مشاهدات روی روش تحلیل چرخشی Shabal توسط طباطبائی و همکاران

در این بخش مشاهدات روی روش تحلیل چرخشی Shabal توسط طباطبائی و همکاران به‌صورت زیر بیان می‌شود:

۱- در Shabal محاسبات روی کلمات ۳۲ بیتی صورت می‌گیرد. بنابراین بین هر تفریق و جمع پیمانه‌ای ۱۶ زنجیره وجود دارد و هر زنجیره ۲ عملگر جمع و تفریق پیمانه‌ای را شامل می‌شود.

۲- در گام دوم از جایگشت P، عملگرهای U و V ویژگی چرخشی را به‌صورت احتمالی حفظ می‌کنند که این موضوع در تحلیل طباطبائی و همکاران نادیده گرفته شده است.

۳- در گام سوم، جمع‌های پیمانه‌ای به‌صورت مارکف نیستند و ۳۶ جمع پیمانه‌ای اتفاق می‌افتد.

۴- مقداری که برای احتمال موفقیت تحلیل چرخشی به‌دست آورده شده است، کوچک‌تر از 2^{-1408} است که نشان می‌دهد نمی‌توان ۱۹ دور از ساختار Shabal را تمایز داد.

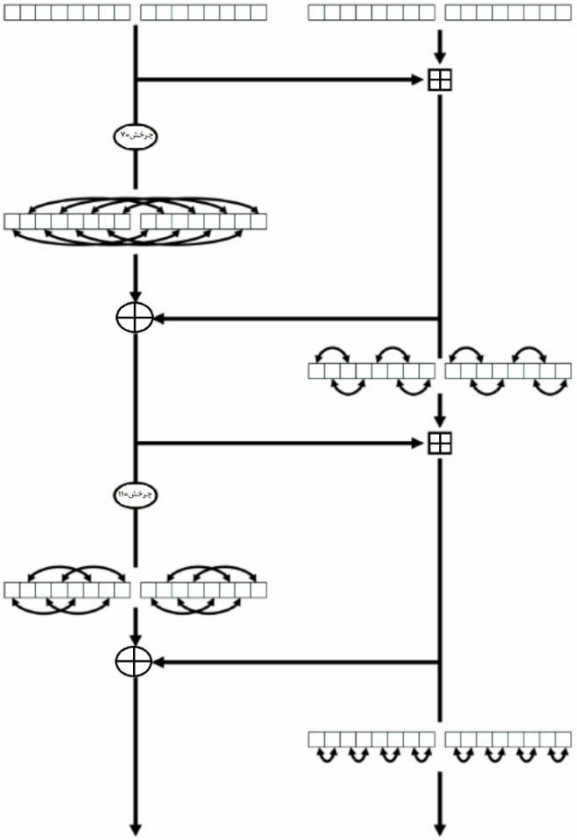
۳-۴- معرفی تابع چکیده‌ساز Cubehash

Cubehash روی کلمات ۳۲ بیتی (n=32) کار می‌کند و از سه عملگر ساده جمع پیمانه‌ای، چرخش بیتی و XOR و همچنین چهار تابع SWAP که به‌صورت $SWAP_1$، $SWAP_2$، $SWAP_3$ و $SWAP_4$ نشان داده می‌شود، استفاده می‌کند [۱۷]. Cubehash یک حالت درونی ۳۲ کلمه‌ای مانند $S = (S_0, S_1, \dots, S_{31})$ دارد و انواع مختلف آن به‌صورت Cubehash-r/b توسط دو پارامتر $r \in \{1,2,3,\dots,128\}$ و $b \in \{1,2,3,\dots,128\}$ نشان داده می‌شود

که در r دور بلوک‌های b بایتی پردازش می‌شوند. مقادیر مختلف r و b بسته به میزان امنیت مورد نظر انتخاب می‌شوند. حالت درونی S بسته به طول پیام چکیده (محدود به ۵۱۲ بیت) و پارامترهای r و b، مقدار مشخصی را به خود می‌گیرد. پیام ورودی لایه گذاری شده و به بلوک‌های پیام b بایتی تقسیم می‌شوند. در هر دور بلوک پیام با اولین b بایت فضای حالت، XOR می‌شود (حالت درونی ۳۲ کلمه‌ای S به‌صورت یک مقدار ۱۲۸ بایتی در نظر گرفته می‌شود). سپس، جایگشت زیر r بار به‌کار برده می‌شود [۱۷]. جایگشت زیر، تابع دور Cubehash می‌باشد که در شکل (۳) نشان داده شده است.

۱) اضافه کردن s_i به s_{i+16} از طریق جمع پیمانه‌ای به ازای $0 \le i \le 15$.
۲) چرخش s_i به میزان ۷ بیت به سمت چپ به ازای $0 \le i \le 15$.
۳) جابجایی s_i و s_{i+8} به ازای $0 \le i \le 7$ (این عمل $SWAP_1$ نامیده می‌شود).
۴) XOR کردن s_{i+16} با s_i به ازای $0 \le i \le 15$.
۵) جابجایی s_i و s_{i+2} به ازای $i \in \{16,17,20,21,24,25,28,29\}$ (این عمل $SWAP_2$ نامیده می‌شود).
۶) اضافه کردن s_i به s_{i+16} از طریق جمع پیمانه‌ای به ازای $0 \le i \le 15$.
۷) چرخش s_i به میزان ۱۱ بیت به سمت چپ به ازای $0 \le i \le 15$.
۸) جابجایی s_i و s_{i+4} به ازای $i \in \{0,1,2,3,8,9,10,11\}$ (این عمل $SWAP_3$ نامیده می‌شود).
۹) XOR کردن s_{i+16} با s_i به ازای $0 \le i \le 15$.
۱۰) جابجایی s_i و s_{i+1} به ازای $i \in \{16,18,20,22,24,26,28,30\}$ (این جابجایی $SWAP_4$ نامیده می‌شود).

در Cubehash-r/b، $b \in \{1,2,3,\dots,128\}$ می‌باشد و اگر در تابع درهم‌ساز Cubehash-r/b، $b = 1$ در نظر گرفته شود، می‌توان اولین نسخه Cubehash، که برای شرکت در مسابقه SHA-3 ارائه‌شده بود (Cubehash-r/1) را از یک تابع تصادفی تمایز داد. همچنین اگر در Cubehash-r/b، $b = 32$ در نظر گرفته شود، می‌توان Cubehash-r/32 را به‌عنوان نسخه پیچیده‌تر Cubehash-r/1 که پس از ارائه نتایج تحلیل‌های صورت گرفته بر روی Cubehash-r/1 به‌عنوان یک نسخه جدید برای چکیده‌های به طول $h = 224, 256, 384, 512$ معرفی شد را از یک تابع تصادفی تمایز داد.



شکل (۳): یک دور از تابع درهم‌ساز Cubehash

۳-۵- تحلیل چرخشی تابع چکیده‌ساز Cubehash توسط طباطبائی و همکاران

طباطبائی و همکاران توضیح دادند که با توجه به شکل (۳) دو جمع پیمانه‌ای که به‌صورت مارکف می‌باشند در ساختار Cubehash وجود دارد. بر اساس رابطه (۳) و همچنین با در نظر گرفتن مقدار چرخش $r = 1$ و اندازه کلمه ۶۴ بیت برای تابع Cubehash-512، احتمال حفظ ویژگی چرخشی $2^{-3.6}$ می‌باشد و چون‌که در نسخه جدید Cubehash تعداد دور برابر ۱۶ است پس احتمال حفظ ویژگی چرخشی برای تمام ۱۶ دور برابر $2^{-3.6\times16} = 2^{-57.6}$ خواهد بود.

۳-۶- مشاهدات روی تحلیل چرخشی Cubehash توسط طباطبائی و همکاران

مشاهدات روی تحلیل چرخشی Cubehash توسط طباطبائی و همکاران به‌صورت زیر قابل بیان است:

۱- در Cubehash کار بر روی کلمات ۳۲ بیتی صورت می‌گیرد و نه کلمات ۶۴ بیتی که در تحلیل فوق محاسبات بر روی کلمات ۶۴ بیتی صورت گرفته است.

۲- با توجه به اینکه کار بر روی کلمات ۳۲ بیتی صورت می‌گیرد، نمی‌توان تمام دو دنباله ۵۱۲ بیتی را با یک جمع پیمانه‌ای به هم اضافه کرد. لذا ادعای وجود تنها یک زنجیره دوتایی از عملگرهای جمع پیمانه‌ای در یک دور از Cubehash ادعای نادرستی است.

۳- در این تحلیل اثر توابع SWAP در نظر گرفته نشده است.

۴- بهبود تحلیل چرخشی توابع چکیده‌ساز Cubehash و Shabal

در این بخش با توجه به مشاهداتی که روی تحلیل چرخشی Shabal و Cubehash در بخش ۳ گزارش شد، تحلیل چرخشی این توابع مورد بازنگری قرار گرفته و دقیق‌تر بیان می‌شود. برای این منظور ابتدا نشان داده می‌شود که تابع چکیده‌ساز Shabal در برابر تحلیل چرخشی مقاومت لازم را دارد. سپس مقاومت تابع چکیده‌ساز Cubehash در برابر تحلیل چرخشی بررسی می‌شود.

۴-۱- بررسی تحلیل چرخشی روی تابع چکیده‌ساز Shabal

یک روش مقاوم‌سازی رمزهای متقارن ARX در برابر تحلیل چرخشی، استفاده از ثابت‌های دوری در ساختارهای این توابع است [۹]. تابع چکیده‌ساز Shabal نیز از جمله توابعی است که در ساختار خود از ثابت‌های دوری استفاده می‌کند. در تابع چکیده‌ساز Shabal تنها می‌توان بلوک پیام را انتخاب کرد و بافرهای A، B و C مقادیر ثابت و غیر چرخشی دارند. بنابراین با توجه به مقادیر بافرهای A، B و C و محدودیت تحلیل چرخشی، نمی‌توان با استفاده از تحلیل چرخشی تابع چکیده‌ساز Shabal را مورد تحلیل و ارزیابی قرار داد.

حال اگر تابع چکیده‌ساز Shabal با حذف بافرهای A، B و C ساده شود و نوع ساده‌شده این تابع در برابر تحلیل چرخشی مورد ارزیابی قرار گیرد؛ می‌توان گفت عملگرهای چرخش بیتی، AND و XOR ویژگی چرخشی را با احتمال ۱ حفظ می‌کنند. میزان احتمال حفظ ویژگی چرخشی توسط عملگر جمع پیمانه‌ای نیز در جدول (۱) آورده شده است. عملگرهای U و V نیز عملگرهای غیرخطی هستند که احتمال حفظ ویژگی چرخشی آن‌ها با توجه به محاسبات صورت گرفته در [۱۵] به‌صورت زیر است:

$$\Pr[u(x \lll 1) = u(x) \lll 1] = 2^{-1.585}$$

$$\Pr[v(x \lll 1) = v(x) \lll 1] = 2^{-1.737}$$

بنابراین، احتمال حفظ ویژگی چرخشی به ازای چرخش به میزان یک بیت برای عملگرهای جمع پیمانه‌ای، U و V به ترتیب برابر $2^{-1.415}$، $2^{-1.585}$ و $2^{-1.737}$ است [۱۵]. درنتیجه با توجه به عملگرهای غیرخطی موجود در جایگشت Shabal می‌توان گفت خروجی $P(M \lll 1, A \lll 1, B \lll 1, C \lll 1)$ به‌صورت احتمالی با $P(M, A, B, C)$ برابر است [۱۶]. جایگشت P شامل ۳۶ عملگر جمع پیمانه‌ای است و عملگرهای U و V نیز هرکدام ۴۸ بار به‌کار برده می‌شوند [۱۶]. بنابراین احتمال حفظ ویژگی چرخشی توسط این جایگشت برابر $2^{-(48\times1.585+48\times1.737+36\times1.415)} = 2^{-210} > 2^{-896}$ خواهد بود.

بین هر تفریق و جمع پیمانه‌ای ۱۶ زنجیره وجود دارد و هر زنجیره ۲ عملگر جمع و تفریق پیمانه‌ای را شامل می‌شود. بنابراین احتمال حفظ ویژگی چرخشی این زنجیره‌ها برای یک ساختار ۵ دوری از Shabal، $2^{-16\times3.585\times4} = 2^{-229.44}$ می‌باشد. از طرف دیگر احتمال مجموع عملگرهای تفریق و جمع پیمانه‌ای ابتدایی ساختار نیز $2^{-2.83} = 2^{-1.415\times2}$ است. بخش مهم در تحلیل ساختار Shabal جایگشت کلید است که احتمال حفظ ویژگی چرخشی توسط این جایگشت 2^{-210} است. بنابراین برای یک ساختار ۵ دوری از Shabal، یک تمایزگر با احتمال موفقیت زیر به‌دست می‌آید:

$$2^{-2.83} \times 2^{-229.44} \times 2^{-210\times5} = 2^{-1282.27} > 2^{-1408}$$

۴-۲- بررسی تحلیل چرخشی روی تابع چکیده‌ساز Cubehash

همان‌طور که در توصیف تابع دور Cubehash نشان داده شد، گام‌های سوم، پنجم، هشتم و دهم از گام‌های ده‌گانه تابع دور Cubehash مربوط به استفاده از توابع SWAP هستند. به همین منظور ابتدا احتمال حفظ ویژگی چرخشی به ازای چرخش به میزان یک بیت برای توابع SWAP در نظر گرفته می‌شود [۱۸].

$SWAP_1$:

فرض کنید $SWAP_1$ تابعی است که در گام سوم تابع دور Cubehash مورد استفاده قرار گرفته شده است. یک X تصادفی انتخاب می‌کنیم و آن را به میزان یک بیت به سمت چپ چرخش می‌دهیم و یک جفت چرخشی $(X, X \lll 1)$ را تولید می‌کنیم. در ادامه احتمال حفظ ویژگی چرخشی این جفت توسط $SWAP_1$ محاسبه می‌شود.

فرض کنید $S = (S_0, S_1, \dots, S_{31})$ حالت ورودی تابع دور Cubehash باشد. با توجه به تعریف $SWAP_1$ در گام سوم از تابع دور، داریم:

$SWAP_1$: جابجایی s_i و s_{i+8} به ازای $0 \le i \le 7$

$$X = s_0 \| s_1 \| s_2 \| s_3 \| s_4 \| s_5 \| s_6 \| s_7 \| s_8 \| s_9 \| s_{10} \| s_{11} \| s_{12} \| s_{13} \| s_{14} \| s_{15}$$

در حقیقت تابع $SWAP_1$ بر روی نیمه سمت چپ عمل می‌کند. این نیمه را به‌صورت زیر در نظر بگیرید:

بنابراین، با توجه به تعریف $SWAP_1$ داریم:

$$SWAP_1(X) = s_8\|s_9\|s_{10}\|s_{11}\|s_{12}\|s_{13}\|s_{14}\|s_{15}\|s_0\|s_1\|s_2\|s_3\|s_4\|s_5\|s_6\|s_7$$

بدون از دست دادن کلیت کار و به‌منظور سادگی، X را به‌صورت X_1 و X_2 در نظر می‌گیریم.

$$X_1 = s_0\|s_1\|s_2\|s_3\|s_4\|s_5\|s_6\|s_7$$
$$X_2 = s_8\|s_9\|s_{10}\|s_{11}\|s_{12}\|s_{13}\|s_{14}\|s_{15}$$

که در آن، X_1 و X_2 طولی برابر ۵۱۲ بیت دارند. فرض کنید نمایش بیتی آن‌ها به‌صورت زیر باشد:

$$X_1 = X_1^0X_1^1X_1^2 \dots X_1^{254}X_1^{255}$$
$$X_2 = X_2^0X_2^1X_2^2 \dots X_2^{254}X_2^{255}$$

با بازنویسی ورودی تابع $SWAP_1$ به‌صورت $X = X_1\|X_2$ داریم:

$$SWAP_1(X) = X_2\|X_1$$

در ادامه X را به مقدار یک بیت به سمت چپ چرخش می‌دهیم:

$$X \lll 1 = X_1^1X_1^2 \dots X_1^{254}X_1^{255}X_2^0\|X_2^1X_2^2 \dots X_2^{254}X_2^{255}X_1^0$$

حال $SWAP_1(X \lll 1)$ را محاسبه می‌کنیم:

$$SWAP_1(X \lll 1) = X_2^1X_2^2 \dots X_2^{254}X_2^{255}X_1^0\|X_1^1X_1^2 \dots X_1^{254}X_1^{255}X_2^0 \quad (۳)$$

و همچنین داریم:

$$SWAP_1(X) \lll 1 = X_2^1X_2^2 \dots X_2^{254}X_2^{255}X_1^0\|X_1^1X_1^2 \dots X_1^{254}X_1^{255}X_2^0 \quad (۴)$$

با توجه به (۳) و (۴) و اینکه

$$SWAP_1(X) \lll 1 = SWAP_1(X \lll 1)$$

می‌باشد، درنتیجه داریم:

$$Pr[SWAP_1(X) \lll 1 = SWAP_1(X \lll 1)] = 1 \quad (۵)$$

$SWAP_2$:

فرض کنید $SWAP_2$ تابعی است که در گام پنجم تابع دور Cubehash مورد استفاده قرار گرفته شده است. یک X تصادفی انتخاب می‌کنیم و آن را به میزان یک بیت به سمت چپ چرخش می‌دهیم و یک جفت چرخشی $(X.X \lll 1)$ را تولید می‌کنیم. در ادامه احتمال حفظ ویژگی چرخشی این جفت توسط $SWAP_2$ محاسبه می‌شود.

فرض کنید $S = (S_0.S_1.\dots.S_{31})$ حالت ورودی تابع دور Cubehash باشد. با توجه به تعریف $SWAP_2$ در گام پنجم از تابع دور، داریم:

$SWAP_2$: جابجایی s_i و s_{i+2} به ازای

$i \in \{16.17.20.21.24.25.28.29\}$

در حقیقت تابع $SWAP_2$ بر روی نیمه سمت راست عمل می‌کند. این نیمه را به‌صورت زیر در نظر بگیرید:

$$X = s_{16}\|s_{17}\|s_{18}\|s_{19}\|s_{20}\|s_{21}\|s_{22}\|s_{23}\|$$
$$s_{24}\|s_{25}\|s_{26}\|s_{27}\|s_{28}\|s_{29}\|s_{30}\|s_{31}$$

بنابراین با توجه به تعریف $SWAP_2$ داریم:

$$SWAP_2(X) = s_{18}\|s_{19}\|s_{16}\|s_{17}\|s_{22}\|s_{23}\|s_{20}\|s_{21}\|$$
$$s_{26}\|s_{27}\|s_{24}\|s_{25}\|s_{30}\|s_{31}\|s_{28}\|s_{29}$$

بدون از دست دادن کلیت کار و به‌منظور سادگی، X را به‌صورت زیر در نظر می‌گیریم.

$X_1 = s_{16}\|s_{17}$ $\quad$ $X_5 = s_{24}\|s_{25}$

$X_2 = s_{18}\|s_{19}$ $\quad$ $X_6 = s_{26}\|s_{27}$

$X_3 = s_{20}\|s_{21}$ $\quad$ $X_7 = s_{28}\|s_{29}$

$X_4 = s_{22}\|s_{23}$ $\quad$ $X_8 = s_{30}\|s_{31}$

که X_i $(1 \le i \le 8)$ طولی برابر ۶۴ بیت دارد. فرض کنید نمایش بیتی آن به‌صورت زیر باشد:

$$X_i = X_i^0X_i^1X_i^2 \dots X_i^{62}X_i^{63}$$

با بازنویسی ورودی تابع $SWAP_2$ به‌صورت:

$$X = X_1\|X_2\|X_3\|X_4\|X_5\|X_6\|X_7\|X_8$$

داریم:

$$SWAP_2(X) = X_2\|X_1\|X_4\|X_3\|X_6\|X_5\|X_8\|X_7$$

در ادامه X را به مقدار یک بیت به سمت چپ چرخش می‌دهیم:

$$X \lll 1 = X_1^1X_1^2 \dots X_1^{63}X_2^0\|X_2^1X_2^2 \dots X_2^{63}X_3^0\|X_3^1X_3^2 \dots X_3^{63}X_4^0$$
$$\|X_4^1X_4^2 \dots X_4^{63}X_5^0\|X_5^1X_5^2 \dots X_5^{63}X_6^0 \ \|X_6^1X_6^2 \dots X_6^{63}X_7^0$$
$$\|X_7^1X_7^2 \dots X_7^{63}X_8^0\|X_8^1X_8^2 \dots X_8^{63}X_1^0$$

حال $SWAP_2(X \lll 1)$ را محاسبه می‌کنیم:

$$SWAP_2(X \lll 1) = X_2^1X_2^2 \dots X_2^{63}X_3^0\|X_1^1X_1^2 \dots X_1^{63}X_2^0\|X_4^1X_4^2 \dots X_4^{63}X_5^0$$
$$\|X_3^1X_3^2 \dots X_3^{63}X_4^0\|X_6^1X_6^2 \dots X_6^{63}X_7^0\|X_5^1X_5^2 \dots X_5^{63}X_6^0$$
$$\|X_8^1X_8^2 \dots X_8^{63}X_1^0\|X_7^1X_7^2 \dots X_7^{63}X_8^0 \quad (۶)$$

و

$$SWAP_2(X) \lll 1 = X_2^1X_2^2 \dots X_2^{63}X_1^0\|X_1^1X_1^2 \dots X_1^{63}X_4^0\|X_4^1X_4^2 \dots X_4^{63}X_3^0$$
$$\|X_3^1X_3^2 \dots X_3^{63}X_6^0\|X_6^1X_6^2 \dots X_6^{63}X_5^0\|X_5^1X_5^2 \dots X_5^{63}X_8^0$$
$$\|X_8^1X_8^2 \dots X_8^{63}X_7^0\|X_7^1X_7^2 \dots X_7^{63}X_2^0 \quad (۷)$$

با توجه به (۶) و (۷) در می‌یابیم که برای برقراری معادله

$$SWAP_2(X) \lll 1 = SWAP_2(X \lll 1)$$

باید شرایط زیر برای برخی از بیت‌های X برقرار باشد:

$$X_2^0 = X_4^0 = X_6^0 = X_8^0 \quad و \quad X_1^0 = X_3^0 = X_5^0 = X_7^0$$

هریک از این شرایط با احتمال $(\frac{1}{2})^3$ برقرار می‌باشد. بنابراین

$$Pr[SWAP_2(X) \lll 1 = SWAP_2(X \lll 1)] = 2^{-6} \quad (۸)$$

$SWAP_3$:

فرض کنید $SWAP_3$ تابعی است که در گام هشتم تابع دور Cubehash مورد استفاده قرار گرفته شده است. یک X تصادفی انتخاب می‌کنیم و آن را به میزان یک بیت به سمت چپ چرخش می‌دهیم و یک جفت چرخشی $(X.X \lll 1)$ را تولید می‌کنیم. در ادامه احتمال حفظ ویژگی چرخشی این جفت توسط $SWAP_3$ محاسبه می‌شود.

فرض کنید $S = (S_0.S_1.\dots.S_{31})$ حالت ورودی تابع دور Cubehash باشد. با توجه به تعریف $SWAP_3$ در گام هشتم از تابع دور، داریم:

$SWAP_3$: جابجایی s_i و s_{i+4} به ازای

$i \in \{0.1.2.3.8.9.10.11\}$

در حقیقت تابع $SWAP_3$ بر روی نیمه سمت چپ عمل می‌کند. این نیمه را به‌صورت زیر در نظر بگیرید:

$$X = s_0\|s_1\|s_2\|s_3\|s_4\|s_5\|s_6\|s_7\|$$

$s_8\|s_9\|s_{10}\|s_{11}\|s_{12}\|s_{13}\|s_{14}\|s_{15}$بنابراین با توجه به تعریف $SWAP_3$ داریم:

$$SWAP_3(X) = s_4\|s_5\|s_6\|s_7\|s_0\|s_1\|s_2\|s_3\|$$
$$s_{12}\|s_{13}\|s_{14}\|s_{15}\|s_8\|s_9\|s_{10}\|s_{11}$$

بدون از دست دادن کلیت کار و به‌منظور سادگی، X را به‌صورت زیر در نظر می‌گیریم.

$$X_1 = s_0\|s_1\|s_2\|s_3$$
$$X_2 = s_4\|s_5\|s_6\|s_7$$
$$X_3 = s_8\|s_9\|s_{10}\|s_{11}$$
$$X_4 = s_{12}\|s_{13}\|s_{14}\|s_{15}$$

که X_i $(1 \le i \le 4)$ طولی برابر ۱۲۸ بیت دارد. فرض کنید نمایش بیتی آن به‌صورت زیر باشد:

$$X_i = X_i^0 X_i^1 X_i^2 \dots X_i^{126} X_i^{127}$$

با بازنویسی ورودی تابع $SWAP_3$ به‌صورت:

$$X = X_1\|X_2\|X_3\|X_4$$

داریم:

$$SWAP_3(X) = X_2\|X_1\|X_4\|X_3$$

در ادامه X را به مقدار یک بیت به سمت چپ چرخش می‌دهیم:

$$X \lll 1 = X_1^1X_1^2 \dots X_1^{127}X_2^0\|X_2^1X_2^2 \dots X_2^{127}X_3^0\|X_3^1X_3^2 \dots X_3^{127}X_4^0$$
$$\|X_4^1X_4^2 \dots X_4^{127}X_1^0$$

حال $SWAP_3(X \lll 1)$ را محاسبه می‌کنیم:

$$SWAP_3(X \lll 1)$$
$$= X_2^1X_2^2 \dots X_2^{127}X_3^0\|X_1^1X_1^2 \dots X_1^{127}X_2^0\|X_4^1X_4^2 \dots X_4^{127}X_1^0$$
$$\|X_3^1X_3^2 \dots X_3^{127}X_4^0 \qquad (۹)$$

و

$$SWAP_3(X) \lll 1$$
$$= X_2^1X_2^2 \dots X_2^{127}X_1^0\|X_1^1X_1^2 \dots X_1^{127}X_4^0\|X_4^1X_4^2 \dots X_4^{127}X_3^0$$
$$\|X_3^1X_3^2 \dots X_3^{127}X_2^0 \qquad (۱۰)$$

با توجه به (۹) و (۱۰) در می‌یابیم که برای برقراری معادله

$$SWAP_3(X) \lll 1 = SWAP_3(X \lll 1)$$

باید شرایط زیر برای برخی از بیت‌های x برقرار باشد:

$$X_1^0 = X_3^0 \qquad \text{و} \qquad X_2^0 = X_4^0$$

هریک از این شرایط با احتمال $\frac{1}{2}$ برقرار می‌باشد. بنابراین

$$\Pr[SWAP_3(X) \lll 1 = SWAP_3(X \lll 1)] = 2^{-2} \qquad (۱۱)$$

$SWAP_4$:

فرض کنید $SWAP_4$ تابعی است که در گام دهم تابع دور Cubehash مورد استفاده قرار گرفته شده است. یک X تصادفی انتخاب می‌کنیم و آن را به میزان یک بیت به سمت چپ چرخش می‌دهیم و یک جفت چرخشی $(X.X \lll 1)$ را تولید می‌کنیم. در ادامه احتمال حفظ ویژگی چرخشی این جفت توسط $SWAP_4$ محاسبه می‌شود.

فرض کنید $S = (S_0.S_1.\dots.S_{31})$ حالت ورودی تابع دور Cubehash باشد. با توجه به تعریف $SWAP_4$ در گام دهم از تابع دور، داریم:

$SWAP_4$: جابجایی s_i و s_{i+1} به ازای

$i \in \{16.18.20.22.24.26.28.30\}$

در حقیقت تابع $SWAP_4$ بر روی نیمه سمت راست عمل می‌کند. این نیمه را به‌صورت زیر در نظر بگیرید:

$$X = s_{16}\|s_{17}\|s_{18}\|s_{19}\|s_{20}\|s_{21}\|s_{22}\|s_{23}\|$$
$$s_{24}\|s_{25}\|s_{26}\|s_{27}\|s_{28}\|s_{29}\|s_{30}\|s_{31}$$

بنابراین با توجه به تعریف $SWAP_4$ داریم:

$$SWAP_4(X) = s_{17}\|s_{16}\|s_{19}\|s_{18}\|s_{21}\|s_{20}\|s_{23}\|s_{22}\|$$
$$s_{25}\|s_{24}\|s_{27}\|s_{26}\|s_{29}\|s_{28}\|s_{31}\|s_{30}$$

بدون از دست دادن کلیت کار و به‌منظور سادگی، X را به‌صورت زیر در نظر می‌گیریم.

$$X_1 = s_{16} \qquad X_9 = s_{24}$$
$$X_2 = s_{17} \qquad X_{10} = s_{25}$$
$$X_3 = s_{18} \qquad X_{11} = s_{26}$$
$$X_4 = s_{19} \qquad X_{12} = s_{27}$$
$$X_5 = s_{20} \qquad X_{13} = s_{28}$$
$$X_6 = s_{21} \qquad X_{14} = s_{29}$$
$$X_7 = s_{22} \qquad X_{15} = s_{30}$$
$$X_8 = s_{23} \qquad X_{16} = s_{31}$$

که X_i $(1 \le i \le 16)$ طولی برابر ۳۲ بیت دارد. فرض کنید نمایش بیتی آن به‌صورت زیر باشد:

$$X_i = X_i^0 X_i^1 X_i^2 \dots X_i^{30} X_i^{31}$$

با بازنویسی ورودی تابع $SWAP_4$ به‌صورت:

$$X = X_1 \| X_2 \| X_3 \| X_4 \| X_5 \| X_6 \| X_7 \| X_8 \|$$
$$X_9 \| X_{10} \| X_{11} \| X_{12} \| X_{13} \| X_{14} \| X_{15} \| X_{16}$$

داریم:

$$SWAP_4(X) = X_2 \| X_1 \| X_4 \| X_3 \| X_6 \| X_5 \| X_8 \| X_7 \|$$
$$X_{10} \| X_9 \| X_{12} \| X_{11} \| X_{14} \| X_{13} \| X_{16} \| X_{15}$$

در ادامه X را به مقدار یک بیت به سمت چپ چرخش می‌دهیم:

$$X \lll 1 = X_1^1 X_1^2 \dots X_1^{31} X_2^0 \| X_2^1 X_2^2 \dots X_2^{31} X_3^0 \| X_3^1 X_3^2 \dots X_3^{31} X_4^0$$
$$\| X_4^1 X_4^2 \dots X_4^{31} X_5^0 \| X_5^1 X_5^2 \dots X_5^{31} X_6^0 \| X_6^1 X_6^2 \dots X_6^{31} X_7^0$$
$$\| X_7^1 X_7^2 \dots X_7^{31} X_8^0 \| X_8^1 X_8^2 \dots X_8^{31} X_9^0 \| X_9^1 X_9^2 \dots X_9^{31} X_{10}^0$$
$$\| X_{10}^1 X_{10}^2 \dots X_{10}^{31} X_{11}^0 \| X_{11}^1 X_{11}^2 \dots X_{11}^{31} X_{12}^0 \| X_{12}^1 X_{12}^2 \dots X_{12}^{31} X_{13}^0$$
$$\| X_{13}^1 X_{13}^2 \dots X_{13}^{31} X_{14}^0 \| X_{14}^1 X_{14}^2 \dots X_{14}^{31} X_{15}^0 \| X_{15}^1 X_{15}^2 \dots X_{15}^{31} X_{16}^0$$
$$\| X_{16}^1 X_{16}^2 \dots X_{16}^{31} X_1^0$$

حال $SWAP_4(X \lll 1)$ را محاسبه می‌کنیم:

$$SWAP_4(X \lll 1) = X_2^1 X_2^2 \dots X_2^{31} X_3^0 \| X_1^1 X_1^2 \dots X_1^{31} X_2^0 \| X_4^1 X_4^2 \dots X_4^{31} X_5^0$$
$$\| X_3^1 X_3^2 \dots X_3^{31} X_4^0 \| X_6^1 X_6^2 \dots X_6^{31} X_7^0 \| X_5^1 X_5^2 \dots X_5^{31} X_6^0$$
$$\| X_8^1 X_8^2 \dots X_8^{31} X_9^0 \| X_7^1 X_7^2 \dots X_7^{31} X_8^0 \| X_{10}^1 X_{10}^2 \dots X_{10}^{31} X_{11}^0$$
$$\| X_9^1 X_9^2 \dots X_9^{31} X_{10}^0 \| X_{12}^1 X_{12}^2 \dots X_{12}^{31} X_{13}^0 \| X_{11}^1 X_{11}^2 \dots X_{11}^{31} X_{12}^0$$
$$\| X_{14}^1 X_{14}^2 \dots X_{14}^{31} X_{15}^0 \| X_{13}^1 X_{13}^2 \dots X_{13}^{31} X_{14}^0 \| X_{16}^1 X_{16}^2 \dots X_{16}^{31} X_1^0 \|$$
$$X_{15}^1 X_{15}^2 \dots X_{15}^{31} X_{16}^0 \qquad (۱۲)$$

و

$$SWAP_4(X) \lll 1 = X_2^1 X_2^2 \dots X_2^{31} X_1^0 \| X_1^1 X_1^2 \dots X_1^{31} X_4^0 \| X_4^1 X_4^2 \dots X_4^{31} X_3^0$$
$$\| X_3^1 X_3^2 \dots X_3^{31} X_6^0 \| X_6^1 X_6^2 \dots X_6^{31} X_5^0 \| X_5^1 X_5^2 \dots X_5^{31} X_8^0$$
$$\| X_8^1 X_8^2 \dots X_8^{31} X_7^0 \| X_7^1 X_7^2 \dots X_7^{31} X_{10}^0 \| X_{10}^1 X_{10}^2 \dots X_{10}^{31} X_9^0$$
$$\| X_9^1 X_9^2 \dots X_9^{31} X_{12}^0 \| X_{12}^1 X_{12}^2 \dots X_{12}^{31} X_{11}^0 \| X_{11}^1 X_{11}^2 \dots X_{11}^{31} X_{14}^0$$
$$\| X_{14}^1 X_{14}^2 \dots X_{14}^{31} X_{13}^0 \| X_{13}^1 X_{13}^2 \dots X_{13}^{31} X_{16}^0 \| X_{16}^1 X_{16}^2 \dots X_{16}^{31} X_{15}^0$$
$$\| X_{15}^1 X_{15}^2 \dots X_{15}^{31} X_2^0 \qquad (۱۳)$$

با توجه به (پ-۱۰) و (پ-۱۱) در می‌یابیم که برای برقراری معادله

$$SWAP_4(X) \lll 1 = SWAP_4(X \lll 1)$$

باید شرایط زیر برای برخی از بیت‌های x برقرار باشد:

$$X_2^0 = X_4^0 = X_6^0 = X_8^0 = X_{10}^0 = X_{12}^0 = X_{14}^0 = X_{16}^0$$
$$X_1^0 = X_3^0 = X_5^0 = X_7^0 = X_9^0 = X_{11}^0 = X_{13}^0 = X_{15}^0$$

هریک از این شرایط با احتمال $(\frac{1}{2})^7$ برقرار می‌باشد. بنابراین

$$Pr[SWAP_2(X) \lll 1 = SWAP_2(X \lll 1)] = 2^{-14} \qquad (۱۴)$$

جدول (۲) احتمال حفظ ویژگی چرخشی توابع $SWAP_1$، $SWAP_2$، $SWAP_3$ و $SWAP_4$ را نشان می‌دهد.

جدول (۲): احتمال حفظ ویژگی چرخشی توابع SWAP [۱۸].

تابع	$SWAP_1$	$SWAP_2$	$SWAP_3$	$SWAP_4$
احتمال چرخشی	1	2^{-6}	2^{-2}	2^{-14}

همان‌طور که در بخش دوم اشاره شد، عملگرهای چرخش بیتی و XOR، ویژگی چرخشی را با احتمال ۱ حفظ می‌کنند. بنابراین احتمال چرخشی به عملگرهای جمع پیمانه‌ای و توابع SWAP بستگی دارد.

در تحلیل چرخشی ابتدا تعداد عملگرهای جمع پیمانه‌ای موجود در ساختار را یافته و بررسی می‌شود که آیا این عملگرها و یا تعدادی از آن‌ها یک زنجیره را تشکیل می‌دهند و یا خیر. در صورت وجود زنجیره، احتمال چرخشی با در نظر گرفتن زنجیره‌ها و تعداد عملگرهای موجود در هر زنجیره، محاسبه می‌شود و در غیر این صورت احتمال چرخشی صرفاً بر اساس تعداد عملگرهای موجود در ساختار محاسبه می‌شود.

با توجه به شکل ۳، عملگرهای جمع پیمانه‌ای موجود در ساختار تابع Cubehash، تشکیل زنجیره می‌دهند. به‌عبارت‌دیگر ورودی‌های هر عملگر جمع پیمانه‌ای، ۱۶ کلمه ۳۲ بیتی می‌باشند که این کلمات دو به دو با یکدیگر جمع می‌شوند. بنابراین، در هر دور ۱۶ زنجیره داریم که هر زنجیره متشکل از ۲ عملگر جمع پیمانه‌ای است.

همان‌طور که گفته شد؛ در هر دور از ساختار Cubehash از چهار تابع SWAP استفاده می‌شود. در ادامه احتمال حفظ ویژگی چرخشی توسط این توابع در یک دور محاسبه می‌شود.

$$Pr(swaps)_{(1Round)} = Pr_{swap_1} \times Pr_{swap_2} \times Pr_{swap_3} \times Pr_{swap_4}$$

$$Pr(swaps)_{(1Round)} = 1 \times 2^{-6} \times 2^{-2} \times 2^{-14} = 2^{-22}$$

با توجه به شکل (۳)، برای ۷ دور از تابع Cubehash، ۱۶ زنجیره ۱۴تایی متشکل از عملگر جمع پیمانه‌ای وجود دارد. با توجه به رابطه (۲)، احتمال هر زنجیره ۱۴تایی برابر $2^{-51.25}$ است. بنابراین احتمال حفظ ویژگی چرخشی برای ۷ دور از تابع Cubehash به‌صورت زیر محاسبه می‌شود.

$$Pr(Cubehash - r/b)_{(7Round)} = (2^{-51.25})^{16} \times (2^{-22})^7 = 2^{-974}$$

همان‌طور که مشاهده می‌شود، احتمال حفظ ویژگی چرخشی توسط ۷ دور از تابع درهم‌ساز Cubehash، 2^{50} مرتبه از 2^{-1024} بزرگ‌تر است. بنابراین، در این تحلیل، ۷ دور از Cubehash با پیچیدگی 2^{974}، از یک تابع تصادفی تمایز داده شد.

در جدول (۳) نتایج حاصل از تحلیل چرخشی در این مقاله و تحلیل‌های چرخشی قبلی صورت گرفته بر روی این دو تابع خلاصه شده است.

جدول (۳): نتایج تحلیل چرخشی توابع چکیده‌ساز Shabal و Cubehash در این مقاله و [۱۳] و [۱۸].

	[۱۸]		[۱۳]		این مقاله	
	تعداد دور	احتمال	تعداد دور	احتمال	تعداد دور	احتمال
Shabal			۱۹	$2^{-3393.58}$	۵	$2^{-1282.27}$
Cube-hash8/b	۸	$2^{-538.5}$				
Cube-hash15/b	۱۶	$2^{-1009.}$	۱۶	$2^{-57.6}$	۷	2^{-974}

۵- نتیجه‌گیری

تحلیل چرخشی ازجمله روش‌های مؤثر جهت ارزیابی ساختارهای ARX است. توابع چکیده‌ساز Shabal و Cubehash به‌عنوان نامزدهای دور دوم مسابقه SHA-3، از جمله ساختارهای ARX هستند. این دو تابع قبلاً در [۱۷] توسط طباطبائی و همکاران مورد تحلیل و ارزیابی قرار گرفته بود. در این مقاله یک سری مشاهدات روی تحلیل‌های ذکرشده گزارش شد. با توجه به این مشاهدات، کاربرد تحلیل چرخشی برای ارزیابی توابع چکیده‌ساز Shabal و Cubehash مورد بازنگری قرار گرفت و نتایج دقیق‌تری حاصل شد. توجه شود که نتایج این مقاله از جهت افزایش دقت تحلیل چرخشی توابع ذکرشده اهمیت دارند. اگر چه این افزایش دقت منجر به کاهش تعداد دورهای آسیب‌پذیر توابع چکیده‌ساز Shabal و Cubehash شده است.

۶- مراجع

[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, LNCS, vol. 9665, pp. 459-483, 2016.

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

[5] X. Wang, H. Yu, and Y. L. Yin, "Efficient Collision Search Attacks on SHA-0," Advances in Cryptology, Crypto 2005, LNCS 3621, pp. 1-16, Springer, 2005.

[6] X. Wang, Y. L. Yin, and H. Yu, "Finding Collisions in the Full SHA-1," Advances in Cryptology, Crypto 2005, LNCS 3621, pp. 17- 36, Springer, 2005.

[7] NIST, "Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA–3) Family," Federal Register, vol. 72, pp. 62212–62220, Nov. 2007.

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

[9] D. Khovratovich and I. Nikoli´c, "Rotational cryptanalysis of ARX," In Proceedings of the 17th international conference on Fast Software Encryption, Springer, pp. 333–346, 2010.

[10] D. Khovratovich, I. Nikoli´c, J. Pieprzyk, P. Sokolowski, and R. Steinfeld, "Rotational cryptanalysis of ARX revisited," In Fast Software Encryption, pp. 519–536, Springer, 2015.

[11] T. Ashur and Y. Liu, "Rotational cryptanalysis in the presence of constants," IACR Transactions on Symmetric Cryptology, pp. 57–70, 2016.

[12] A. Ranea, Y. Liu, and T. Ashur, "An Easy-to-Use Tool for Rotational-XOR Cryptanalysis of ARX Block Ciphers," Proceedings of the Romanian Academy, Series A, pp. 307–316, 2017.

[13] S. A. Tabatabaei Feiz Abad, A. Gaini, and B. Keshavarzi, "Rotational Cryptanalysis on Shabal and CubeHash," In Journal of Electronical & Cyber Defence, Springer, pp. 59–64, 2018. (In Persian)

[14] M. Daum, "Cryptanalysis of Hash Functions of the MD4-Family," PhD thesis, RuhrUniversit¨at Bochum May, 2005.

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

[16] A. Nieke, "Cryptanalysis of Hash Functions," Macquarie University & Eindhoven University of Technology, 2011.

[17] Daniel J. Bernstein, "CubeHash specification (2.b.1)," Submission to NIST, 2008.

[18] J. Alizadeh and A. Mirghadri, "A new distinguisher for CubeHash-8/b and CubeHash-15/b compression functions," IACR eprint, 2011.

Journal of Electronical & Cyber Defence
Vol. 9, No. 1, 2021, Serial No. 33

Improvement of Rotational Cryptanalysis of Shabal and Cubehash Hash Functions

M. Aboei Mehrizi, J. Alizadeh*

*Imam Hossein Comprehensive University

(Received: 12/04/2020, Accepted: 05/08/2020)

ABSTRACT

A cryptographic hash function maps an arbitrary length input to a fixed length output. These functions are used in many cryptographic applications such as digital signatures. They must be secure against collision, preimage and 2-preimage attacks. Rotational cryptanalysis is an approach to the analysis of ARX ciphers. The Hash functions Shabal and Cubehash, which are two candidates of the second round of the SHA-3 competition, have an ARX structure. They have been analyzed with respect to rotational cryptanalysis by Tabatabaei et al. In this paper we consider their analysis and present some observations. Our observations show that the results of Tabatabaei et al.'s cryptanalysis are not accurate. Then we present some new results about rotational cryptanalysis of Shabal and Cubehash. Thereafter we present some new results and show that rotational cryptanalysis is effective on a smaller number of rounds on Shabal and Cubehash Hash functions.

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

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