مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"
سال چهارم، شماره ۲، تابستان ۱۳۹۵، ص ۵۹- ۵۳

تحلیل خطی نسخه‌های مورس با تعداد دور کاهش یافته

صادق صادقی[۱]، نصور باقری*[۲]

۱- دانشجوی دکتری، دانشکده علوم ریاضی و کامپیوتر، دانشگاه خوارزمی، ۲- استادیار، دانشکده مهندسی برق، دانشگاه تربیت دبیر شهید رجایی

(دریافت: ۹۴/۱۰/۱۲، پذیرش: ۹۵/۰۵/۱۱)

چکیده

مسابقه سزار یک رقابت برای طراحی طرح‌های رمزنگاری احراز اصالت شده (AE) می‌باشد. طرح‌هایی که در این مسابقه مورد بررسی قرار می‌گیرند، طرح‌های احراز اصالت مبتنی بر داده‌های همراه (AEAD) می‌باشند. اخیرا ۳۰ کاندید از بین ۵۷ کاندید اولیه توانستند به دور دوم راه پیدا کنند. در این مقاله ما طرح مورس (MORUS) که در مسابقه سزار به دور دوم راه یافته است را مورد تحلیل خطی قرار می‌دهیم. در این تحلیل طول داده‌های همراه را برابر با صفر در نظر گرفته‌ایم (|AD|=0) و سپس با استفاده از روش برنامه‌ریزی عدد صحیح آمیخته (MILP)، توانستیم یک مشخصه خطی سه دوری برای دو نسخه از طرح MORUS یعنی MORUS-640 و MORUS-1280 به ترتیب با اریبی 2^{-31} و 2^{-32} به‌دست آوریم. کار انجام شده در این مقاله اولین تحلیل خطی‌دور کاهشی می‌باشد که تاکنون بر طرح مورس انجام شده است.

واژه‌های کلیدی: مورس، تحلیل خطی، برنامه‌ریزی عدد صحیح آمیخته

۱- مقدمه

رمز نگاری احراز اصالت[۲](AE) شامل طرح‌هایی هستند که در آن تامین دو هدف محرمانگی و احراز اصالت به صورت توأم در نظر گرفته شده است. رمزنگاری احراز اصالت شده با داده همراه[۳] (AEAD) به طرح‌های رمزنگاری احراز اصالت شده‌ای گفته می‌شود که همراه با داده‌های رمز نشده است. این داده‌های همراه از جمله می‌توانند سرآیند بسته‌های شبکه باشند تا مسیریاب‌ها بتوانند با خواندن آن‌ها پیام رمز شده را در مسیر درست هدایت کرده و به مقصد برسانند.

در سال ۲۰۱۳ رقابت برای رمزنگاری احراز اصالت با سه محور امنیت، کاربرد و قدرتمندی اعلام گردید. این رقابت با نام مسابقه سزار[۴] توسط انجمن بین‌المللی استانداردها و تکنولوژی آمریکا[۵] پشتیبانی گردید. مسابقه سزار از الگوی رقابت‌های موفق قبلی از جمله [۱] AES و [۲] SHA-3 بهره می‌برد.

هدف مسابقه سزار انتخاب الگوریتم یا الگوریتم‌هایی است که هم قابلیت اعتماد و هم جامعیت داشته باشند. این که الگوریتم‌های مرحله نهایی به صورت استاندارد درآیند امری محتمل خواهد بود.

در ۱۵ مارس ۲۰۱۴ تعداد ۵۷ کاندید به مسابقه سزار راه یافتند که از این تعداد ۳۰ طرح به دور دوم مسابقه راه یافتند. در این مقاله ما اولین تحلیل خطی دور کاهشی[۶] برای یکی از الگوریتم‌های راه‌یافته به دور دوم مسابقه سزار، طرح رمزنگاری احراز اصالت شده مبتنی بر داده‌های همراه به نام مورس[۷]، را ارائه می‌دهیم.

در ادامه ابتدا در بخش بعدی به معرفی طرح مورس می‌پردازیم. در بخش ۳ به کاربرد برنامه‌ریزی عدد صحیح آمیخته[۸] برای تحلیل دور کاهشی از طرح مورس پرداخته می‌شود. در بخش ۴، نتایج به‌دست‌آمده از اعمال MILP بر طرح مورس را بیان و در انتها در بخش ۵، نتیجه‌گیری کلی از مقاله آورده شده است.

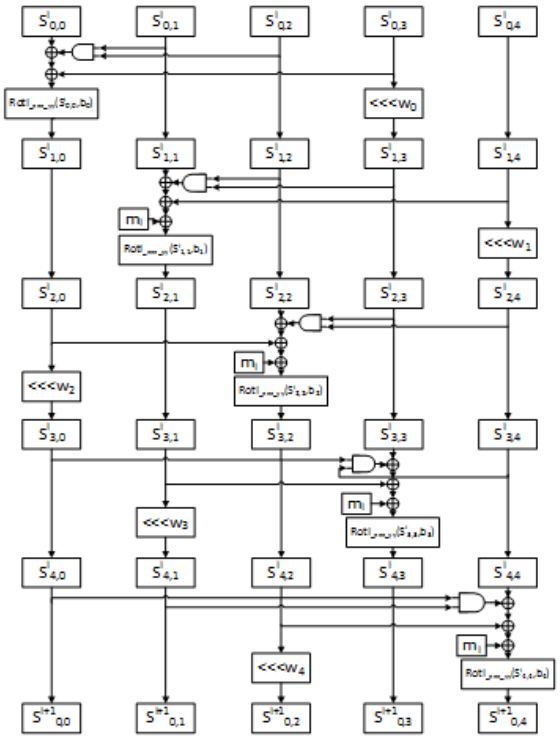
۲- معرفی طرح مورس

طرح رمزنگاری مورس یکی از کاراترین طرح‌های رمزنگاری احراز اصالت شدهٔ راه یافته به دور دوم مسابقه سزار است که در

* رایانامه نویسنده مسئول: Nbagheri@srttu.edu

۲ -Authenticated Encryption
۳ -Authenticated Encryption supporting Associated Data
۴ -CAESAR
۵ -NIST
۶ -Linear cryptanalysis Round-reduced
۷ -MORUS
۸ -Mixed Integer Linear Programming(MILP)

ساختار خود تنها از عملگرهای بیتی شیفت چرخشی به چپ[۱] (با نماد ⋘)، XOR (با نماد ⊕) و AND (با نماد ∧) استفاده می‌کند. در ساختار مورس از کلیدهای ۱۲۸ و ۲۵۶ بیتی استفاده شده است. سه نسخه از طرح مورس به نام‌های MORUS-640-128، MORUS-1280-128 و MORUS-1280-256 توسط نویسندگان پیشنهاد شده است. این نسخه‌ها از مورس ساختاری مشابه به هم دارند که تفاوت اصلی استفاده از کلیدهای ۱۲۸ و ۲۵۶ بیتی و همچنین طول کلمات حالت میانی می‌باشد. ساختار اصلی طرح مورس از یک تابع بهنگام رسان به نام $\text{stateupdate}(S^i, m_i)$ استفاده می‌کند (شکل (۱)).



شکل (۱). ساختار تابع به روزرسان استفاده شده در طرح مورس

در این تابع S^i حالت[۲] شروع گام iام و m_i پیام مربوط به بلوک iام از پیام مورد نظر را نشان می‌دهد. این تابع به روزرسان از ۵ زیردور[۳] تشکیل شده است که این زیردورها از نظر ساختاری مشابه هم هستند. حالت آغازین قبل از زیردور jام با S^i_j نشان داده می‌شود. در هر یک از این زیردورها، پنج اِلمان وجود دارد که با نماد $S^i_{j,k}$، $(0 \le k \le 4)$ نشان داده می‌شوند. از این پنج المان موجود در هر زیردور، تنها دو المان نسبت به دور بعد تغییر می‌کنند، که این تغییرات یکی توسط عملگر چرخشی شیفت به چپ (⋘) به اندازه w_i بیت، و دیگری هم توسط عملگر $\text{Rotl} - \text{xxx} - \text{yy}(x, b_i)$ با ضرایب b_i، $(i \in \{0,1,2,3,4\})$ اعمال می‌شوند، مقادیر ضرایب این دو عملگر در جدول (۱) آورده شده است. عملگر چرخشی شیفت به چپ یک رشته بیت را به عنوان ورودی دریافت می‌کند و سپس بیت‌های آن را به اندازه w_i بیت به‌صورت چرخشی به سمت چپ انتقال می‌دهد. هم‌چنین عملگر $\text{Rotl} - \text{xxx} - \text{yy}$ یک رشته بیت را به عنوان ورودی دریافت می‌کند و سپس این رشته بیت را به چهار بخش با تعداد بیت‌های مساوی تقسیم و هربخش را به اندازه b_i به سمت چپ به صورت چرخشی شیفت می‌دهد.

جدول (۱). ضرایب استفاده شده در تابع بهنگام رسانی

	MORUS-640	MORUS-1280
b_0	5	13
b_1	31	46
b_2	7	38
b_3	22	7
b_4	13	4

	MORUS-640	MORUS-1280
w_0	32	64
w_1	64	128
w_2	96	192
w_3	64	128
w_4	32	64

در ادامه ما مراحل اجرای طرح MORUS-640 را که در چهار مرحله اصلی صورت می‌پذیرد بیان می‌کنیم. این مراحل برای دیگر نسخه‌های طرح مورس نیز به‌طور مشابه انجام می‌گیرد که تفاوت در اندازه بیت‌ها و مقداردهی اولیه می‌باشد.

۱. مقداردهی اولیه[۴]:

در اولین مرحله یا همان مرحله مقداردهی اولیه المان‌های ورودی تابع $\text{stateupdate}(S^i, 0)$ به ترتیب با رشته بیت‌های تصادفی IV، کلید k و سه مقدار ثابت از پیش تعیین شده مقداردهی اولیه می‌شوند و سپس این تابع بهنگام رسان بعد از مقدار دهی اولیه، به اندازه ۱۶ دور بهنگام رسانی می‌شود. در نهایت المان دوم با کلید k، XOR می‌شود و سپس وارد مرحله دوم به صورت زیر می‌شود:

۲. پردازش داده همراه (AD):

بعد از اولین مرحله، تابع $\text{stateupdate}(S^i, AD_i^{128})$ برای هر بلاک ۱۲۸ بیتی از داده همراه AD بهنگام رسانی می‌شود. در تحلیل ما فرض بر این است که داده همراه وجود ندارد یعنی $|AD| = 0$.

۳. رمزنگاری[۵]:

بعد از مرحله دوم، متن مورد نظر در قالب‌های ۱۲۸ بیتی m_i به متن‌های رمزشده c_i تبدیل می‌شود، سپس متن m_i با بهنگام رسانی حالت برای رمزنگاری بلوک بعدی (m_{i+1}) مورد استفاده قرار می‌گیرد.

۱- Rotation to the left
۲- State
۳- Sub-Round
۴- Initialization
۵- Encryption

۴. مرحله پایانی[۱] (تولید برچسب[۲]):

در مرحله پایانی برای تولید برچسب، هشت مرتبه از تابع بهنگام رسان استفاده می‌شود. در این مرحله از طول داده همراه (adlen) و طول متن (msglen) نیز استفاده می‌شود. این مرحله از مراحل طرح نیز در تحلیل ما مورد استفاده قرار نمی‌گیرد.

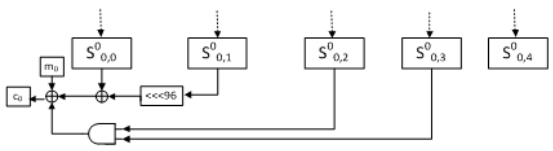
برای آشنایی با جزئیات بیشتر از طرح مورس به [۳] مراجعه شود.

همان‌طور که ذکر شد در تحلیل خطی دور کاهشی انجام شده در این مقاله از دو مرحله پردازش داده همراه و مرحله پایانی استفاده‌ای نشده است لذا از آوردن جزئیات این دو مرحله خودداری کرده‌ایم. فرض کنید $S^{-16} = (S_{0,0}^{-16}, S_{0,1}^{-16}, S_{0,2}^{-16}, S_{0,3}^{-16})$ مقدار حالت ورودی به مرحله اول باشد. هم‌چنین $S^0 = (S_{0,0}^0, S_{0,1}^0, S_{0,2}^0, S_{0,3}^0)$ حالت خروجی بعد از اجرای مرحله اول باشد. از آنجا که در این تحلیل طول داده‌های همراه را برابر صفر در نظر گرفته‌ایم، متن رمز شده c_0 از متن اصلی m_0 در پایان مرحله سوم به صورت زیر به دست می‌آید (شکل (۲)):

$$c_0 = m_0 \oplus S_{0,0}^0 \oplus (S_{0,1}^0 \lll 96) \oplus (S_{0,2}^0 \,\&\, S_{0,3}^0)$$

در این مقاله طول متن اصلی برای نسخه ۶۴۰ از طرح مورس برابر با ۱۲۸ بیت و برای نسخه ۱۲۸۰ برابر با ۲۵۶ بیت در نظر گرفته شده است.

در بخش بعدی چگونگی اعمال روش MILP را بر طرح مورس برای به دست آوردن یک مشخصه خطی بین ورودی مرحله اول و خروجی مرحله سوم شرح می‌دهیم.



شکل (۲). مرحله رمزنگاری متن اصلی بعد از مرحله اول

۳- کاربرد برنامه‌ریزی خطی عدد صحیح آمیخته در تحلیل خطی

مدل برنامه‌ریزی خطی با اعداد صحیح[۳]، مدل برنامه‌یزی ریاضی است که متغیرهای آن عدد صحیح هستند. مدلی که در آن تنها تعدادی از متغیرها اعداد صحیح باشند مدل برنامه ریزی خطی عدد صحیح آمیخته (MILP) نامیده می‌شود. شکل کلی یک مسئله MILP از نوع مینیمم با تابع هدف[۴] f به صورت زیر می‌باشد:

$$\min f = \sum_i c_i x_i$$
$$S.t \quad Ax \le b$$
$$x \ge 0$$
$$x \in \mathbb{Z}^k \times \mathbb{R}^{n-k} \subseteq \mathbb{R}^n,$$

که در آن، $(c_1, \dots, c_n) \in \mathbb{R}^n$، $A \in \mathbb{R}^{m \times n}$ و $b \in \mathbb{R}^m$ می‌باشد.

موها و همکارانش [۴]، از روش MILP برای پیدا کردن کمترین S-boxهای فعال در تحلیل تفاضلی[۵] و خطی طرح‌های رمزنگاری که مبتنی بر بایت-گرا[۶] بودند، استفاده کردند. بعد از آن نویسندگان مقاله‌های [۶-۵] با استفاده از روش MILP، شیوه‌ای را برای به‌دست آوردن مقادیر دقیق مشخصه‌های خطی در تحلیل تفاضلی و خطی با کمترین S-box های فعال ارائه نمودند.

برای اعمال روش MILP، متناظر با هر بیت از ورودی و خروجی عملگرهای استفاده شده در طرح، متغیر x_i طوری تعریف می‌شود که بازای بیت‌های فعال مقدار یک و بازای بیت‌های غیر فعال مقدار صفر را اختیار کند. همچنین برای هر S-box یک متغیر x_j تعریف می‌شود که این متغیر بر اساس این‌که خروجی S-box مربوطه فعال یا غیر فعال باشد به ترتیب مقادیر یک یا صفر را اختیار می‌کند. سپس از آنجا که جمع x_j ها تعداد S-boxهای فعال را نشان می‌دهد تابع هدف را می‌توان به صورت مینیمم جمع x_j ها در نظر گرفت، یعنی $f = \sum_j x_j$. در ادامه جزئیات بیشتر اعمال این روش بر طرح مورس را با توجه به عملگرهای استفاده شده در این طرح و هم‌چنین با توجه به مقاله‌های [۵، ۷ و ۸] شرح داده می‌شود.

۳-۱- اعمال MILP بر طرح مورس

در این مقاله ما با استفاده از روش MILP، برای دو نسخه از طرح مورس یعنی MORUS-640 و MORUS-1280 تحلیل خطی با تعداد دور کاهش یافته را انجام داده‌ایم. بدین منظور متناظر با عملگرهایی که در ساختار طرح مورس به‌کار رفته است می‌توانیم محدودیت‌هایی را به مسئله MILP به صورت زیر اضافه

۱- Finalization
۲- Tag
۳- Integer Linear Programming
۴- Objective Function
۵- Differential Cryptanalysis
۶- Byte-Oriented

نماییم.

• محدودیت‌های مربوط به عملگرهای خطی:

۱. برای عملگر XOR با ماسک‌های ورودی[۱] a و b و ماسک خروجی[۲] c، داریم:

$$a = b = c$$

۲. برای حالت سه شاخه‌ای[۳] (⊢) با ماسک ورودی a و ماسک‌های خروجی b و c داریم:

$$a + b + c \geq 2d,$$
$$d \geq a, d \geq b, d \geq c,$$
$$a + b + c \leq 2.$$

که d در اینجا، یک متغیر ساختگی دودویی[۴] می‌باشد.

۳. برای عملگر چرخشی شیفت به چپ به اندازه w بیت (⋘)، با ماسک ورودی $u = (u[1], \dots, u[n])$ و ماسک خروجی $v = (v[1], \dots, v[n])$ ، محدودیت‌های زیر را داریم:

$$u[i] = v[i + w \mod n] \quad i = 1, \dots, n.$$

• محدودیت‌های مربوط به S-box ها:

با درنظر گرفتن تنها عملگرهای غیرخطی AND موجود در ساختار مورس به عنوان S-boxهایی 1×2 و با توجه به ساختار عملگر AND، اریبی[۵] مربوط به رابطه بین ماسک‌های ورودی و ماسک خروجی، این عملگر غیرخطی را به صورتی که در جدول (۲) نشان داده شده است در نظر می‌گیریم (اریبی یک مشخصه خطی با احتمال p برابر با $p - \frac{1}{2}$ تعریف می‌شود).

جدول (۲). اریبی عملگر غیرخطی **AND** با توجه به ماسک‌های ورودی و خروجی

اریبی	0	1
00	2^{-1}	2^{-2}
01	0	2^{-2}
10	0	2^{-2}
11	0	-2^{-2}

لذا با توجه به جدول (۲) و نامگذاری ماسک‌های ورودی با $\alpha = (\alpha_1, \alpha_2)$ و ماسک خروجی با β، می‌توانیم محدودیت‌های خطی زیر را به مسئله MILP اضافه کنیم:

$$\beta[i] \geq \alpha_1[i]$$

$$\beta[i] \geq \alpha_2[i]$$

این محدودیت‌ها تضمین می‌کنند که هیچ مشخصه خطی با اریبی صفر به دست نیاید. با این تعریف از S-box، مجموع ماسک‌های خروجی فعال، تعداد S-boxهای فعال را نشان می‌دهند. هم‌چنین با توجه به ساختار مورس، S-boxهای در نظر گرفته شده مستقل از هم می‌باشند.

• ساختار تابع هدف:

از آنجا که هدف پیدا کردن یک مشخصه خطی با کمترین S-box فعال می‌باشد. بنابراین بهترین انتخاب برای تابع هدف مینیمم کردن مجموع ماسک‌های خروجی S-boxها می‌باشد، یعنی:

$$min \sum_i \beta[i]$$

با توجه به تعریف محدودیت‌ها و تعریف تابع هدف که در بالا ذکر شد می‌توانیم مسئله MILP را برای یافتن یک مشخصه خطی با تعداد دور کاهش‌یافته برای طرح مورس به کار ببریم. در بخش بعد نتایجی که با استفاده از اعمال روش MILP بر طرح مورس به‌دست آمده است را بیان می‌کنیم.

۴- نتایج اعمال MILP بر نسخه‌های مختلف مورس

ذیلا نتایج اعمال روش MILP بر دو نسخه از طرح مورس آورده شده است. در این مقاله برای حل مدل MILP از نرم افزار CPLEX استفاده شده است [۹].

۴-۱- نسخه ۶۴۰ از طرح مورس

همان‌طور که در بخش ۲ ذکر کردیم با در نظر گرفتن $S^{-16} = (S_{0,0}^{-16}, S_{0,1}^{-16}, S_{0,2}^{-16}, S_{0,3}^{-16}, S_{0,4}^{-16})$ به عنوان ورودی مرحله اول در این نسخه از مورس، هر کدام از این المان‌ها به صورت زیر مقدار دهی می‌شوند [۳]:

$$S_{0,0}^{-16} = IV, \ S_{0,1}^{-16} = k, S_{0,2}^{-16} = 1^{128},$$
$$S_{0,3}^{-16} = t_0, S_{0,4}^{-16} = t_1$$

که منظور از 1^{128} یک رشته بیت ۱۲۸ بیتی تمام یک می‌باشد. هم‌چنین مقادیر ثابت t_0 و t_1 (در مبنا ۱۶) به صورت زیر تعریف می‌شوند:

$$t_0 = 0x000101020305080d1522375990e97962$$

$$t_1 = 0xdb3d18556dc22ff12011314273b528dd$$

پس از به کاربردن روش MILP با توجه به توضیحات بخش

۱- Input Masks
۲- Output Mask
۳- Fork-branch
۴- Binary Dummy Variable
۵- Bias

۳، مشخصه خطی زیر برای ۳ دور از نسخه ۶۴۰ طرح مورس بدون در نظر گرفتن داده های همراه (AD) و تنها بر حسب کلید، مقدار تصادفی IV، متن اصلی و متن رمز شده بدست می‌آید. در جدول (۳) بیت‌های فعال برای زیر دورهای هر دور از MORUS-640 آورده شده است. در این جدول تنها بیت‌هایی که در هر یک از المان‌های $S_{i,j}^{k}$ با توجه به شکل (۱) فعال می‌باشند، آورده شده است. هم‌چنین بیت‌های مربوط به خروجی S-box های فعال با پس زمینه متفاوت مشخص شده‌اند. بنابراین با توجه به جدول (۳)، مشخصه خطی برای ۳ دور از نسخه ۶۴۰ این طرح به صورت زیر می‌باشد:

$$\begin{pmatrix} (IV)_{28,40,94,100.108} \\ \oplus(K)_{11,40,46,62.92,98,100,108} \\ \oplus(1)_{1,28,45,105.108,123} \\ \oplus(t_0)_{14,28,40,59,73,94,\ 100,106,108} \\ \oplus(t_1)_{11,27,34,41,46,48,\ 62,74,92,98,116} \end{pmatrix} = \begin{pmatrix} (m_0)_{27} \\ \oplus(c_0)_{27} \end{pmatrix} \quad (۱)$$

که در آن $(X)_{i_1,\dots,i_n} = (X)_{i_1} \oplus \dots \oplus (X)_{i_n}$. حال با توجه مشخصه خطی بالا و ثابت بودن $\text{const } t_0$ و $\text{const } t_1$ داریم:

$$\begin{pmatrix} \oplus(1)_{1,28,45,105.108,123} \\ \oplus(t_0)_{14,28,40,59,73,94,100,106,108} \\ \oplus(t_1)_{11,27,34,41,46,48,62,74,92,98,116} \end{pmatrix} = 0$$

لذا رابطه (۱) را می توانیم به صورت زیر بازنویسی کنیم:

$$\begin{pmatrix} (IV)_{28,40,94,100.108} \\ \oplus(K)_{11,40,46,62.92,98,100,108} \end{pmatrix} = \begin{pmatrix} (m_0)_{27} \\ \oplus(c_0)_{27} \end{pmatrix} \quad (۲)$$

با توجه به جدول(۲)، اریبی هر S-box فعال برابر با $\frac{1}{4}$ می‌باشد. بنابراین طبق لم piling-up [10]، اریبی مشخصه خطی رابطه (۲) برای N، S-box فعال برابر است با

$$2^{N-1} \times \left(\frac{1}{4}\right)^{N} = 2^{-(N+1)}$$

حال با توجه به جدول (۳)، تعداد ۳۰، S-box فعال داریم که بنا به لم piling-up اریبی این رابطه خطی برابر است با 2^{-31}.

در ادامه ما نسخه دیگر از طرح مورس یعنی نسخه ۱۲۸۰ از این طرح را مورد تحلیل قرار می‌دهیم.

۴-۲- نسخه ۱۲۸۰ از طرح مورس

در این نسخه از مورس با توجه به اینکه هریک از المان‌های ورودی ۲۵۶ بیتی می‌باشند، ورودی‌های مرحله اول به صورت زیر مقداردهی می‌شوند [۳]:

$$S_{0,0}^{-16} = IV, S_{0,1}^{-16} = k, S_{0,2}^{-16} = 1^{256}, S_{0,3}^{-16} = 0^{256}, S_{0,4}^{-16} = const\ t$$

که منظور از 0^{256}، یک رشته بیت ۲۵۶ بیتی تمام صفر می‌باشد. هم‌چنین مقدار ثابت const t از الحاق دو مقدار ثابت t_0 و t_1 به‌وجود می‌آید. با توجه به این ورودی‌ها و جدول ۴، مشخصه خطی زیر برای سه دور از نسخه ۱۲۸۰ این طرح به صورت زیر به دست می‌آید:

$$\begin{pmatrix} (IV)_{52,77,83,125.155,223} \\ \oplus(K)_{61,183,204,214.220} \\ \oplus(1)_{74,90,96,168} \\ \oplus(0)_{14,28,40,59,73,94,100,106,108} \\ \oplus(const\ t)_{61,183,192,198,204,214,220,240} \end{pmatrix} = \begin{pmatrix} (m_0)_6 \\ \oplus(c_0)_6 \end{pmatrix} \quad (۳)$$

با توجه به ثابت بودن const t داریم:

$$\begin{pmatrix} \oplus(1)_{74,90,96,168} \\ \oplus(0)_{14,28,40,59,73,94,100,106,108} \\ \oplus(const\ t)_{61,183,192,198,204,214,220,240} \end{pmatrix} = 1$$

لذا رابطه (۳) را می‌توانیم به صورت زیر بازنویسی کنیم:

$$\begin{pmatrix} (IV)_{52,77,83,125.155,223} \\ \oplus(K)_{61,183,204,214.220} \oplus 1 \end{pmatrix} = \begin{pmatrix} (m_0)_{27} \\ \oplus(c_0)_{27} \end{pmatrix}$$

حال با توجه جدول (۴) تعداد ۳۱، S-box فعال داریم لذا بنا به لم piling-up اریبی این رابطه خطی برابر است با 2^{-32}.

جدول (۳). ماسک‌های ورودی هریک از المان‌های MORUS-640

Rounds		$S_{i,0}$	$S_{i,1}$	$S_{i,2}$	$S_{i,3}$	$S_{i,4}$
1	0	28,40,94,100,108	11,40,46,62,92,98,100,108	1,28,45,105,108,123	14,28,40,59,73,94,100,106,108	11,27,34,41,46,48,62,74,92,98,116
	1	1,45,67,105,113	11,46,62,92,98	1,45,105,123	10,46,91,105	11,27,34,41,46,48,62,74,92,98,116
	2	1,45,67,105,113	10,45,61,91,97	1,45,105,123	10,91,105	10,52,91,98,105,112
	3	35,81,95	10,45,61,91,97	8,52,98,112	10,45,91	10,52,91,98,112
	4	35,81	33,125	8,52,98,112	0,35,81	52,98,112
	5	35,81	33,125	40	0,35,81	33,111,125
2	0	35,81	33,125	40	0,35,81	33,111,125
	1	40,86	33,125	40	32	33,111,125
	2	40,86	32,124	40	32	47
	3	54	32,124	47	32	47
	4	52	60	47	54	47
	5	54	60	--	54	60
3	0	54	60	--	54	60
	1	59	60	--	--	60
	2	59	59	--	--	--
	3	27	59	--	--	--
	4	27	123	--	--	--
	5	27	123	--	--	--

جدول (۴). ماسک‌های ورودی هریک از المان‌های MORUS-1280

Rounds		$S_{i,0}$	$S_{i,1}$	$S_{i,2}$	$S_{i,3}$	$S_{i,4}$
1	0	52,77,83,125,155,223	61,183,204,214,220	74,90,96,168	52,77,83,101,125,155,186,223,235	61,183,192,198,204,214,220,240
	1	1,74,90,96,168,236	61,183,204,214,220	74,90,96,168	43,165,250	61,183,192,198,204,214,220,240
	2	1,74,90,96,168,236	43,165,196,202,250	74,90,96,168	43,165,250	64,70,112
	3	127,193	43,165,196,202,250	64,70,112,142	43,165,250	64,70,112
	4	127,193	68,74	64,70,112,142	50,172,193	64,70,112
	5	127,193	68,74	206	50,172,193	48,74,116
2	0	127,193	68,74	206	50,172,193	48,74,116
	1	185,206	68,74	206	114	68,74,116
	2	185,206	114,120	206	114	68,74,116
	3	121	114,120	244	114	244
	4	121	248	244	121	244
	5	121	248	--	121	248
3	0	121	248	--	121	248
	1	70	248	--	--	248
	2	70	230	--	--	--
	3	6	230	--	--	--
	4	6	102	--	--	--
	5	6	102	--	--	--

می‌شود.

۵- نتیجه‌گیری

در این مقاله، اولین تحلیل خطی با تعداد دور کاهش یافته از طرح رمزنگاری احراز هویت مورس مورد تحلیل قرار گرفت. لذا بدون در نظر گرفتن مرحله دوم و سوم از مراحل الگوریتم و استفاده از روش برنامه‌ریزی عدد صحیح آمیخته یک مشخصه خطی سه‌دوری برای MORUS-640 و MORUS-1280 به ترتیب با اریبی 2^{-31} و 2^{-32} با کمترین تعداد S-boxهای فعال ممکن به‌دست آمد.

۶- سپاسگزاری

در تهیه این مقاله، مرکز تحقیقات پردازش‌های فوق سریع و سیستم ابررایانه ملی امیرکبیر و هم‌چنین سیستم محاسباتی دانشگاه تربیت دبیر شهید رجایی برای حل مسائل MILP مورد استفاده قرار گرفته است که از زحمات مسئولان آنان سپاسگزاری

۷- مراجع

[1] National Institute of Standards and Technology, "Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard (AES)," Federal Register. vol. 62, Sep. 1997.

[2] Kayser and F. Richard, "Announcing request for candidate algorithm nominations for a new cryptographic hash algorithm (SHA-3) family," Federal Register, vol. 72, p. 63, 2007.

[3] H. Wu and T. Huang, "The Authenticated Cipher Morus (v1)," 2015. Available: http://www.competitions.cr.yp.to/round2/morusv11.pdf,

[4] N. Mouha, Q. Wang, D. Gu, and B. Preneel, "Differential and Linear Cryptanalysis Using Mixed-Integer Linear Programming," Information Security and Cryptology, pp. 55–76, 2011.

[5] S. Sun, L. Hu, M. Wang, P. Wang, K. Qiao, X. Ma, D. Shi, L. Song, and K. Fu, "Towards finding the best characteristics of some bit-oriented block ciphers and automatic enumeration of (related-key) differential and linear characteristics with predefined properties,"

Cryptology ePrint Archive, Report 2014/747, 2014. Available: http://eprint. iacr.org/2014/747.

[6] S. Sun, L.Hu, P. Wang, K. Qiao, X. Ma, and L. Song, "Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES (L) and other bit-oriented block ciphers," In Advances in Cryptology–Asiacrypt, Springer Berlin Heidelberg, pp. 158-178, 2014.

[7] D. Shi, L. Hu, S. Sun, L. Song, K. Qiao, and X. Ma, "Improved Linear (hull) Cryptanalysis of Round-reduced Versions of SIMON," IACR Cryptology ePrint Archive, Report 2015/964, 2014. Available: http://eprint.iacr.org/2014/973.

[8] D. Shi, L. Hu, S. Sun, L. Song, "Improved Linear (hull) Cryptanalysis of Round-reduced Versions of KATAN," IACR Cryptology e-Print Archive, Report 2015/964, 2015, Available: http://eprint.iacr.org/2015/964.

[9] ILOG, IBM, "CPLEX optimizer," 2012. Available:http://www-01.ibm. Com/software/commerce/optimization/cplex-optimizer.

M. Matsui, "Linear cryptanalysis method for DES cipher," In Advances in Cryptology, Springer Berlin Heidelberg, pp. 386-397, 1993.

Journal Of Electronical & Cyber Defence
Vol. 4, No. 2, 2016, Serial No.14

Linear Cryptanalysis of Reduced-round Versions of MORUS

S. Sadeghi, N. Bagheri*

*Shahid Rajaee Teacher Training University

(Received: 02/01/2016, Accepted: 01/08/2016)

ABSTRACT

CAESAR is a competition for designing authenticated encryption schemes (AE). The schemes that are considered in this competition are supported associated data (AEAD). 57 candidates have been submitted to this competition, out of them 30 candidates later announced as the second round candidates.

In this paper, we analysis the security of MORUS, a second round candidate of CAESAR, against mixed integer linear programing based linear cryptanalysis. In this study, the length of associated data is considered as zero (AD|=0|) and linear characteristics for two version of MORUS, MORUS-640 and MORUS-1280, reduced to 3 rounds with bias 2^{-31} *and* 2^{-32} *respectively are presented. The result of this paper is the first third party linear analysis on round reduced of MORUS, to the best of our knowledge.*

Keywords: MORUS, Linear cryptanalysis, Mixed Integer Linear Programming

* Corresponding Author Email: Nbagheri@srttu.edu