تحلیل رمز چرخشی برروی *EnRupt , Blender-n*

سیدعلی طباطبائی فیض آباد*[۱]، احمد گائینی[۲]، بهبد کشاورزی[۳]

۱- کارشناسی ارشد ریاضی کاربردی دانشگاه جامع امام حسین (ع)
۲- عضو هیئت علمی گروه ریاضی و آمار دانشگاه جامع امام حسین (ع)
۳- کارشناسی ارشد ریاضی رمز دانشگاه شاهد

چکیده

برقراری امنیت اطلاعات و ارتباطات اهمیت ویژه‌ای در استفاده از اطلاعات و ارتباطات در هر حوزه‌ای مانند حوزه های نظامی سیاسی و غیره دارد و یکی از مولفه‌های امنیت پروتکل‌های رمزنگاری توابع چکیده‌ساز به‌کار رفته در آنها است. توابع چکیده‌ساز توابعی هستند یک طرفه که رشته صفر و یک ورودی با طول دلخواه را به یک رشته صفر و یک با طول ثابت n تبدیل می‌کند. توابع چکیده‌ساز توابعی یک طرفه هستند که دارای سه شرط امنیتی مقاوم بودن در برابر برخورد[۱]، پیش تصویر[۲] و پیش تصویر دوم[۳] می‌باشند. از کاربردهای توابع چکیده‌ساز می‌توان به امضای رقمی[۴]، کد های احراز اصالت[۵] و غیره اشاره کرد. تحلیل رمز چرخشی یک حمله نسبتا جدیدی است که جزء حملات عمومی بر توابع چکیده‌ساز محسوب می‌شود و برروی الگوریتم هایی که در ساختارشان از سه عملگر چرخش[۶]، جمع پیمانه‌ای[۷] و یای انحصاری[۸] استفاده می‌کنند، یعنی ساختاری *ARX* دارند، موثر است. در این مقاله برای اولین بار برروی دو الگوریتم رمز *ARX* مسابقه *SHA-3* یعنی الگوریتم‌های *Blender-n* و *EnRupt* با در نظر گرفتن فرض مارکوف[۹]، تحلیل رمز چرخشی انجام دادیم و به پیچیدگی $2^{-125.33}$ برای کل دور های *Blender-n-512* و پیچیدگی $2^{59.33}$ برای *EnRupt-512* رسیدیم.

کلمات کلیدی: توابع چکیده‌ساز، تحلیل رمز چرخشی، جمع پیمانه‌ای، فرض زنجیره مارکوف،*Blender-n,EnRupt*

* *Corresponding author: Seyed Ali TabaTabaei Feiz Abad*
Email: Syedalitabatabaei@gmail.com

[۱] *Collision*
[۲] *Preimage*
[۳] *Second Preimage*
[۴] *Digital Signature*
[۵] *Message Authentication Code*
[۶] *Rotation*
[۷] *Mudolar Addition*
[۸] *Xor*
[۹] *Markov*

۱. مقدمه

توابع چکیده‌ساز یکی از مهمترین توابع رمز نگاری می‌باشند که رشته صفر و یک ورودی با طول دلخواه را به یک رشته صفر و یک با طول ثابت n تبدیل می‌کند. توابع چکیده‌ساز توابعی یک طرفه هستند که دارای سه شرط امنیتی مقاوم بودن در برابر برخورد، پیش تصویر و پیش تصویر دوم می‌باشند [1]. از کاربردهای توابع چکیده‌ساز می‌توان به امضای رقمی، کد های احراز اصالت و غیره اشاره کرد. که این توابع چکیده‌ساز در دو خانواده *MD(1990)* و *SHA* تقسیم بندی می‌شوند.

تابع چکیده‌ساز *MD4* در سال ۱۹۹۰ توسط رایوست ارایه گردید ولی در سال ۱۹۹۲ یک نسخه کامل‌تر از آن یعنی *MD5* را پشنهاد داد. تابع چکیده‌ساز *MD5* [2] به مدت چهار سال به طور گسترده مورد استفاده قرار گرفت، اما در سال ۱۹۹۶ یک ضعف امنیتی در تابع فشرده‌ساز این تابع چکیده‌ساز پیدا شد ولی در عین حال باز هم یکی از توابع چکیده‌ساز پر کاربرد باقی ماند. در سال ۲۰۰۴ یک گروه از محققین چینی به سرپرستی خانم وانگ و همکارانش حمله موثری بر روی *MD5* اعمال کردند طوری که باعث شکست خانواده *MD*ها شدند [3]. بعد از شکست خانواده *MD*ها در حمله های صورت گرفته بروی این دسته از توابع چکیده‌ساز، الگوریتم چکیده امن[۱] توسط موسسه ملی استاندارد و تکنولوژی آمریکا[۲] گسترش یافت و توسط استاندارد پردازش اطلاعات فدرال[۳] منتشر شد [4]. برای اقدام مقابل در برابر حملات مهم روی توابع چکیده‌ساز استاندارد، مانند *MD5* و *SHA-1*، *NIST* در سال ۲۰۰۷ مسابقه‌ای را برای انتخاب یک تابع چکیده‌ساز امن به نام *SHA-3* آغاز کرد، یک معیار مهم برای انتخاب تابع چکیده‌ساز*SHA-3* ، مقاومت این تابع در برابر حملات شناخته شده روی توابع چکیده‌ساز و نیز حملات جدید بود [5].

تجزیه و تحلیل رمز یا شکستن رمز، به کلیه اقدامات مبتنی بر اصول ریاضی و علمی اطلاق می‌گردد که هدف آن از بین بردن امنیت رمزنگاری و در نهایت بازکردن رمز و دستیابی به اطلاعات اصلی باشد. در تجزیه و تحلیل رمز، سعی می‌شود تا با بررسی جزئیات مربوط به الگوریتم رمز و یا پروتکل رمزنگاری مورد استفاده و به کار گرفتن هرگونه اطلاعات جانبی موجود، ضعف‌های امنیتی احتمالی موجود در سیستم رمزنگاری یافت شود و از این طریق به نحوی کلید رمز به دست آمده و یا محتوای اطلاعات رمز شده استخراج گردد. تجزیه و تحلیل رمز، گاهی به منظور شکستن امنیت یک سیستم رمزنگاری و به عنوان خرابکاری و یک فعالیت ضد امنیتی انجام می‌شود و گاهی هم به منظور ارزیابی یک پروتکل یا الگوریتم رمزنگاری و برای کشف ضعف‌ها و آسیب‌پذیری‌های احتمالی آن صورت می‌پذیرد [6].

تحلیل رمز چرخشی[۴] یک حمله نسبتا جدید است که توسط دیمیتری خووراتویچ[۵] و ایویکا نیکولیچ[۶] در تحلیل سیستم های *ARX* به صورت فرمولی به کار رفته شده است [7]. ایده اصلی تحلیل چرخشی این‌است که برخی تبدیل‌ها روی ورودی‌های چرخش‌یافته، خروجی‌های چرخش‌یافته تولید می‌کنند (در واقع دشمن انتشار روابط چرخشی را در سرتاسر تبدیل‌های الگوریتم بررسی می‌کند). در سال ۲۰۱۵ خووراتویچ و نیکولیچ مقاله قبلی خود را که فقط تعداد

---

[۱] *Secure Hash Algorithm*
[۲] *NIST*
[۳] *FIPS-180*
[۴] *Rotational Cryptanalysis*
[۵] *Dimitry Khovratovich*
[۶] *Ivica Nikolic*

جمع‌های پیمانه 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 [8].

در این مقاله برای اولین بار با توجه به شرایط و الزامات تحلیل رمز چرخشی در مراجع [7] و [8] بر دو کاندیدای *SHA-3* یعنی الگوریتم‌های *Blender-n* و *EnRupt* که ساختاری *ARX* دارند با توجه به فرض زنجیره مارکوف تحلیل رمز چرخشی اعمال می‌شود. در بخش دوم این مقاله تحلیل رمز چرخشی تشریح و الزامات اجرای تحلیل رمز چرخشی مورد بررسی قرار می‌گیرد و در بخش سوم به بررسی مختصری از الگوریتم‌های *Blender-n* و *EnRupt* پرداخته می‌شود و در بخش چهارم تحلیل رمز چرخشی را بر الگوریتم‌هایرمز اعمال و در بخش آخر نتیجه بحث را ارائه می‌شود.

۲. تشریح تحلیل رمز چرخشی

در مرجع [7] روش کلی برای تحلیل سیستم های *ARX* را داریم، ایده کلی فرض جفت کلمه‌هاست که یکی چرخش دیگری به اندازه r-بیت می‌باشد. که عملگرهای چرخشی به وسیله r >>> یا 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 که $(x, \vec{x})$ جفت چرخشی به اندازه r-بیت می‌نامیم. به عبارت دیگر برخی تبدیل‌ها روی ورودی‌های چرخش‌یافته، خروجی‌های چرخش‌یافته تولید می‌کنند (در واقع دشمن انتشار روابط چرخشی را در سرتاسر تبدیل‌های الگوریتم بررسی می‌کند).

اثبات اینکه یک جفت چرخشی با هر تبدیل بیتی حفظ می‌شود آسان است مخصوصا یای انحصاری و چرخش که در رابطه (۱) نشان داده شده است.

$$x \oplus y = \overrightarrow{x} \oplus \overrightarrow{y}, \overrightarrow{x} \quad \forall r \in \mathbb{Z} \quad \Leftrightarrow \quad x \quad r \in \mathbb{Z} \tag{1}$$

جمع پیمانه‌ای را به مد 2^n در نظر می گیریم، احتمال اینکه جفت چرخشی از جمع پیمانه‌ای بیرون آید طبق لم زیر داریم:

لم ۱: احتمال چرخشی با در نظر گرفتن مقدار چرخشی r از رابطه (۲) محاسبه می گردد.

$$p_r(x \ (\ y \in \mathbb{Z}\ r = x \in \mathbb{Z}\ r \ (\ y \in \mathbb{Z}\ r) = \frac{1}{4}(1 + 2^{r-n} + 2^{-r} + 2^{-n}) \tag{2}$$

برای n های بزرگ و r کوچک جدول ۱ را داریم:

جدول ۱- احتمالات چرخشی به ازای مقدار چرخشی متفاوت

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 در نظر بگیریم قضیه ۱ 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 $\mathcal{S}(\vec{I}) = \overrightarrow{\mathcal{S}(I)}$ با احتمال ${P_r}^q$ محاسبه می‌شود.

اثبات: به کمک استقرا بروی اندازه طرح در مرجع [8].

به منظور اعمال تحلیل چرخشی، سعی می‌کنیم تا ورودی‌های طرح ARX تشکیل جفت چرخشی دهند. برای یک تابع تصادفی P که به z_2^t نگاشت می‌شود، احتمال اینکه $P(\vec{I}) = \overrightarrow{P(I)}$ برای I تصادفی 2^{-t} است. بنابراین می‌توانیم یک تابع غیر تصادفی بیابیم اگر تابع بتواند با q جمع پیمانه‌ای اجرا شود و ${P_r}^q > 2^{-t}$. مرجع [8] نشان می‌دهد که احتمالات چرخشی ARX، تنها به تعداد جمع‌های پیمانه‌ای بستگی ندارد بلکه به طریقه اتصال آنها بستگی دارد. احتمال چرخشی نمی‌تواند با ضرب احتمال تک تک جمع‌ها به دست آید. این بدین معنی است که فرض رمز مارکوف استفاده شده برای محاسبه ضمنی احتمال از این طریق امکان پذیر نیست. دنباله‌ای از متغییرهای تصادفی گسسته $v_0, \dots, v_r$ یک دنباله مارکوف است اگر برای $0 < i < r$ رابطه (۳) برقرار باشد:

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

به سادگی با شمارش تعداد جمع محاسبه نمی‌شود. در عوض باید روابط موقعیت‌های جمع ARXپاحتمال چرخشی پیمانه‌ای را بررسی کنیم. یعنی آیا آنها زنجیره‌ای یا جدا شده با جمع‌ها هستند. درحقیقت زنجیره بزرگتر برای جمع‌های پیمانه‌ای برای هر جمع متوالی، احتمال چرخشی کمتری دارد. احتمال چرخشی جمع‌های پیمانه‌ای زنجیره ای در لم ۲ آمده است.

لم۲: فرض کنید $a_1, \dots, a_k$ کلمه های n-بیتی باشند که به صورت تصادفی انتخاب شده باشند و r یک عدد صحیح مثبت که $0 < r < n$ آنگاه احتمال چرخشی از رابطه (۴) بدست می آید:

$$P_r([(a_1 \boxplus a_2) \lll r = a_1 \lll r \boxplus a_2 \lll r] \wedge [(a_1 \boxplus a_2 \boxplus a_3) \lll r = a_1 \lll r \boxplus a_2 \lll r \boxplus a_2 \lll r] \wedge \dots \wedge [(a_1 \boxplus \dots \boxplus a_k) \lll r = a_1 \lll r \boxplus \dots \boxplus a_k \lll r]) = \frac{1}{2^{nk}} \binom{k + 2^r - 1}{2^r - 1} \binom{k + 2^{n-r} - 1}{2^{n-r} - 1} \quad (4)$$

به طور خلاصه، احتمال چرخشی لزوما برابر با حاصلضرب تک تک احتمالات چرخشی نیست و طریقه اتصال جمع‌های پیمانه‌ای در بدست آوردن احتمال موثر است و باعث افزایش دقت آن می‌شود.

۳. معرفی الگوریتم‌های *Blender-n* و *EnRupt*

در این بخش به معرفی مختصری از الگوریتم‌های *Blender-n* و *EnRupt* می‌پردازیم و این الگوریتم‌ها را متناسب با شرایط و قواعد تحلیل رمز چرخشی تشریح می‌کنیم.

۳-۱. الگوریتم *Blender-n*

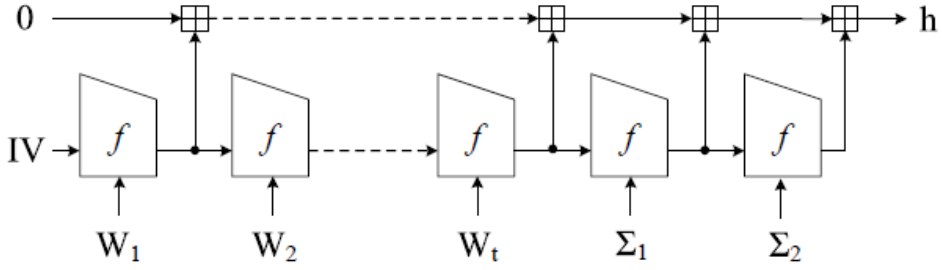
تابع چکیده‌ساز *Blender-n* یک تابع چکیده‌ساز تکراری است. که بلوک های پیام ۳۲(یا ۶۴) بیتی را به عنوان ورودی پردازش می‌کنند و یک مقدار چکیده ۲۲۴،۲۵۶(یا ۳۸۴،۵۱۲) بیتی را تولید می‌کنند. نماد $\neg$ به عنوان متمم و نماد $\sum$ به عنوان مجموع به پیمانه 2^w تعریف می‌شود که w اندازه کلمه (۳۲ یا ۶۴) بیتی است . مقدار چکیده h از مقادیر زنجیره ای A_i به صورت رابطه ۵ تعریف می‌شود:

$$h = \sum_{i=1}^{t+2} A_i \qquad (5)$$

مقادیر زنجیره ای A_i به صورت رابطه ۶ تعریف می‌شوند:

$$\begin{aligned} &A_0 = IV \\ &A_i = f(A_{i-1}, w_i) \quad for\ 0 < i < t \\ &A_{t+1} = f(A_t, \sum_1) \\ &A_{t+2} = f(A_{t+1}, \sum_2) \end{aligned} \qquad (6)$$

که $\sum_1 = \neg \sum_{i=1}^{t} W_i$ و $\sum_2 = \sum_{i=1}^{t} \neg W_i$ و IV به عنوان مقدار اولیه در نظر گرفته می‌شود. ساختار تابع چکیده‌ساز *Blender-n* در شکل ۱ نشان داده شده است.



شکل ۱- ساختار تابع چکیده‌ساز *Blender-n* [9].

که مثلا برای *Blender-n-512* ، ۸ متغییر ۶۴-بیتی استفاده می‌شود. همچنین از دو بیت تنها متغییرهای حمل $c1$ و $c2$ استفاده می‌شود. این الگوریتم همچنین از سه مقدار میانه ۶۴-بیتی $T,T1,T2$ و یک مقدار صحیح میانه r برای برقراری عامل چرخش استفاده می‌کند. تابع فشرده ساز از ۴ گام ابتدایی تشکیل شده و یک دور کامل از کل ۵ گام زیر پیروی می‌کند:

۱) محاسبه مقادیر میانه اولیه با استفاده از رابطه ۷:

$$\begin{aligned} &[c1, T1] = (a5 \oplus W_t) + \left(a1 \oplus rot^8(a3)\right) + c1 \\ &[c1, T1] = \left(a0 \oplus rot^8(W_t)\right) + \left(a4 \oplus rot^8(a2)\right) + c2 \end{aligned} \qquad (7)$$

۲) محاسبه عامل چرخش

$$r = 8 - (c1 + c2) \quad (8)$$

۳) چرخش مقادیر میانه

$$T1 = rot^{r}(T1) \quad (9)$$
$$T2 = rot^{r}(T2)$$

۴) محاسبه حالت بعدی

$$\begin{aligned} T &= rot^{7}(a0) \\ a0 &= a1 \oplus T2 \\ a1 &= a2 \oplus T1 \\ a2 &= a3 \oplus T2 \\ a3 &= a4 \oplus T1 \\ a4 &= a5 \oplus T2 \\ a5 &= a6 \oplus T1 \\ a6 &= a7 \oplus T2 \\ a7 &= T \oplus T1 \end{aligned} \quad (10)$$

۵) بروزرسانی متغییرهای نتایج چکیده

$$\begin{aligned} H0 &= H0 + a0 \\ H1 &= H1 + a1 \\ H2 &= H2 + a2 \\ H3 &= H3 + a3 \\ H4 &= H4 + a4 \\ H5 &= H5 + a5 \\ H6 &= H6 + a6 \\ H7 &= H7 + a7 \end{aligned} \quad (11)$$

این ۵ گام ، یک دور از الگوریتم است [9].

۳-۲. الگوریتم *EnRupt*

EnRupt یک شبکه فیستلی نامتوازن مقیاس پذیر است که اولین بار در *XXTEA* پیشنهاد شده است. که آن بر w-بیت کلمه در فرمت *little-endian* عمل می‌کند. پهنای کلمه w ۳۲-بیت ثابت شده است. *EnRupt* دارای چهار پارامتر است:

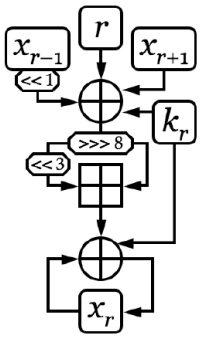
۱) منبع بلوک k (کلید).

۲) اندازه kw.

۳) بلوک هدف x .

۴)اندازه xw .[10].

بلوک *EnRupt* در شکل ۲ نشان داده شده است.



شکل ۲- یک بلوک *EnRupt* [10]

۴. اعمال تحلیل رمز چرخشی بر روی *Blender-n-512* و *EnRupt-512*

در این بخش با توجه به الگوریتم‌های معرفی شده در بخش‌های ۳-۱ و ۳-۲ با رویکرد مراجع [7] و [8] تحلیل رمز چرخشی را بدین صورت که ابتدا تعداد جمع‌های پیمانه‌ای را در کل الگوریتم پیدا می‌کنیم و بررسی می‌کنیم که اگر جمع‌های پیمانه‌ای الگوریتم به صورت مارکوف بود آنگاه با توجه به لم ۲ احتمال چرخشی را با در نظر گرفتن مقدار چرخشی r (در اینجا تحلیل چرخشی را با مقدار چرخشی $r = 1$ در نظر می گیریم) و صرف نظر کردن از ثابت ها (در صورت وجود) و n-بیت کلمه (با توجه به الگوریتم) محاسبه می‌کنیم و در غیر این صورت از لم ۱ برای محاسبه احتمال چرخشی استفاده می‌کنیم.

۴-۱. تحلیل رمز چرخشی بر *Blender-512*

در شکل ۱، ۱۰ جمع پیمانه‌ای به صورت مارکوف داریم که برای ۶۴-بیت کلمه و مقدار چرخش ۱ احتمال چرخشی برابر با $2^{-28.33}$ است و برای تابع فشرده ساز احتمال چرخشی برابر با $2^{-1.415*4} = 2^{-5.66}$ است و برای دو $\sum_1$ و $\sum_2$ بنا به تعریفشان هر کدام احتمال چرخشی برابر با $2^{-20,12}$ که به صورت مارکوف هستند و در نهایت احتمال کل برابر با $2^{-28.33-5.66*10-20.12*2} = 2^{-125.33}$ می‌باشد و همچنین به علت نوع الگوریتم قادر به محاسبه احتمال تک دور نیستیم و آن را به صورت کلی محاسبه می‌کنیم و در جدول ۲ نشان داده است.

جدول۲- خلاصه تحلیل رمز چرخشی *Blender-512*

الگوریتم رمز	دورها	احتمال تک دور	احتمال کل دور ها
Blender-512	۲+۸	–	$2^{-125.33}$

۴-۲. تحلیل رمز چرخشی بر *EnRupt*

از آنجا که چرخش و شیفت دارای احتمال چرخشی $P((x \ll s) \lll r = (x \lll r) \ll s) = 2^{-2t}$ برای شیفت به سمت راست و یا $P((x \gg s) \lll r = (x \lll r) \gg s) = 2^{-2t}$ برای شیفت به سمت چپ می‌باشد به ازای t که برابر است با $t = min(r, s, n-r, n-s)$. پس $t = min(8,3,32-3,32-8) = 3$. آنگاه احتمال شیفت و چرخش بنا به شکل ۲ برابر 2^{-6} . و احتمال چرخشی یک جمع پیمانه‌ای نیز برابر $2^{-1.415}$ که جمع کل احتمالات برابر $2^{-7.415}$ می‌باشد. که برای مثلا ۸ دور آن احتمالی برابر با $2^{8*(-7.415)} = 2^{-59.32}$ دارد که در جدول ۳ آمده است.

جدول۳- خلاصه تحلیل رمز چرخشی *EnRupt-512*

احتمال کل دور ها	احتمال تک دور	دورها	الگوریتم رمز
$2^{-59.32}$	$2^{-7.415}$	۸-دور	*EnRupt-512*

۵. نتیجه

در این مقاله برای اولین بار تحلیل رمز چرخشی را برای دو الگوریتم *Blender-n-512* و *EnRupt-512* انجام دادیم و چون این دو الگوریتم دارای ساختاری *ARX* هستند پس یکی از بهترین و جدیدترین حملات شناخته شده بر آنها تحلیل رمز چرخشی می‌باشد. در این مقاله از یک ابزار قدرتمندی به نام فرض مارکوف استفاده می‌شود و احتمال چرخشی را با در نظر گرفتن این فرض محاسبه می‌شود که باعث کاهش احتمال چرخشی و افزایش پیچیدگی حمله می‌شود، پس طراح می‌تواند با افزایش تعداد جمع‌های پیمانه‌ای، به صورت زنجیره ای از جمع‌های پیمانه‌ای که خاصیت فرض مارکوف در آن رعایت شده باشد باعث افزایش پیچیدگی شود.

با توجه به بخش ۴ دیدیم الگوریتم *Blender-n-512* احتمال چرخشی $2^{-125.33}$ را دارد که در مقایسه با الگوریتم *EnRupt-512* احتمال چرخشی کل آن $2^{-59.32}$ می‌باشد. پس به دلیل نوع طراحی الگوریتم و محل قرار گرفتن جمع‌های پیمانه‌ای الگوریتم *Blender-n-512* مقاومت بیشتری نسبت به *EnRupt-512* در مقابل تحلیل رمز چرخشی دارد. نتایج در جدول ۴ آمده است.

جدول ۴- نتایج تحلیل چرخشی بر توابع چکیده‌ساز *Blender-n-512* و *EnRupt-512*

تابع چکیده‌ساز	تعداد دور هر الگوریتم	احتمال تک دور	احتمال کل
Blender-512	۲+۸	–	$2^{-125.33}$
EnRupt	۸-دور	$2^{-7.415}$	$2^{-59.32}$

۶. منابع و مراجع

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

[2] R. Rivest, " The MD5 message-digest alghorithm," Technical report. EETF, 2000.

[3] D.Wagner, "A Generalized Birthday Problem pages," Advances in cryptology CRYPTO 2002,LNCS, vol. 2442, pp. 288-303, 2002.

[4] "Secure hash standard," FIPS PUB 180-2, 2002.

[5] T. Peyrin, "Improved Differential Attacks for ECHO and Grøstl," Crypto 2010 2010.

[6] S. Klaus, "Cryptography and public key infrastructure on the Internet," 2003.

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

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

[9] C. Bradbury, "blender,A Proposed New Family of Cryptographic Hash Algorithms," 2008.

[10] S. OÕNeil , "EnRUPT,First all-in-one symmetric cryptographic primitive," SASC, 2008.