نشریه علمی «نوآوری های فناوری اطلاعات و ارتباطات کاربردی»
سال اول، شماره ۱، پاییز ۱۳۹۸؛ ص ۴۳- ۳۷

تحلیل رمز چرخشی برروی BMW , SIMD

سید علی طباطبائی فیض‌آباد[۱]، احمد گائینی[۲*]، بهبد کشاورز[۳]
۱ و ۲- کارشناسی ارشد، ۳- استادیار، دانشگاه جامع امام حسین (ع)
(دریافت: ۹۸/۰۲/۰۴؛ پذیرش: ۹۸/۰۴/۱۰)

چکیده

تابع چکیده‌ساز تابعی است یک طرفه که رشته صفر و یک ورودی با طول دلخواه را به یک رشته صفر و یک با طول ثابت n تبدیل می‌کند. تابع چکیده‌ساز باید سریع، ساده و یک طرفه باشد و در برابر حملات برخورد، پیش تصویر و پیش تصویر دوم مقاوم باشد. یکی از مهم‌ترین کاربردهای توابع چکیده‌ساز در امضای رقمی است، با استفاده از توابع چکیده‌ساز، امضا کننده به‌جای این‌که کل پیام را امضا کند، ابتدا مقدار چکیده پیام را به‌دست آورده و سپس این مقدار را امضا می‌کند. لذا این کار باعث افزایش امنیت و کاهش حجم محاسبات می‌شود. تجزیه و تحلیل رمز یا شکستن رمز، به کلیه اقدامات مبتنی‌بر 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. تحلیل رمز چرخشی یکی از بهترین و جدیدترین حملات بر علیه سیستم‌های ARX می باشد. در این مقاله برای اولین‌بار بر الگوریتم‌های SIMD, BMW که کاندیداهای دور دوم مسابقه SHA-3 هستند و در ساختار خود مطابق سیستم‌های ARX از سه عملگر چرخش، جمع پیمانه‌ای و یای انحصاری استفاده می کنند، با در نظر گرفتن فرض مارکوف تحلیل رمز چرخشی انجام می‌شود و به ترتیب پیچیدگی $2^{180,68}$ برای یک دور از ۱۶-دور BMW و پیچیدگی $2^{101,88}$ برای کل دورهای SIMD را داریم. با توجه به نتایج به‌دست‌آمده مشاهده می‌شود که به‌علت وجود تعداد بیشتری از جمع‌های پیمانه‌ای که به‌صورت زنجیره مارکوف هستند، الگوریتم BMW مقاومت بیشتری نسبت به الگوریتم SIMD در برابر تحلیل رمز چرخشی از خود نشان می‌دهد و احتمال موفقیت کمتری دارد.

واژگان کلیدی

توابع چکیده ساز، تحلیل رمز چرخشی، جمع پیمانه ای، فرض زنجیره مارکوف

۱- مقدمه

یکی از توابع پایهٔ مورد استفاده در رمزنگاری تابع چکیده‌ساز[1] است که به‌عنوان مثال دارای کاربرد در امر جامعیت اطلاعات و امضاء رقمی می باشد. تابع چکیده ساز تابعی است که یک پیام با طول تصادفی را به‌عنوان ورودی دریافت کند و یک نتیجهٔ چکیده ساز با طول ثابت از آن تولید کند. در یک تابع چکیده‌ساز شرط لازم برای این‌که خروجی آن بتواند یک اثر منحصربه‌فرد از پیام را ارائه کند این است که پیدا کردن زوج‌های دارای تلاقی، پیام‌هایی که به یک خروجی یکسان نگاشت شوند، عملی نباشد [۱].

در پاسخ به 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 [۲].

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 به‌کار گرفتن هرگونه اطلاعات جانبی موجود، ضعف‌های امنیتی احتمالی موجود در سیستم رمزنگاری یافت شود و از این طریق به‌نحوی کلید رمز به‌دست‌آمده و یا محتوای اطلاعات رمزشده استخراج گردد. تجزیه و تحلیل رمز، گاهی به‌منظور

* رایانامه نویسنده پاسخگو: a.gaeini20@gmail.com
[1] Hash function

شکستن امنیت یک سیستم رمزنگاری و به‌عنوان خرابکاری و یک فعالیت ضد امنیتی انجام می‌شود و گاهی هم به‌منظور ارزیابی یک پروتکل یا الگوریتم رمزنگاری و برای کشف ضعف‌ها و آسیب‌پذیری‌های احتمالی آن صورت می‌پذیرد [۳].

تحلیل رمز چرخشی[1] جزء حملات عمومی است که بر روی الگوریتم هایی که از سه عملگر چرخش و جمع پیمانه‌ای و یا انحصاری در ساختارشان استفاده می‌کنند موثر است و اولین بار دیمیتری خوواراتویچ[2] و ایویکا نیکولیچ[3] آن را در سال ۲۰۱۰ ارائه دادند و در سال ۲۰۱۵ آن را بهبود بخشیدند بدین صورت که ابتدا بر این باور بودند که برای انجام یک تحلیل رمز مناسب و بدست آوردن احتمال مطلوب باید تنها عملگر جمع پیمانه‌ای را شمرد و احتمال چرخشی را محاسبه نمود [۴] در صورتی که در سال ۲۰۱۵ تحلیل رمز خود را مورد بازبینی قرار دادند و یک شرط جدید به مسئله اضافه کردند و آن این بود که برای محاسبه احتمال چرخشی علاوه‌بر شمارش تعداد جمع‌های پیمانه‌ای باید به محل قرار گرفتن آنها نیز توجه شود بدین صورت که اگر خروجی یک جمع پیمانه‌ای به‌عنوان ورودی برای جمع پیمانه‌ای بعدی باشد باید فرض زنجیره مارکوف[4] برای جمع‌های پیمانه‌ای در نظر گرفته شود و آنها با این توضیحات یک احتمال جدیدی برای محاسبه احتمال چرخشی ارائه دادند [۵].

در این مقاله برای اولین بار رویکرد مراجع [۵-۴] را برای محاسبه احتمال چرخشی دو الگوریتم SIMD, BMW[5] که کاندیدای راه یافته به دور دوم مسابقه SHA-3 هستند و ساختار ARX دارند را به‌کار می‌بریم. در بخش دوم این مقاله حمله تحلیل رمز چرخشی را تشریح می‌کنیم و الزامات اجرای تحلیل رمز چرخشی را مورد بررسی قرار می‌دهیم و در بخش سوم به بررسی مختصری از الگوریتم‌های SIMD, BMW می‌پردازیم و در بخش چهارم تحلیل رمز چرخشی را بر الگوریتم‌های رمز اعمال کرده و در بخش آخر نتیجه بحث را ارائه می‌کنیم.

۲- تشریح تحلیل رمز چرخشی

در مرجع [۴] روش کلی برای تحلیل سیستم‌های ARX نشان داده شده است، ایده کلی فرض جفت کلمه‌ها است که یکی چرخش دیگری به اندازه r-بیت می‌باشد. که عملگرهای چرخشی به‌وسیله r ⋙یا r ⋘ و یا به‌طور معادل $\vec{x}$ و $\tilde{x}$ تعریف می‌شوند. که $\vec{x}$ چرخش x به‌اندازه r-بیت به سمت راست را نشان می‌دهد که $(x.\vec{x})$ جفت چرخشی به اندازه r-بیت می‌نامیم. اثبات این‌که یک جفت چرخشی با هر تبدیل بیتی حفظ می‌شود آسان است مخصوصا یای انحصاری[6] و چرخش که در رابطه (۱) نشان داده است.

$$\overrightarrow{x \oplus y} = \vec{x} \oplus \vec{y} \;.\; \vec{x} \ggg r \cdot = \overrightarrow{x \ggg r} \cdot \qquad (۱)$$

جمع پیمانه‌ای را به مد 2^n در نظر می‌گیریم، احتمال این که جفت چرخشی از جمع پیمانه‌ای[7] بیرون آید توسط لم ۱ محاسبه می‌شود.

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

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

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

جدول (۱): احتمالات چرخشی به‌ازای مقادیر 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 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 $\mathcal{S}(\vec{I}) = \overrightarrow{\mathcal{S}(I)}$ با احتمال $P_r{}^q$.

اثبات: به کمک استقرا بروی اندازه طرح [۴].

به‌منظور اعمال تحلیل چرخشی، سعی می‌کنیم تا ورودی‌های

[1] Rotational Cryptanalysis
[2] Dimitry Khovratovich
[3] Ivica Nikolic
[4] Markov chaining
[5] Blue MidNight Wish
[6] xor
[7] Mudolar Addition

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

مرجع [۵] 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 به‌دست آید. این بدین معنی است که فرض رمز مارکوف استفاده شده برای محاسبه ضمنی احتمال از این طریق امکان‌پذیر نیست.

دنباله‌ای از متغییر های تصادفی گسسته $v_0 . \dots . v_r$ یک دنباله مارکوف است اگر برای $0 < i < r$ رابطه (۳) برقرار باشد:

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

احتمال چرخشی ARX به سادگی با شمارش تعداد جمع محاسبه نمی‌شود و باید روابط موقعیت جمع‌های پیمانه‌ای را بررسی کنیم، یعنی این که آیا جمع‌های پیمانه‌ای به‌صورت متوالی در الگوریتم آمده اند یا جدا جدا و در بین عملگرهای دیگر آمده‌اند. درحقیقت زنجیره بزرگتر برای جمع‌های پیمانه‌ای احتمال چرخشی کمتری دارد. احتمال چرخشی جمع‌های پیمانه ای زنجیره ای در لم ۲ آمده است:

لم۲: فرض کنید $a_1 . \dots . a_k$ کلمه‌های n-بیتی باشند که به‌صورت تصادفی انتخاب شده باشند و r یک عدد صحیح مثبت که $0 < r < n$ آن‌گاه احتمال چرخشی از رابطه (۳) به‌دست می‌آید.

$$\begin{aligned} P_r([(a_1 + a_2) \lll r = a_1 \lll r + a_2 \\ \lll r] \wedge [(a_1 + a_2 + a_3) \lll r \\ = a_1 \lll r + a_2 \lll r + a_2 \\ \lll r] \wedge \dots \\ \wedge [(a_1 + \dots + a_k) \lll r = a_1 \\ \lll r + \dots + a_k \lll r]) = \end{aligned}$$

$$\frac{1}{2^{nk}} \binom{k + 2^r - 1}{2^r - 1} \binom{k + 2^{n-r} - 1}{2^{n-r} - 1} \quad (۴)$$

به طور خلاصه، احتمال چرخشی رمزنگاری لزوما برابر با حاصلضرب تک تک احتمالات چرخشی نیست. چنین میانبری در تخمین احتمال نه کران بالا نه کران پایین از احتمال واقعی را می‌دهد. بعد از تایید زنجیره مارکوف می‌توان احتمال را تخمین زد. در غیر این‌صورت، احتمال چرخشی باید اقتضایی محاسبه گردد.

۳- معرفی الگوریتم‌های BMW, SIMD

در این بخش به معرفی کوتاهی از هر الگوریتم می پرداریم و با توجه به تحلیل رمز چرخشی، الگوریتم‌ها را برای یافتن تعداد جمع پیمانه ای به کار رفته شده در آنها و فرض زنجیره مارکوف در توابع فشرده ساز و ساختارشان بررسی می‌کینم.

۳-۱- الگوریتم BMW-512

در اینجا الگوریتم BMW-512 را باختصار برای یافتن تعداد جمع های پیمانه‌ای و طریقه اتصال آنها مورد بررسی قرار می‌دهیم، برای تشریح الگوریتم، با توجه به شکل (۱) مشاهده می‌کنیم که بعد از مراحل لایه گذاری[1] و مقداردهی اولیه $H^{(0)}$، مقدار چکیده[2] از کد زیر محاسبه می‌شود.

For $i = 1$ to N

{

$Q_a^{(i)} = f_0(M^{(i)}, H^{(i-1)});$

$Q_b^{(i)} = f_1(M^{(i)}, H^{(i-1)}, Q_a^{(i)});$

$H^{(i)} = f_2(M^{(i)}, Q_a^{(i)}, Q_b^{(i)});$

}

شکل (۱): محاسبه مقدار چکیده که در آن N=16 تعداد بلوک‌های پیام که از مرحله لایه گذاری به‌دست می‌آید [۶]

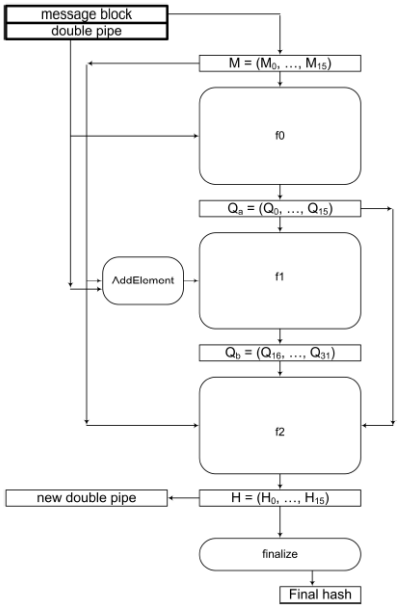
با توجه به شکل (۳) درانتها یک دور پایانی نیز داریم که مقدار چکیده نهایی[3] را محاسبه می‌کند که کد آن مطابق شکل (۲) است.

$$Q_a^{final} = f_0(H^{(N)}, CONST^{final});$$
$$Q_b^{final} = f_1(H^{(N)}, CONST^{final}, Q_a^{final});$$
$$H^{final} = f_2(H^{(N)}, Q_a^{final}, Q_b^{final});$$

شکل (۱): محاسبه مقدار چکیده پایانی الگوریتم BMW-512 [۶]

همان‌طور که در شکل (۳) می‌بینیم الگوریتم دارای سه تابع f_0، f_1، f_2 و با توجه به شکل (۲) برای محاسبه دور پایانی نیز سه تابع f_0، f_1، f_2 راداریم. باتوجه به شکل (۴) تابع f_0 ۱۶- جمع پیمانه‌ای به‌صورت فرض زنجیره مارکوف دارد و ۶۴- جمع پیمانه‌ای دارد، همچنین با توجه به شکل (۵) تابع f_1 هیچ جمع پیمانه‌ای ندارد و با توجه به شکل (۶) تابع f_2، ۲۴- جمع پیمانه‌ای دارد. همچنین الگوریتم BMW-512، ۱۶- دور اصلی و یک دور پایانی دارد.

[1] Padding
[2] Hash Value
[3] Final



شکل (۲۰): الگوریتم تابع فشرده‌ساز Blue MidNight Wish [۶].

$f_0 : \{0,1\}^{2m} \rightarrow \{0,1\}^m$

Input: Message block $M^{(i)} = (M_0^{(i)}, M_1^{(i)}, \ldots, M_{15}^{(i)})$, and the previous double pipe $H^{(i-1)} = (H_0^{(i-1)}, H_1^{(i-1)}, \ldots, H_{15}^{(i-1)})$.
Output: First part of the quadruple pipe $Q_a^{(i)} = (Q_0^{(i)}, Q_1^{(i)}, \ldots, Q_{15}^{(i)})$.

1. Bijective transform of $M^{(i)} \oplus H^{(i-1)}$:

$$
\begin{aligned}
W_0^{(i)} &= (M_5^{(i)} \oplus H_5^{(i-1)}) - (M_7^{(i)} \oplus H_7^{(i-1)}) + (M_{10}^{(i)} \oplus H_{10}^{(i-1)}) + (M_{13}^{(i)} \oplus H_{13}^{(i-1)}) + (M_{14}^{(i)} \oplus H_{14}^{(i-1)})\\
W_1^{(i)} &= (M_6^{(i)} \oplus H_6^{(i-1)}) - (M_8^{(i)} \oplus H_8^{(i-1)}) + (M_{11}^{(i)} \oplus H_{11}^{(i-1)}) + (M_{14}^{(i)} \oplus H_{14}^{(i-1)}) - (M_{15}^{(i)} \oplus H_{15}^{(i-1)})\\
W_2^{(i)} &= (M_0^{(i)} \oplus H_0^{(i-1)}) + (M_7^{(i)} \oplus H_7^{(i-1)}) + (M_9^{(i)} \oplus H_9^{(i-1)}) - (M_{12}^{(i)} \oplus H_{12}^{(i-1)}) + (M_{15}^{(i)} \oplus H_{15}^{(i-1)})\\
W_3^{(i)} &= (M_0^{(i)} \oplus H_0^{(i-1)}) - (M_1^{(i)} \oplus H_1^{(i-1)}) + (M_8^{(i)} \oplus H_8^{(i-1)}) - (M_{10}^{(i)} \oplus H_{10}^{(i-1)}) + (M_{13}^{(i)} \oplus H_{13}^{(i-1)})\\
W_4^{(i)} &= (M_1^{(i)} \oplus H_1^{(i-1)}) + (M_2^{(i)} \oplus H_2^{(i-1)}) + (M_9^{(i)} \oplus H_9^{(i-1)}) - (M_{11}^{(i)} \oplus H_{11}^{(i-1)}) - (M_{14}^{(i)} \oplus H_{14}^{(i-1)})\\
W_5^{(i)} &= (M_3^{(i)} \oplus H_3^{(i-1)}) - (M_2^{(i)} \oplus H_2^{(i-1)}) + (M_{10}^{(i)} \oplus H_{10}^{(i-1)}) - (M_{12}^{(i)} \oplus H_{12}^{(i-1)}) + (M_{15}^{(i)} \oplus H_{15}^{(i-1)})\\
W_6^{(i)} &= (M_4^{(i)} \oplus H_4^{(i-1)}) - (M_0^{(i)} \oplus H_0^{(i-1)}) - (M_3^{(i)} \oplus H_3^{(i-1)}) - (M_{11}^{(i)} \oplus H_{11}^{(i-1)}) + (M_{13}^{(i)} \oplus H_{13}^{(i-1)})\\
W_7^{(i)} &= (M_1^{(i)} \oplus H_1^{(i-1)}) - (M_4^{(i)} \oplus H_4^{(i-1)}) - (M_5^{(i)} \oplus H_5^{(i-1)}) - (M_{12}^{(i)} \oplus H_{12}^{(i-1)}) - (M_{14}^{(i)} \oplus H_{14}^{(i-1)})\\
W_8^{(i)} &= (M_2^{(i)} \oplus H_2^{(i-1)}) - (M_5^{(i)} \oplus H_5^{(i-1)}) - (M_6^{(i)} \oplus H_6^{(i-1)}) + (M_{13}^{(i)} \oplus H_{13}^{(i-1)}) - (M_{15}^{(i)} \oplus H_{15}^{(i-1)})\\
W_9^{(i)} &= (M_0^{(i)} \oplus H_0^{(i-1)}) - (M_3^{(i)} \oplus H_3^{(i-1)}) + (M_6^{(i)} \oplus H_6^{(i-1)}) - (M_7^{(i)} \oplus H_7^{(i-1)}) + (M_{14}^{(i)} \oplus H_{14}^{(i-1)})\\
W_{10}^{(i)} &= (M_8^{(i)} \oplus H_8^{(i-1)}) - (M_1^{(i)} \oplus H_1^{(i-1)}) - (M_4^{(i)} \oplus H_4^{(i-1)}) - (M_7^{(i)} \oplus H_7^{(i-1)}) + (M_{15}^{(i)} \oplus H_{15}^{(i-1)})\\
W_{11}^{(i)} &= (M_8^{(i)} \oplus H_8^{(i-1)}) - (M_0^{(i)} \oplus H_0^{(i-1)}) - (M_2^{(i)} \oplus H_2^{(i-1)}) - (M_5^{(i)} \oplus H_5^{(i-1)}) + (M_9^{(i)} \oplus H_9^{(i-1)})\\
W_{12}^{(i)} &= (M_1^{(i)} \oplus H_1^{(i-1)}) + (M_3^{(i)} \oplus H_3^{(i-1)}) - (M_6^{(i)} \oplus H_6^{(i-1)}) - (M_9^{(i)} \oplus H_9^{(i-1)}) + (M_{10}^{(i)} \oplus H_{10}^{(i-1)})\\
W_{13}^{(i)} &= (M_2^{(i)} \oplus H_2^{(i-1)}) + (M_4^{(i)} \oplus H_4^{(i-1)}) + (M_7^{(i)} \oplus H_7^{(i-1)}) + (M_{10}^{(i)} \oplus H_{10}^{(i-1)}) + (M_{11}^{(i)} \oplus H_{11}^{(i-1)})\\
W_{14}^{(i)} &= (M_3^{(i)} \oplus H_3^{(i-1)}) - (M_5^{(i)} \oplus H_5^{(i-1)}) + (M_8^{(i)} \oplus H_8^{(i-1)}) - (M_{11}^{(i)} \oplus H_{11}^{(i-1)}) - (M_{12}^{(i)} \oplus H_{12}^{(i-1)})\\
W_{15}^{(i)} &= (M_{12}^{(i)} \oplus H_{12}^{(i-1)}) - (M_4^{(i)} \oplus H_4^{(i-1)}) - (M_6^{(i)} \oplus H_6^{(i-1)}) - (M_9^{(i)} \oplus H_9^{(i-1)}) + (M_{13}^{(i)} \oplus H_{13}^{(i-1)})
\end{aligned}
$$

2. Further bijective transform of $W_j^{(i)}, j = 0, \ldots, 15$:

$$
\begin{aligned}
&Q_0^{(i)} = s_0(W_0^{(i)}) + H_1^{(i-1)}; \quad Q_1^{(i)} = s_1(W_1^{(i)}) + H_2^{(i-1)}; \quad Q_2^{(i)} = s_2(W_2^{(i)}) + H_3^{(i-1)}; \quad Q_3^{(i)} = s_3(W_3^{(i)}) + H_4^{(i-1)};\\
&Q_4^{(i)} = s_4(W_4^{(i)}) + H_5^{(i-1)}; \quad Q_5^{(i)} = s_0(W_5^{(i)}) + H_6^{(i-1)}; \quad Q_6^{(i)} = s_1(W_6^{(i)}) + H_7^{(i-1)}; \quad Q_7^{(i)} = s_2(W_7^{(i)}) + H_8^{(i-1)};\\
&Q_8^{(i)} = s_3(W_8^{(i)}) + H_9^{(i-1)}; \quad Q_9^{(i)} = s_4(W_9^{(i)}) + H_{10}^{(i-1)}; \quad Q_{10}^{(i)} = s_0(W_{10}^{(i)}) + H_{11}^{(i-1)}; \quad Q_{11}^{(i)} = s_1(W_{11}^{(i)}) + H_{12}^{(i-1)};\\
&Q_{12}^{(i)} = s_2(W_{12}^{(i)}) + H_{13}^{(i-1)}; \quad Q_{13}^{(i)} = s_3(W_{13}^{(i)}) + H_{14}^{(i-1)}; \quad Q_{14}^{(i)} = s_4(W_{14}^{(i)}) + H_{15}^{(i-1)}; \quad Q_{15}^{(i)} = s_0(W_{15}^{(i)}) + H_0^{(i-1)};
\end{aligned}
$$

شکل (۳): عملکرد تابع f_0 [۶]

$f_1 : \{0,1\}^{3m} \rightarrow \{0,1\}^m$

Input: Message block $M^{(i)} = (M_0^{(i)}, M_1^{(i)}, \ldots, M_{15}^{(i)})$, the previous double pipe $H^{(i-1)} = (H_0^{(i-1)}, H_1^{(i-1)}, \ldots, H_{15}^{(i-1)})$ and the first part of the quadruple pipe $Q_a^{(i)} = (Q_0^{(i)}, Q_1^{(i)}, \ldots, Q_{15}^{(i)})$.
Output: Second part of the quadruple pipe $Q_b^{(i)} = (Q_{16}^{(i)}, Q_{17}^{(i)}, \ldots, Q_{31}^{(i)})$.

1. Double pipe expansion according to the tunable parameters $ExpandRounds_1$ and $ExpandRounds_2$.

1.1 For $ii = 0$ to $ExpandRounds_1 - 1$

$$Q_{ii+16}^{(i)} = expand_1(ii + 16)$$

1.2 For $ii = ExpandRounds_1$ to $ExpandRounds_1 + ExpandRounds_2 - 1$

$$Q_{ii+16}^{(i)} = expand_2(ii + 16)$$

شکل (۴): عملکرد تابع f_1 [۶]

Folding $f_2 : \{0,1\}^{3m} \rightarrow \{0,1\}^m$

Input: Message block $M^{(i)} = (M_0^{(i)}, M_1^{(i)}, \ldots, M_{15}^{(i)})$,
quadruple pipe $Q^{(i)} = (Q_0^{(i)}, Q_1^{(i)}, \ldots, Q_{15}^{(i)}, Q_{16}^{(i)}, \ldots, Q_{31}^{(i)})$.
Output: New double pipe $H^{(i)} = (H_0^{(i)}, H_1^{(i)}, \ldots, H_{15}^{(i)})$.

1. Compute the cumulative temporary variables XL and XH.

$$XL = Q_{16}^{(i)} \oplus Q_{17}^{(i)} \oplus \ldots \oplus Q_{23}^{(i)}$$
$$XH = XL \oplus Q_{24}^{(i)} \oplus Q_{25}^{(i)} \oplus \ldots \oplus Q_{31}^{(i)}$$

2. Compute the new double pipe $H^{(i)}$:

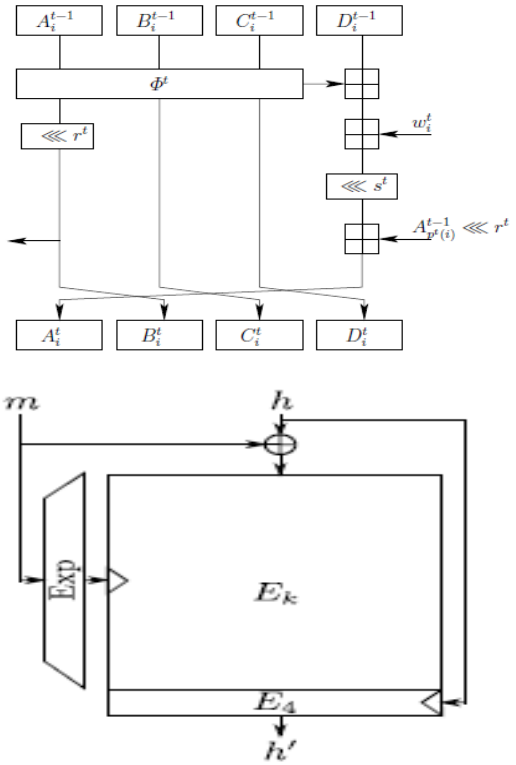
$$H_0^{(i)} = \left(SHL^5(XH) \oplus SHR^5(Q_{16}^{(i)}) \oplus M_0^{(i)}\right) + \left(XL \oplus Q_{24}^{(i)} \oplus Q_0^{(i)}\right)$$
$$H_1^{(i)} = \left(SHR^7(XH) \oplus SHL^8(Q_{17}^{(i)}) \oplus M_1^{(i)}\right) + \left(XL \oplus Q_{25}^{(i)} \oplus Q_1^{(i)}\right)$$
$$H_2^{(i)} = \left(SHR^5(XH) \oplus SHL^5(Q_{18}^{(i)}) \oplus M_2^{(i)}\right) + \left(XL \oplus Q_{26}^{(i)} \oplus Q_2^{(i)}\right)$$
$$H_3^{(i)} = \left(SHR^1(XH) \oplus SHL^5(Q_{19}^{(i)}) \oplus M_3^{(i)}\right) + \left(XL \oplus Q_{27}^{(i)} \oplus Q_3^{(i)}\right)$$
$$H_4^{(i)} = \left(SHR^3(XH) \oplus Q_{20}^{(i)} \oplus M_4^{(i)}\right) + \left(XL \oplus Q_{28}^{(i)} \oplus Q_4^{(i)}\right)$$
$$H_5^{(i)} = \left(SHL^6(XH) \oplus SHR^6(Q_{21}^{(i)}) \oplus M_5^{(i)}\right) + \left(XL \oplus Q_{29}^{(i)} \oplus Q_5^{(i)}\right)$$
$$H_6^{(i)} = \left(SHR^4(XH) \oplus SHL^6(Q_{22}^{(i)}) \oplus M_6^{(i)}\right) + \left(XL \oplus Q_{30}^{(i)} \oplus Q_6^{(i)}\right)$$
$$H_7^{(i)} = \left(SHR^{11}(XH) \oplus SHL^2(Q_{23}^{(i)}) \oplus M_7^{(i)}\right) + \left(XL \oplus Q_{31}^{(i)} \oplus Q_7^{(i)}\right)$$
$$H_8^{(i)} = ROTL^9(H_4^{(i)}) + \left(XH \oplus Q_{24}^{(i)} \oplus M_8^{(i)}\right) + \left(SHL^8(XL) \oplus Q_{23}^{(i)} \oplus Q_8^{(i)}\right)$$
$$H_9^{(i)} = ROTL^{10}(H_5^{(i)}) + \left(XH \oplus Q_{25}^{(i)} \oplus M_9^{(i)}\right) + \left(SHR^6(XL) \oplus Q_{16}^{(i)} \oplus Q_9^{(i)}\right)$$
$$H_{10}^{(i)} = ROTL^{11}(H_6^{(i)}) + \left(XH \oplus Q_{26}^{(i)} \oplus M_{10}^{(i)}\right) + \left(SHL^6(XL) \oplus Q_{17}^{(i)} \oplus Q_{10}^{(i)}\right)$$
$$H_{11}^{(i)} = ROTL^{12}(H_7^{(i)}) + \left(XH \oplus Q_{27}^{(i)} \oplus M_{11}^{(i)}\right) + \left(SHL^4(XL) \oplus Q_{18}^{(i)} \oplus Q_{11}^{(i)}\right)$$
$$H_{12}^{(i)} = ROTL^{13}(H_0^{(i)}) + \left(XH \oplus Q_{28}^{(i)} \oplus M_{12}^{(i)}\right) + \left(SHR^3(XL) \oplus Q_{19}^{(i)} \oplus Q_{12}^{(i)}\right)$$
$$H_{13}^{(i)} = ROTL^{14}(H_1^{(i)}) + \left(XH \oplus Q_{29}^{(i)} \oplus M_{13}^{(i)}\right) + \left(SHR^4(XL) \oplus Q_{20}^{(i)} \oplus Q_{13}^{(i)}\right)$$
$$H_{14}^{(i)} = ROTL^{15}(H_2^{(i)}) + \left(XH \oplus Q_{30}^{(i)} \oplus M_{14}^{(i)}\right) + \left(SHR^7(XL) \oplus Q_{21}^{(i)} \oplus Q_{14}^{(i)}\right)$$
$$H_{15}^{(i)} = ROTL^{16}(H_3^{(i)}) + \left(XH \oplus Q_{31}^{(i)} \oplus M_{15}^{(i)}\right) + \left(SHR^2(XL) \oplus Q_{22}^{(i)} \oplus Q_{15}^{(i)}\right)$$

شکل (۵): عملکرد تابع f_2 [۶]

۳-۲- الگوریتم SIMD-512

SIMD یک تابع چکیده‌ساز تکراری که از طرح مرکل- دمگارد پیروی می کند. جزء اصلی یک تابع چکیده‌ساز، تابع فشرده‌ساز آن است. در مورد SIMD-512 برای محاسبه چکیده پیام M، در ابتدا آن را به k تکه ۱۰۲۴- بیتی تقسیم می‌کنیم. با استفاده از گسترش پیام، هر بلوک به ۸۱۹۲- بیت گسترش می‌یابد. سپس تابع فشرده‌ساز برای فشرده‌سازی تکه‌های پیام و فضای حالت داخلی مورد استفاده قرار می‌گیرد. قانون لایه‌گذاری برای پر کردن آخرین بلوک به‌عنوان مرکل- دمگارد شناخته شده است. مقدار اولیه حالت درونی IV نامیده می‌شود و در مشخصات تابع چکیده‌ساز ثابت شده است. خروجی تابع چکیده‌ساز به‌وسیله محاسبه یک تابع نهایی بر آخرین فضای حالت درونی به‌دست می‌آید.

فضای حالت درونی SIMD شامل ۳۲ تا کلمه ۳۲-بیتی است و دو برابر بزرگتر از خروجی است. SIMD شامل ۴-دور است که هر دور شامل ۸-گام است. همان‌طور که در شکل (۸) می بینیم چهار مرحله اضافی با IV به‌عنوان ورودی پیام داریم. قسمت هسته SIMD تابع گام به‌روز رسانی فضای حالت است. شکل (۷) تابع گام را در گام t نشان می‌دهد.



شکل (۶): تابع به‌روز رسانی SIMD در گام t به ازای i=0,...,7.

[۷] شکل (۷۰) ساختار SIMD با k=32 [۸]

۳۲-گام SIMD به چهار دور تقسیم می‌شوند که هر کدام دارای ۸-گام می باشند که هر گام ۳ جمع پیمانه‌ای دارد که دوتای آنها خاصیت مارکوف دارند و ۴-گام اضافی بعدی نیز تابع گام[1] مشابه با گام های قبلی دارد [۷-۸].

۴- اعمال تحلیل رمز چرخشی بر روی BMW-512 و SIMD-512

در این بخش با توجه به تجزیه و تحلیل انجام شده در بخش‌های ۳-۱ ، ۳-۲ و لم‌های ۱و۲ تحلیل رمز چرخشی را بر الگوریتم‌های BMW-512 و SIMD-512 اعمال می‌کنیم و در این مقاله مقدار چرخشی $r = 1$ قرار می‌دهیم و از ثابت‌ها درصورت وجود صرف نظر می‌کنیم و مقدار n را با توجه به الگوریتم ها ۳۲-بیت کلمه در نظر می‌گیریم.

۴-۱- تحلیل رمز چرخشی بر BMW-512

بنا به توضیحات بخش ۳-۱، سه تابع f_0، f_2 شامل جمع پیمانه‌ای بودند که در f_0، ۸۰-جمع پیمانه ای داریم که ۱۶ تای آن مارکوف می باشد پس برای محاسبه ۱۶ جمع پیمانه ای با فرض مارکوف از لم ۲ مقدار احتمال چرخشی برابر با $2^{-56,16}$ می‌باشد و همچنین ۶۴ جمع پیمانه‌ای الگوریتم بنا به لم ۱ داری احتمال چرخشی $2^{-90,56}$ می‌باشد. در تابع f_2، ۲۴ جمع پیمانه‌ای داریم که بنا به لم ۱، احتمال چرخشی آن برابر $2^{-33,96}$ می‌باشد. که مجموع آن برابر $2^{-180,68}$ می باشد. حال می‌دانیم که الگوریتم BMW-512، ۱۶-دور دارد پس داریم $2^{-2890,88} = 2^{-180,68*16}$ می‌شود که با احتساب یک دور پایانی داریم $2^{-2892,30} = 2^{-2890,88-1,415}$.

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

الگوریتم رمز	دورها	احتمال تک دور	احتمال کل دور ها
Blue MidNight Wish	۱+۱۶ دور پایانی	$2^{-180,68}$	$2^{-2892,30}$

۴-۲- تحلیل رمز چرخشی بر SIMD-512

همان‌طور که در شکل (۷) مشاهده می‌کنیم و بنا به توضیحات بخش ۳-۲ و با استفاده از لم ۲ برای محاسبه احتمال چرخشی برای دو جمع پیمانه‌ای که خاصیت مارکوف دارند و اندازه کلمه ۳۲-بیت و مقدار چرخشی ۱ و بدون در نظر گرفتن ثابت‌ها

[1] Step Function

احتمال $2^{-1,415}$ را داریم. و برای یک جمع پیمانه‌ای دیگر که خاصیت مارکوف ندارد با استفاده از لم ۱ احتمال $2^{-1,415}$ را داریم که با جمع این دو احتمال، احتمال چرخشی برای این سه جمع پیمانه‌ای برابر با $2^{-2,83}$ می‌باشد که برای ۳۶-گام احتمال برابر با $2^{-101,88} = 2^{-2,83\cdot 36}$ می‌باشد.

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

احتمال کل گام‌ها	احتمال یک گام	گام‌ها	الگوریتم رمز
$2^{-101,88}$	$2^{-2,83}$	۳-گام	SIMD-512

۴-۳- مقایسه پیچیدگی تحلیل رمز چرخشی در الگوریتم‌های BMW و SIMD با دیگر حملات

در مرجع [۹] بر روی الگوریتم SIMD-512 حملات تصادم نزدیک[1] و تمایزگز[2] انجام شده است که در حمله تصادم نزدیک پیچیدگی حمله برابر با 2^{235} و برای حمله تمایزگر پیچیدگی برابر با 2^{475} می‌باشد اما در تحلیل رمز چرخشی پیچیدگی $2^{101.88}$ را داریم. همچنین در مرجع [۸] برای BMW-384 پیچیدگی حمله تمایز چرخشی برابر $2^{354.50}$ می‌باشد درصورتی که در تحلیل رمز چرخشی برای الگوریتم BMW-512 پیچیدگی برابر $2^{180,68}$ می‌باشد.

۵- نتیجه‌گیری

در این مقاله برای اولین بار بر دو کاندیدای دور دوم SHA-3 یعنی الگوریتم‌های BMW-512 و SIMD-512 که ساختاری ARX دارند تحلیل رمز چرخشی را با رویکرد مراجع [۵-۴] و با در نظر گرفتن فرض زنجیره مارکوف انجام دادیم و به پیچیدگی کل $2^{2892,30}$ برای BMW-512 و پیچیدگی کل $2^{101,88}$ برای SIMD-512 رسیدیم که علت بیشتر بودن مقاومت الگوریتم BMW-512 در برابر تحلیل رمز چرخشی، بستگی به نوع اتصال و تعداد جمع‌های پیمانه‌ای دارد. این بدین معنی است که طراح برای جلوگیری از حمله چرخشی، می تواند جمع‌های پیمانه‌ای را به‌صورت زنجیره‌ای مطابق فرض مارکوف در الگوریتم قرار دهد.

تابع چکیده ساز	تعداد دور هر الگوریتم	احتمال تک دور	احتمال کل
BMW-512	۱۶	$2^{-180,68}$	$2^{-2892,30}$
SIMD-512	۳۶ گام	$2^{-2,83}$	$2^{-101,88}$

[1] Near collision attack
[2] Distinguisher attack

۶- مراجع

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

[2] F. Mendel and T. Nad, "A Distinguisher for the Compression Function of SIMD-512," INDOCRYPT,, vol. 5922, pp. 219-232, 2010.

[3] I. Nikolic, J. Pieprzyk, P. law, S. lowski and R. Steinfeld, "Rotational Cryptanalysis of ((Modified) version of BMW and SIMD," 2011.

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

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

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

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

[8] X. Wang and H. Yu, "Cryptanalysis of the Compression Function of SIMD," ACISP 2011, pp. 157-171, 2011.

[9] D. Gligoroski, V. Klima, S. J. Knapskog, M. El-Hadedy, J. Amundsen and S. F. Mjølsnes, "Cryptographic Hash Function BLUE MIDNIGHT WISH," Submission, 2010.

Journal of "Innovations of Applied Information and Communication Technologies"

Vol. 1, No. 1, 2019 (Serial No. 1)

Rotational Cryptanalysis on BMW and SIMD

S. A. Tabatabaei Feyz Abad, A. Ghaeini*, B. Keshavarz

Imam Hossein Comprehensive University

Abstract

The hash function is a one-way function that converts a string of zero and one input with arbitrary length to a string of zero and one with a constant length n. The hash function should be fast, simple and one-way and resistant to collision attacks, Preimage and Second –Preimage. One of the most important applications of the hash function is digital signature. By using the hash functions, instead of entire signed message the signer first obtains the hash value of the message and then signs the value. This will increase the security and reduce the amount of computing. Cryptanalysis refers to all actions based on the principles of mathematics and science whose purpose is to eliminate cryptographic security and ultimately to unlock the code and access to the original information. Rotational cryptanalysis is one of the best and most recent attacks on ARX systems. In this paper, for the first time, we apply a rotational cryptanalysis and with Given the assumption of the Markov chain for the modular additions sequence employed in two algorithms SIMD and BMW, which are second-round candidates for the SHA-3 competition that use the ARX property in their structure. That for the BMW algorithm we arrived at the complexity of 2^(180˛68) for one round of 16-rounds and the complexity of 2^(101˛88) for the entire 16-round SIMD, according to the obtained results, it can be seen that due to the large number of modular additions As a Markov chain, the BMW algorithm exhibits greater resistance to the SIMD algorithm and Against the rotational cryptanalysis is has less likely to succeed.

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

* Corresponding author E-mail: a.gaeini20@gmail.com