مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"
سال پنجم، شماره ۱، بهار ۱۳۹۶، ص ۸-۱

حمله تفاضلی با دور کاهش یافته بر روی رمزهای قالبی SIMON32 و SIMON48 و SIMON64

احمد اسکوئیان [۱]، نصور باقری [۲*]

۱- کارشناسی ارشد مخابرات، دانشگاه تربیت دبیر شهید رجایی
۲- استادیار، دانشکده مهندسی برق، دانشگاه تربیت دبیر شهید رجایی
(دریافت: ۹۴/۰۳/۰۹، پذیرش: ۹۵/۰۸/۱۰)

چکیده

در ژوئن سال ۲۰۱۳ خانواده‌ای از رمزهای قالبی با نام SIMON توسط بیولیو و همکارانش از آژانس امنیت ملی آمریکا معرفی شد. این خانواده از رمزهای قالبی جزء رمزهای قالبی سبک‌وزن دسته‌بندی می‌شوند و می‌توانند طول کلید و طول قالب متفاوتی را بپذیرند. SIMON در مقایسه با بسیاری از رمزهای قالبی سبک‌وزن دیگر، عملکرد بهتری در سخت‌افزار و نرم‌افزار دارد این برتری درزمینه سخت‌افزاری محسوس‌تر است. هدف اصلی این مقاله، بهبود حملات تفاضلی ارائه‌شده بر روی این خانواده از رمزهای قالبی است. با کمک گرفتن از ایده‌ها و دیدگاه‌های جدید مطرح‌شده در مورد روش‌ها و سیاست‌های حدس کلید، توانستیم حمله تفاضلی بهبودیافته‌ای را بر روی ۲۲ دور ۳۲/۶۴ SIMON، ۲۳ دور SIMON ۴۸/۹۶ و ۲۹ دور SIMON ۶۴/۱۲۸ به انجام برسانیم. این حمله به تعداد دورهای حمله تفاضلی ارائه‌شده تا زمان ارسال این مقاله یک دور اضافه می‌کند.

واژه‌های کلیدی: SIMON، حمله تفاضلی، رمزهای قالبی سبک وزن.

۱- مقدمه

در تعریف امنیت اطلاعات، می‌توان محرمانگی[۱]، جامعیت[۲] و دسترس‌پذیری[۳] را به‌عنوان سه اصل مهم آن بیان و علم رمزنگاری را به‌عنوان مهم‌ترین ابزار برای برآوردن اصل‌های امنیتی، محرمانگی و جامعیت تعریف کرد. الگوریتم‌های رمزنگاری با هدف اصلی تأمین محرمانگی اطلاعات طراحی می‌شوند. برای این کار در این الگوریتم‌ها از مؤلفه‌ای به نام کلید استفاده می‌شود. فرستنده با استفاده از یک الگوریتم رمزنگاری و کلید رمزگذاری، اطلاعات را رمز می‌کند و گیرنده نیز با استفاده از همان الگوریتم رمزنگاری و کلید رمزگشایی، اطلاعات رمزی را رمزگشایی می‌کند. بسته به این‌که کلید رمزگذاری و رمزگشایی یکسان باشند یا باهم متفاوت باشند، الگوریتم‌های رمزنگاری را به دو دسته متقارن و نامتقارن تقسیم می‌کنند. الگوریتم‌های رمزنگاری متقارن در دو دسته کلی رمزهای قالبی و رمزهای دنباله‌ای تقسیم‌بندی می‌شوند.

در طول دهه گذشته شاهد استقبال روزافزون جامعه رمزنگاری از رمزهای قالبی و جایگزینی بیشتر رمزهای دنباله‌ای با رمزهای قالبی در پروتکل‌های رمزنگاری بوده‌ایم. به‌عنوان مثال در نسل جدید تلفن همراه، رمزهای دنباله‌ای A5/2 و A5/1 [۱] با الگوریتم رمز قالبی کاسومی[۴] [۲] جایگزین شده است. امر مسلم، این است که امروزه رمزهای قالبی جای خود را به‌صورت گسترده بازکرده‌اند و اکثر پروتکل‌های رمزنگاری از رمزهای قالبی استفاده می‌کنند.

تعریف یک رمز قالبی [۳]: یک رمز قالبی تابعی است به شکل $E:\{0,1\}^K\times\{0,1\}^N\to\{0,1\}^N$ که یک ورودی K بیتی را به‌عنوان کلید (k) و یک ورودی N بیتی دیگر را به‌عنوان متن آشکار (P) می‌گیرد و در مقابل متن رمز C=E(k,P) را برمی‌گرداند. برای هر رمز قالبی و هر کلید k، تابع E_k یک جایگشت روی $\{0,1\}^N$، یعنی تابعی یک به یک از $\{0,1\}^N$ به $\{0,1\}^N$ است و بنابراین، دارای یک معکوس، مثل E_k^{-1} است. هم تابع رمز و هم معکوس آن باید به‌سادگی قابل‌محاسبه باشند؛ به این معنا که با داشتن P و k بتوان C=E(k,P) را محاسبه کرد و همچنین با داشتن C و k بتوان $P=E_k^{-1}(k,C)$ را به دست آورد.

* رایانامه نویسنده مسئول: Nbagheri@srttu.edu

1- Confidentiality
2- Integrity
3- Availability
4- Kasumi

از مهم‌ترین مسائلی که در هر طرح و الگوریتم رمزنگاری، ازجمله رمزهای قالبی باید در نظر گرفته شود، امنیت و کارآیی آن‌ها است. امنیت یک رمز قالبی در مدل‌های مختلفی قابل بحث است؛ اما مهم‌ترین مدل امنیتی که در این مورد در نظر گرفته می‌شود، مدل امنیت محاسباتی است. به‌صورت غیررسمی گفته می‌شود که یک رمز قالبی در مدل امنیت محاسباتی، امن است اگر این رمز در برابر تمام انواع حملات شناخته‌شده روی رمزهای قالبی مقاوم باشد. منظور از کار آیی یک طرح و الگوریتم رمزنگاری، مانند رمزهای قالبی، سرعت و الزامات حافظه برای پیاده‌سازی آن است. با توجه به این امر، رمزهای قالبی را می‌توان در دو دسته کلی رمزهای قالبی معمولی و رمزهای قالبی سبک‌وزن در نظر گرفت. رمزهای قالبی سبک‌وزن در مقایسه با رمزهای قالبی معمولی، حافظه کمتری برای پیاده‌سازی لازم دارند. با توجه به اهمیت فضای حافظه، در سال‌های اخیر توجه زیادی به رمزهای قالبی سبک‌وزن شده است؛ به‌طوری‌که می‌توان از CLEIFA [۴]، HIGHT [۵]، LED [۶]،TWINE [۷]، PICCOLO [۸] و PRESENT [۹] به‌عنوان چند نمونه از رمزهای قالبی سبک‌وزن جدید نام برد.

در سال ۲۰۱۳، آژانس امنیت ملی آمریکا خصوصیات خانواده رمزهای قالبی سبک‌وزن SIMON را منتشر کرد. در مقایسه با دیگر رمزهای قالبی سبک‌وزن موجود، این خانواده عملکرد مناسبی را برای ابزار منبع محدود مانند برچسب‌های RFID دارد به‌گونه‌ای که می‌تواند به‌صورت گسترده‌ای در این ابزار به کار گرفته شود.

حمله تفاضلی [۱۰] ابتدا توسط بیهام[1] و همکاران به‌عنوان یک حمله محبوب بر روی رمزهای قالبی معرفی شد. در خلال سال‌ها، حمله تفاضلی برای تحلیل بسیاری از انواع مختلف رمزهای قالبی گسترش‌یافته است. حمله تفاضلی مراتب بالاتر توسط Lai در ۱۹۹۴ معرفی شد. در همان سال، نودسن[2] تفاضل ناقص را معرفی کرد [۱۱] که برای تحلیل رمز قالبی DES بکار گرفته شد. در ۱۹۹۸، نودسن [۱۲] و بیهام و همکاران [۱۳] مستقلاً، ایده حمله تفاضلی غیرممکن را منتشر کردند که به حمله‌کننده اجازه جداسازی کلیدهای اشتباه توسط تمیز دادن مشخصه‌های تفاضلی غیرممکن می‌دهد. برای ساخت یک تمیز دهنده طولانی توسط اتصال دو مشخصه تفاضلی کوتاه، وگنر[3] حمله بومرنگ[4] را در ۱۹۹۹ [۱۴] معرفی کرد که توسط کلسی[5] و همکاران به‌عنوان حمله بومرنگ تقویت‌شده بهبودیافته [۱۵] و به‌صورت جداگانه توسط بیهام و همکاران به‌عنوان حمله مستطیلی معرفی شد [۱۶].

در این مقاله تنها بر روی حمله تفاضلی بر روی SIMON۳۲، SIMON۴۸ و SIMON۶۴ تمرکز شده است. خانواده SIMON شامل ۱۰ رمز است که هرکدام از آن‌ها با توجه به اندازه حالت (اندازه قالب) N و طول کلید K به‌صورت SIMON N/K نامیده می‌شوند. تنها یک نمونه برای اندازه حالت ۳۲ بیت وجود دارد، یعنی SIMON۳۲/۶۴ و دو نمونه برای اندازه نمونه‌های ۴۸ و ۶۴ و ۹۶ و سه نمونه برای اندازه حالت ۶۴ بیتی وجود دارد.

ارائه این خانواده، خیلی زود توجهات تعداد زیادی از تحلیل گران رمز را برانگیخت. الخزیمی[6] و لاریدسن[7] [۱۷] حمله تفاضلی را روی ۵ نوع مختلف SIMON با ۱۶ و ۱۸، ۲۴، ۲۹ و ۴۰ دور که به ترتیب متناظر با ۵ اندازه قالب مختلف این رمز می‌باشند را ارائه داده‌اند. آن‌ها همچنین حملات تفاضلی غیرممکن را روی ۱۴، ۱۵، ۱۶، ۱۹ و ۲۲ دور انواع مختلف این رمز ارائه داده‌اند. بیریوکوف[8] و ولیچکوف[9] [۱۸] مشخصه‌های تفاضلی را تا ۱۳، ۱۵ و ۲۱ دور برای SIMON بهبود دادند که می‌توان از آن‌ها به ترتیب برای حمله بر روی کلیدهای ۳۲، ۴۸ و ۶۴ بیتی از این رمز استفاده کرد. به‌طور مثال می‌توان به ۱۹ دور برای SIMON۳۲/۶۴ و ۲۰ دور برای SIMON۴۸/۷۲ و ۲۰ دور برای SIMON۴۸/۹۶ و ۲۶ دور SIMON۶۴/۱۲۸ به ترتیب توسط $2^{۳۳}$، $2^{۵۲}$، $2^{۸۹}$ و $2^{۱۲۱}$ بار رمز کردن حمله کرد. علاوه بر این عابد[10] و لیست[11] [۱۹] حمله تفاضلی را تا ۱۸، ۱۰، ۲۶، ۳۵ و ۴۶ دور به ترتیب برای ۵ نوع مختلف SIMON ارائه دادند.

در اینجا ما به دنبال بعضی از مهم‌ترین رفتارهای بیتی انواع مختلف تفاضلات موجود برای SIMON بوده‌ایم و تعداد زیادی شرایط در دسترس را برای بیت‌ها در جهت توسعه مسیرهای تفاضلی با ۴ یا ۵ دور در بالای آن (به‌طور مثال بالای ۱۳ دور تفاضلی برای SIMON ۳۲) به‌دست آوردند. به‌طور خاص، بعضی از شرایط بیتی که در آن‌ها بیت‌های کلید مخفی مستقل هستند، انگیزه ما را برای به‌وجود آوردن راهبرد جدیدی برای جستجوهای لازم در جهت حدس بیت کلید افزایش داد. بر پایه این شرایط بیتی و شرایط حدس بیت‌های کلید، حمله تفاضلی کاهش‌یافته بر روی انواع SIMON را با اندازه قالب ۳۲، ۴۸ و ۶۴ انجام دادیم.

1- Biham
2- Knudsen
3- Wagner
4- Boomerang
5- Kelsey
6- Alkhzaimi
7- Lauridsen
8- Biryukov
9- Velichkov
10- Abed
11- list

جدول ۱. نتایج به‌دست‌آمده و مقایسه با بهترین نتایج

SIMON		تفاضلی				تفاضلی غیرممکن		همبستگی صفر	انتگرالی	خطی			پوشش خطی	
		[۲۲]	[۱۸]	[۲۰]	بخش ۳	[۱۹]	[۲۳]	[۲۳]	[۲۳]	[۱۹]	[۲۴]	[۲۵]	[۲۶]	[۲۴]
۳۲/۶۴	تعداد دور	۱۸	۱۹	۲۱	۲۲	۱۳	۱۸	۲۰	۲۱	۱۱	۱۳	۱۸	۲۱	۲۲
	پیچیدگی زمانی	2^{46}	2^{32}	2^{46}	$2^{58/69}$	$2^{50/1}$	$2^{61/14}$	$2^{56/96}$	2^{63}			$2^{61/5}$		$2^{58/06}$
	پیچیدگی داده	$2^{31/2}$	2^{31}	2^{31}	$2^{29/69}$	2^{30}	2^{32}	2^{32}	2^{31}	2^{23}	2^{32}	2^{32}	$2^{30/19}$	$2^{30/56}$
۴۸/۹۶	تعداد دور	۱۹	۲۰	۲۲	۲۳	۱۵	۱۹	۲۱		۱۴	۱۶	۲۱	۲۱	۲۲
	پیچیدگی زمانی	2^{76}	2^{75}	2^{71}	$2^{84/05}$	2^{53}	$2^{85/82}$	$2^{72/63}$				2^{90}		$2^{92/61}$
	پیچیدگی داده	2^{46}	2^{46}	2^{45}	$2^{43/05}$	2^{38}	2^{48}	2^{48}		2^{47}	2^{46}	2^{46}	$2^{42/28}$	$2^{44/11}$
۶۴/۱۲۸	تعداد دور	۲۶	۲۶	۲۸	۲۹	۱۷				۱۶	۱۹	۲۴	۲۹	۲۹
	پیچیدگی زمانی	2^{94}	2^{121}	2^{60}	$2^{110/53}$	2^{71}						$2^{116/5}$		$2^{110/53}$
	پیچیدگی داده	2^{63}	2^{63}	2^{59}	$2^{60/53}$	2^{52}				2^{61}	2^{58}	2^{58}	$2^{61/1}$	$2^{62/53}$

این حمله بر روی این دو نوع SIMON با یک یا دو دور بیشتر، بهتر از حملاتی است که تابه‌حال ارائه شده است. به‌واسطه بخش اصلی این حمله، آشکار می‌شود که چگونه توابع بیتی وابسته به بیت‌های کلید کنترل می‌شوند، این حمله را حمله تفاضل بیتی می‌نامند.

درنتیجه، حمله تفاضلی به‌صورت ۲۲ دور بر روی SIMON۳۲/۶۴ با احتمال موفقیت ۰/۴۳۶۷ و ۲۳ دور بر روی SIMON۴۸/۹۶ با احتمال موفقیت ۰/۷۲۶ و ۲۹ دور بر روی SIMON۶۴/۱۲۸ با احتمال موفقیت ۰/۶۲۸ به‌دست‌آمده است.

در بخش دوم این مقاله توصیف مختصری از SIMON ارائه می‌شود سپس در بخش سوم حمله تفاضلی بهبودیافته‌ای بر روی این رمز ارائه می‌شود و در بخش چهارم نتیجه‌گیری مختصری ارائه می‌گردد.

۲- توصیف مختصری از SIMON

۲-۱- نوشتار

نوشتار زیر در این مقاله استفاده‌شده است:

X_r: ورودی دور r-ام

L_{r-1}: نیمه چپ ورودی دور r-ام

R_{r-1}: نیمه راست ورودی دور r-ام

K_r: زیر کلید استفاده‌شده در دور r-ام

X[i]: i امین بیت X، اندیس بیت‌ها از چپ به راست است

X<<<r: چرخش چپ بیت‌های X با اندازه r موقعیت

X>>>r: چرخش راست بیت‌های X با اندازه r موقعیت

$\oplus$: XOR

$\cap$: AND

ΔX: تفاضل XOR از X و X´

+: اضافه

۲-۲- خلاصه توصیفی از رمزهای قالبی SIMON

رمز قالبی SIMON یک ساختار فیستلی است با ورودی N بیتی و با کلید K بیتی به‌صورت SIMON N/K نامیده می‌شود که N=2n و K=mn و n در اینجا برابر با ۱۶، ۲۴، ۳۲، ۴۸ یا ۶۴ بیت و m=2,3,4 است پس می‌توان نتیجه گرفت که N=2K/m است. این خانواده شامل ۱۰ رمز قالبی با تعداد متفاوت دور n_r وجود دارد. تعداد دورها و خصوصیات ۱۰ نوع SIMON در [۲۱] نشان داده‌شده است. تمام انواع SIMON از توابع دوری مشابهی استفاده می‌کنند.

تابع دور: برای عملکرد بهتر روی زمینه‌های سخت‌افزاری و نرم‌افزاری، SIMON از تابع دور بسیار ساده‌ای استفاده می‌کند که در تعداد دور زیادی تکرار می‌شوند. تابع $F(X)=(X<<<8) \cap (X<<<1) \oplus (X<<<2)$ یک انتقال غیرخطی از $\{0,1\}^n$ به $\{0,1\}^n$ است که توسط ۳ عملگر بیتی $\cap$ و $\oplus$ و <<< انجام می‌پذیرد. متن اصلی به‌صورت $P=(L_0,R_0)$ است و تابع دور i ام به‌صورت زیر توصیف می‌گردد:

$$L_i = R_{i-1} \oplus F(L_{i-1}) \oplus K_{i-1} \quad (1)$$

$$R_i = L_{i-1} \quad (2)$$

جایی که $i=1,\ldots,n_r$ است. متن رمزی C به‌صورت (R_{nr}, L_{nr}) انتخاب می‌شود. در اینجا، برای راحتی توصیف حمله تفاضلی بیتی، توصیفی برای تابع دور بیتی داده‌شده است. بدین‌صورت که:

$L_i = \{X_i[n], X_i[n-1],..., X_i[2n-1]\}$,
$R_i = \{X_i[0], X_i[1],..., X_i[n-1]\}$

و سپس تابع دور i–ام به‌صورت زیر نشان داده می‌شود:

$$X_i[q+n] \oplus X_{i-1}[(q+2)\%n+n] \oplus X_{i-1}[q] \oplus K_{i-1}[q], \\ = X_{i-1}[(q+1)\%n+n] \cap X_{i-1}[(q+8)\%n+n]) \\ X_i[q] = X_{i-1}[q+n]$$

جایی که q=0,1,…,n-1 و $X_i[n]$ پرارزش‌ترین پست L_i و $X_i[2n-1]$ کم‌ارزش‌ترین بیت L_i است و $X_i[0]$ پرارزش‌ترین بیت R_i و $X_i[n-1]$ کم‌ارزش‌ترین بیت R_i است.

هر یک رشته از n_r زیر کلید دوری $\{K_0,\ldots..K_{nr-1}\}$ را از کلید اصلی $\{K_0\ldots K_{m-1}\}$ با طول‌های کلید متفاوت mn، توسط تابع کلید به‌صورت زیر استخراج می‌کنند. وقتی‌که i=1,…,m-1 باشد داریم $K_i=k_i$ و وقتی‌که i=m,m+1,…,nr باشد از توابعی استفاده می‌شود که با تغییر مقدار m این توابع نیز تغییر می‌کند.

برای جزئیات بیشتر بهتر است به [۲۱] مراجعه شود. درواقع، برنامه کلید خطی است، کلید اصلی می‌تواند از هر mn بیت زیر کلید مستقل استنباط گردد.

اصول کار این رمز را می‌توان بر پایه معادلات زیر نشان داد که این معادلات خود با استفاده از خصوصیات عملگر AND و XOR به‌دست‌آمده‌اند:

$$\Delta X_{i+1}[q+n] = \\ (\Delta X_i[(q+1)\%n+n] \cap X_i[(q+8)\%n+n]) \oplus \\ X_i[(q+1)\%n+n] \cap \Delta X_i[(q+8)\%n+n) \oplus \\ (\Delta X_i[(q+1)\%n+n] \cap \Delta X_i[(q+8)\%n+n] \oplus) \\ \Delta X_i[(q+2)\%n+n] \oplus \Delta X_i[q], \quad (۳)$$

$$X_i[(q+1)\%n+n] = (X_{i-1}[(q+2)\%n+n] \cap \oplus \\ X_{i-1}[(q+9)\%n+n]) \\ X_{i-1}[(q+3)\%n+n] \oplus X_{i-1}[(q+1)\%n] \oplus \\ K_{i-1}[(q+1)\%n]) \quad (۴)$$

$$X_i[(q+8)\%n+n] = (X_{i-1}[(q+9)\%n+n] \cap \\ X_{i-1}[(q+16)\%n+n]) \oplus X_{i-1}[(q+10)\%n+n] \oplus \\ X_{i-1}[(q+8)\%n] \oplus K_{i-1}[(q+8)\%n] \quad (۵)$$

با توجه به معادلات بالا می‌توان استنباط کرد که اگر:

$$\Delta X_i[(q+1)\%n+n] \cap \Delta X_i[(q+8)\%n+n]=(0,0)$$

درنتیجه هیچ بیت کلیدی نیاز به حدس زدن ندارد که این موضوع می‌تواند به کاهش پیچیدگی زمانی کمک کند. ولی اگر به‌صورت (0,1) و (1,0) و (1,1) باشد باید کلیدهای موردنیاز حدس زده شود. ازآنجاکه زیر کلید K_i با ورودی X_i به‌صورت خطی است، واضح است که ΔX_i از K_i مستقل خواهد بود.

۳- حمله تفاضلی روی SIMON

در نگاه اول با توجه به اصول تابع دور این رمز، به نظر می‌رسد که حمله تفاضلی می‌تواند حمله‌ای مؤثر بر روی این رمز باشد که این استدلالی درست است در ادامه بحث بیشتر به این حمله می‌پردازیم و چرایی آن را بررسی می‌کنیم و در ابتدا به توصیف حمله تفاضلی بیتی روی SIMON۳۲/۶۴ با دور کاهش‌یافته می‌پردازیم و در پیوست ۱ و ۲ بیت‌های زیر کلیدهای درگیر در حمله بر روی SIMON۴۸ و SIMON۶۴ را مشخص نمودیم تا روند حمله بر روی این دو الگوریتم نیز مشخص گردد.

۳-۱- حمله تفاضلی روی SIMON۳۲

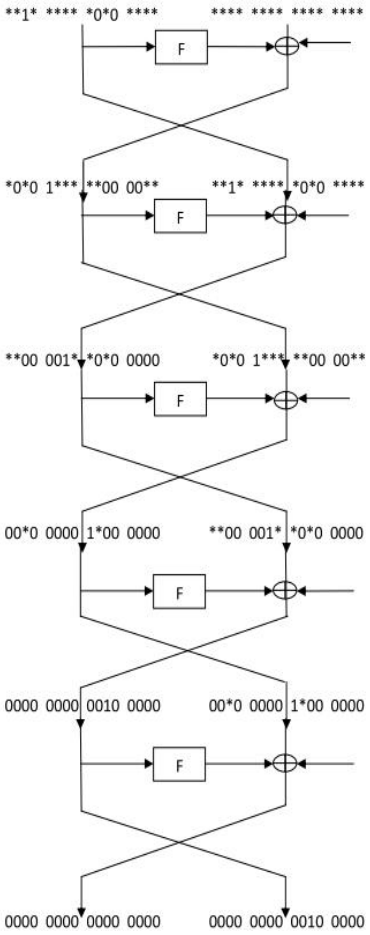
در اینجا از مسیر تفاضلی ۱۳ دوری [۱۸] برای حمله بر روی ۲۲ دور SIMON۳۲ استفاده‌شده که با افزودن ۵ دور در بالای این تفاضل و ۴ دور به انتهای آن، تعداد دورها به ۲۲ دور رسیده است. برای سادگی در ادامه بحث، $C=\{L_{nr}, R_{nr}\}$ جایگزین $C=\{L_{nr}, L_{nr}\}$ می‌گردد.

۳-۲- شرایط حمله تفاضلی

برای این حمله، تفاضل شیفت یافته ۱۳ دوری زیر را که در [۱۸] با احتمال $2^{-29/64}$ به‌دست آمده است را در نظر می‌گیریم:

D_1: (0000, 0020) → (2000, 0000)

افزودن ۵ دور به بالای تفاضل موردنظر به‌صورت شکل (۱) به دست می‌آید.



شکل (۱). نحوه محاسبه ورودی بعد از افزودن ۵ دور به ابتدای مشخصه

که در آن، از تفاضل به‌دست‌آمده شروع می‌کنیم سپس سمت راست تفاضل را طبق تابع F مربوط به SIMON یک و دو و هشت بیت شیفت می‌دهیم و در تابع F قرار می‌دهیم هرکجا که AND

بیتی بین عدد صفر و یک باشد آن بیت در خروجی به شکل ستاره نشان داده می‌شود. این روند برای ۴ دور خروجی نیز ثابت است. در اینجا تفاضل ورودی را با این روش به دست آوردیم که در آن:

ΔP_1: (**1* **** *0*0 ****,

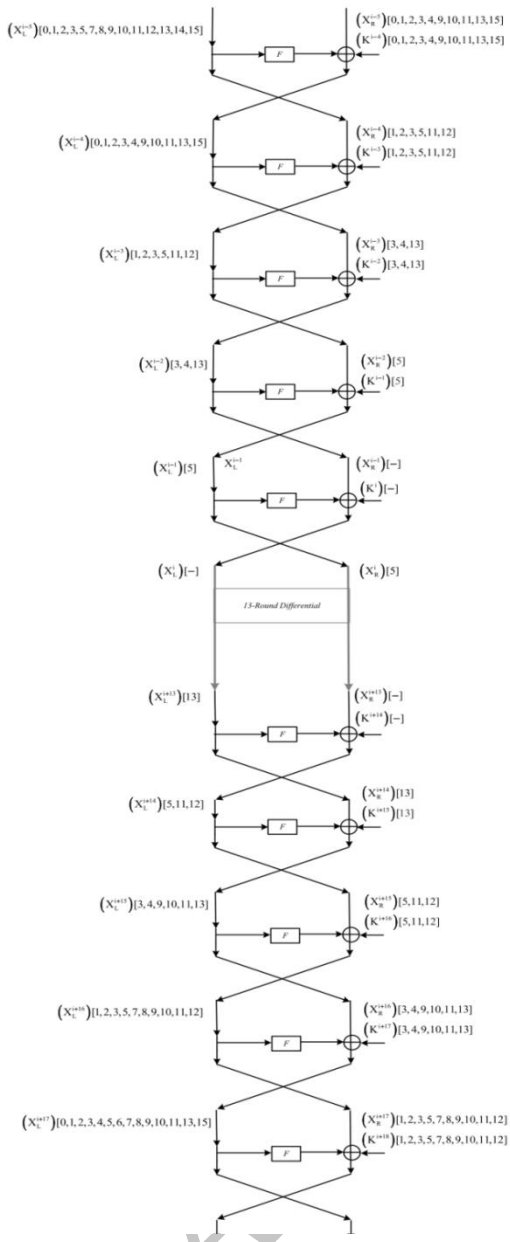
**** **** **** ****)

بعد از افزودن ۴ دور به انتهای این تفاضل، خروجی تفاضل به شکل زیر برای SIMON۳۲ به دست می‌آید.

ΔC_1: (*0*0, ****, **1*, ****,

00, 00, *0*0, 1***)

تفاضل D1 که بر اساس داشتن کمترین بیت فعال انتخاب‌شده است. تمرکز بیشتر تفاضلاتی که تا به حال از آن‌ها برای حمله بر روی این رمز قالبی استفاده شده بود بر روی احتمال مشخصه بوده است ولی در اینجا تمرکز ما روی افزایش تعداد دور حمله بوده است و کوچک بودن احتمال به‌عنوان اولویت دوم ما در نظر گرفته شده بود. به همین دلیل از تفاضل موجود در شکل ۱ برای این حمله استفاده نمودیم چون این تفاضل توانست تعداد زیرکلیدهای موردنیاز ما را کاهش دهد. در رمزگشایی ۵ دور ابتدایی و ۴ دور انتهایی، ۲۸ حالت (شرایط) مستقل از کلید مخفی و ۳۶ حالت وابسته به کلید مخفی وجود دارند زیرا با توجه به روابط ۳ و ۴ و ۵، مقادیر به‌دست‌آمده در دور i–ام در داخل رابطه ۳ گنجانده می‌شود و اگر مقدار تفاضلات موردنظر در رابطه ۳ نامعلوم باشد یا اگر مقدار یک داشته آنگاه چون طبق فرمول ۳ با X متناظر خود XOR می‌شوند در نتیجه ما به محاسبه X احتیاج پیدا می‌کنیم. X طبق روابط ۴ و ۵ وابسته به یک بیت زیرکلید است درنتیجه وقتی هر دو تفاضل در فرمول ۳ مقدار صفر داشته باشند تفاضل اصلی دور i–ام، وابسته به هیچ زیرکلیدی نیست و به همین صورت داریم اگر سه حالت دیگر وجود داشته باشد یعنی دو تفاضل فرمول ۳ به‌صورت (۰،۱) و (۱،۰) و (۱،۱) حدس زده شوند حداقل یک بیت زیرکلید و حداکثر دو بیت زیرکلید باید حدس زده شوند و درنتیجه در این حالت وابستگی به زیرکلیدها وجود دارد. ۳۲ حالت از متن اصلی و ۵ دور اول برای رسیدن به خروجی این ۵ دور به صورت (۰۰۲۰،۰۰۰۰) لازم و کافی است. برای این حمله علاوه بر روش بالا می‌توان از روش زیر بهره گرفت که دارای پیچیدگی کمتری نسبت به روش قبل است. حال در مورد محاسبه مقدار پیچیدگی و تعیین زیرکلیدهای فعال به بحث می‌پردازیم. هدف این روش این است که به‌گونه‌ای از تمام شرایط کلیدهای مخفی‌ای که نیاز به حدس آن‌ها وجود دارد استفاده شود تا تعداد بیت‌های زیرکلید کمتری حدس زده شوند. روش کار در شکل (۲) نشان داده شده است.



شکل (۲). روند حمله بر روی SIMON۳۲

ازآنجا که تعداد شرایط زیادی برای متن اصلی و خروجی دور اول وجود دارد که آن‌ها را از کلید مخفی مستقل می‌کند، درنتیجه از این شرایط برای ساختن ساختارهای موردنیاز حمله‌ای و کاهش پیچیدگی زمانی جفت‌های متن اصلی جمع شونده، بهره می‌گیریم. در شکل (۲) تعداد بیت‌هایی زیرکلیدی که باید در هر دور حدس زده شود مشخص‌شده است اگر بخواهیم با یک مثال نحوه محاسبه این بیت‌ها را شرح دهیم می‌توان به‌طور مثال بیت شماره ۱ در دور دوم را در نظر گرفت همان‌طور که قبلاً اشاره شد تابع SIMON شامل یک شیفت ۸ بیتی و یک شیفت ۱ بیتی است که با یکدیگر AND شده و در انتها با یک شیفت دوبیتی ورودی، XOR می‌شود پس طبق این خصوصیت ما نیاز به یافتن ۳ زیرکلید برای هر بیت فعال سمت چپ ساختار فیستل داریم

پس درنتیجه برای مثال بالا بیت ۱ از سمت چپ بیت ۲ و ۳ و ۹ از سمت راست را فعال می‌کند و درنتیجه ۳ زیرکلید فعال می‌شود ولی مهم‌ترین نکته در اینجا هم‌پوشانی زیرکلیدهای فعال‌شده است که باعث کاهش تعداد زیرکلیدهایی می‌شود که باید حدس زده شود این عامل با انتخاب درست مشخصه تفاضلی حاصل می‌شود.

پیچیدگی در اینجا برابر است با تعداد کل بیت‌های زیرکلید فعال‌شده ضرب در پیچیدگی زمانی ضرب در ۲. پس پیچیدگی برای SIMON۳۲ به‌صورت زیر به دست می‌آید:

$$۲^{۵۸/۶۹} = ۲^{۲۸} \times ۲^{۲۹/۶۹} \times ۲$$

۴- نتیجه‌گیری

در این مقاله، حمله تفاضلی بر روی سه الگوریتم از خانواده رمزهای قالبی SIMON مورد بررسی قرارگرفته است. با به‌کارگیری حمله تفاضلی می‌توان به تحلیل امنیت این سه رمز و ایده‌هایی جهت حملات جدیدتر دست یافت. حمله ارائه‌شده، بهترین حمله تفاضلی ارائه‌شده تابه‌حال بوده و به بهترین حمله موجود در هرکدام از این سه الگوریتم یک دور می‌افزاید.

ازآنجا که SIMON یک رمز بر پایه ARX بسیار ساده هست، هر حمله‌ای بر روی رمزهای ARX مانند Threefish می‌تواند یک تهدید برای این رمز باشد. به‌هرحال، یک جنبه مثبت امنیت SIMON، افزودن کلید به‌صورت دوری و سادگی آن است. هم‌زمان با این که ساختار کلید قدرتمندی را داراست، به‌طور مؤثری می‌تواند این رمز را از حملاتی نظیر meet-in-the-middle در تعداد دور معقول حفاظت می‌کند.

۵- قدردانی

این پژوهش با حمایت مالی دانشگاه تربیت دبیر شهید رجایی طبق قرارداد شماره ۱۹۰۹۵مورخ ۹۵/۸/۱ انجام گردیده است.

۶- مراجع

[1] M. Briceno, I. Goldverg, and D. Wagner, "A Pedagogical Implementation of the GSM A5/1 and A5/2 "voice privacy" encryption algorithms," 1999.

[2] 3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects," 3G Security, Specification of the 3GPP Confidentiality and Integrity Algorithms, Document 2: KASUMI Specification, V3.1.1, 2001.

[3] "New European Schemes for Signatures, Integrity, and Encryption," 2002-2003. http://www.cryptonessie.org

[4] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-bit Blockcipher CLEFIA (extended abstract)," FSE, vol. 4593 of Lecture Notes In Computer Science, pp. 181– 195, Springer, 2007.

[5] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. J. Kim, and S. Chee, "Hight: A New Nlock Cipher Suitable for Low-resource Device," In L. Goubin, and M. Matsui, editors, CHES, vol. 4249 of Lecture Notes in Computer Science, pp. 46–59, Springer, 2006.

[6] J. Guo, T. Peyrin, A. Poschmann, and M. J. B. Robshaw, "The LED Block Cipher," In Preneel and Takagi, pp. 326–341.

[7] T. Suzaki, K. Minematsu, S. Morioka, and E. Kobayashi, "${{twine}} $: A Lightweight Block Cipher For Multiple Platforms," In L. R. Knudsen and H. Wu, editors, Selected Areas in Cryptography, volume 7707 of Lecture Notes in Computer Science, pp. 339–354, Springer, 2012.

[8] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai, "Piccolo: An Ultra-lightweight Blockcipher," In Preneel and Takagi, pp. 342–357.

[9] A. Bogdanov, L. Knudsen, R. Leander, G. Paar, C. Poschmann, A. M. J. Robshaw, B. Y. Seurin, and C. Vikkelsoe, "Present: An Ultra-lightweight Block Cipher," In P. Paillier, and I. Verbauwhede, editors, CHES, vol. 4727 of Lecture Notes in Computer Science, pp. 450–466, Springer, 2007.

[10] E. Biham and A. Shamir, "Differential Cryptanalysis of the Data Encryption Standard," Springer, 1993.

[11] L. R. Knudsen, "Truncated and Higher Order Differentials," In B. Preneel, (ed.) Fast Software Encryption –FSE'94, Lecture Notes in Computer Science, vol. 1008, pp. 196–211, Springer, 1994.

[12] L. Knudsen, "DEAL-a 128-bit Block Cipher," Complexity vol. 258, no. 2, 1998.

[13] E. Biham, A. Biryukov, and A. Shamir, "Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials," pp. 12–23, Springer-Verlag, 1999.

[14] D. Wagner, "The Boomerang Attack," In L. R. Knudsen, editor, FSE, vol. 1636 of Lecture Notes in Computer Science, pp. 156-170, Springer, 1999.

[15] J. Kelsey, T. Kohno, and B. schneier, "Amplified Boomerang Attacks against Reduced-Round MARS and Serpent," In Fast Software Encryption, pp. 75-93, 2000.

[16] E. Biham, O. Dunkelman, and N. Keller, "The Rectangle Attack- Rectangling the Serpent," In Birgit Pfitzmann, editor, Eurocrypt, vol. 2045 of Lecture Notes in Computer Science, pp. 340–357, Springer, 2001.

[17] H. A. Alkhzaimi and M. M. Lauridsen, "Cryptanalysis of the SIMON Family of Block Ciphers," Cryptology ePrint Archive, Report 2013/543, 2013.

[18] A. Biryukov, A. Roy, and V. Velichkov, "Differential Analysis of Block Ciphers SIMON and SPECK," In FSE, 2014.

[19] F. Abed, E. List, S. Lucks, and J. Wenzel, "Differential and Linear Cryptanalysis of Round-Reduced Simon Family of Block Ciphers," Cryptology ePrint Archive, Report 2013/568, 2013.

[20] N. Wang, X. Wang, K. Jia, and J. Zhao, "Improved Differential Attacks on Reduced SIMON Versions," Cryptology ePrint Archive, Report 2014/448, 2014.

[21] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK Families of Lightweight Block Ciphers," Cryptology ePrint Archive, Report 2013/404, 2013.

[22] F. Abed, E. List, J. Wenzel, and S. Lucks, "Differential Cryptanalysis of round-reduced Simon and Speck," Preproceedings of Fast Software Encryption, In FSE, 2014.

[23] Q. Wang, Z. Liu, K.Varıcı, Y. Sasaki, V. Rijmen, and Y. Todo, "Cryptanalysis of Reduced-round SIMON32 and SIMON48," In Progress in Cryptology Indocrypt Springer International Publishing, pp. 143-160, 2014.

[24] J. Alizadeh, H. A. Alkhzaimi, M. R. Aref, N. Bagheri, P. Gauravaram, A. Kumar, and S. K. Sanadhya, "Cryptanalysis of Simon variants with Connections," In Radio Frequency Identification: Security and Privacy Issues, pp. 90-107, Springer International Publishing, 2014.

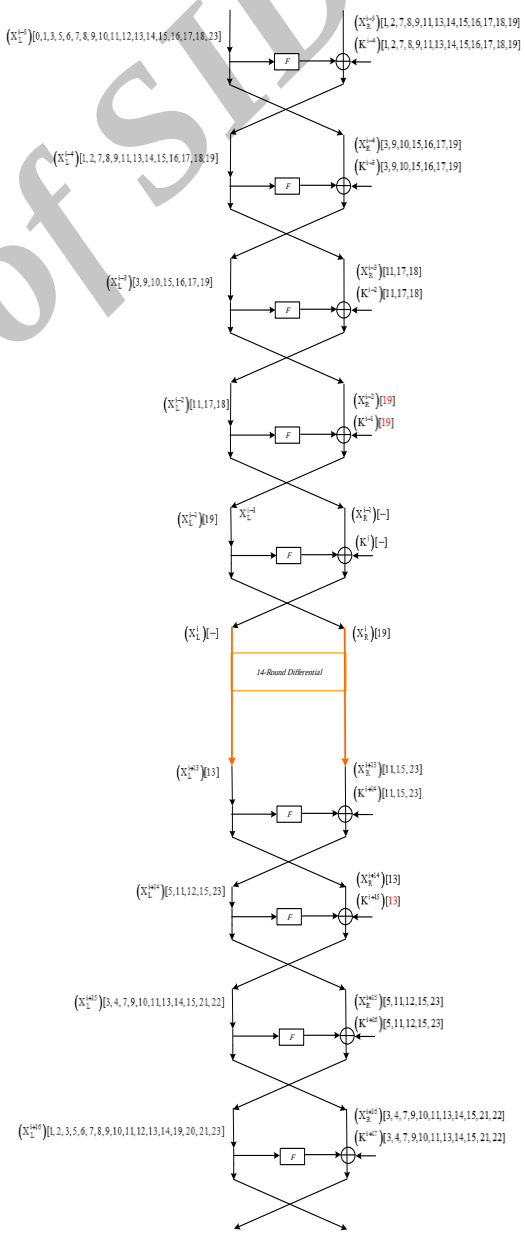
[25] J. Alizadeh, H. A. Alkhzaimi, M. R. Aref, N. Bagheri, P. Gauravaram, and M. M. Lauridsen, "Improved linear cryptanalysis of round reduced SIMON," IACR Cryptology

ePrint Archive, Reprot 2014/681. http://eprint. iacr. org/2014/681.pdf, 2014.

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

پیوست ۱

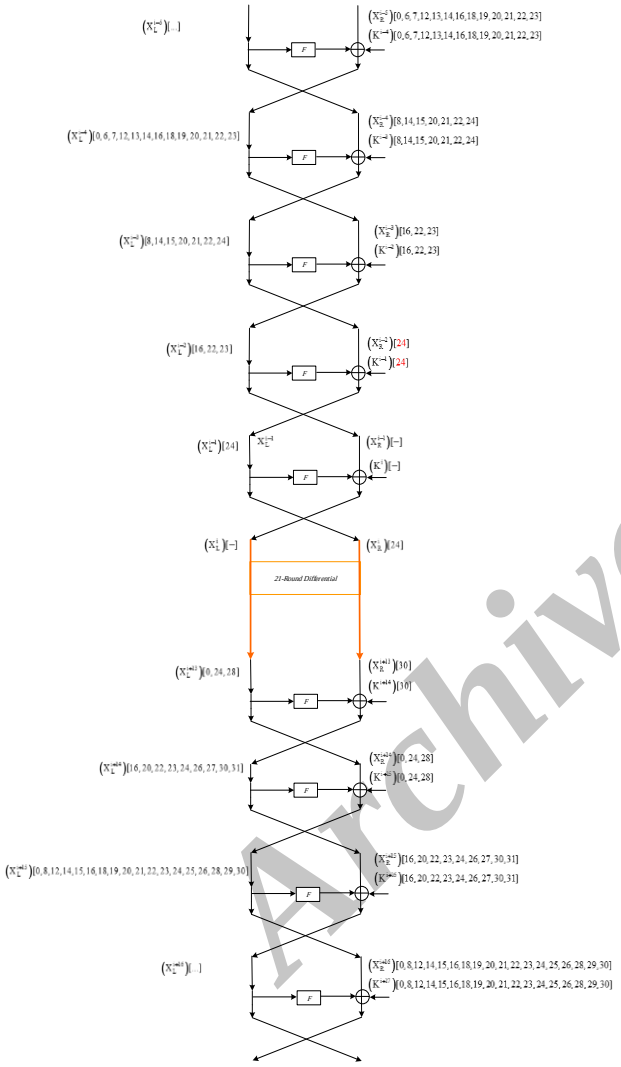
حمله تفاضلی بـه ۲۳ دور SIMON۴۸/۹۶: در ایـن روش حملـه، مشابه با روش دوم مطرح شده در حمله بر روی SIMON استفاده نمودیم یعنی مشخصه‌ای را یافتیم که کمتـرین بیـت فعـال را در ورودی و خروجی داشته باشد سپس بیت‌های فعال زیرکلید را بـا توجه به خصوصیات تابع F پیدا نمودیم. در شـکل (۳) حملـه بـر روی ۲۳ دور SIMON۴۸/۹۶ نشان داده شده است.



شکل (۳). حمله بر روی ۲۳ دور SIMON۴۸/۹۶

پیوست ۲

حمله تفاضلی به ۲۹ دور SIMON۶۴/۱۲۸: در ایـن روش حملـه، مشابه با روش دوم مطرح شده در حمله بر روی SIMON استفاده نمودیم یعنی مشخصه‌ای را یافتیم که کمتـرین بیـت فعـال را در ورودی و خروجی داشته باشد سپس بیت‌های فعال زیرکلید را بـا توجه به خصوصیات تابع F پیدا نمودیم. در شـکل (۴) حملـه بـر روی ۲۹ دور SIMON۶۴/۱۲۸ نشان داده شده است.



شکل (۴). حمله بر روی ۲۹ دور SIMON۶۴/۱۲۸

Journal Of Electronical & Cyber Defence
Vol. 5, No. 1, 2017, Serial No. 17

Differential Cryptanalysis of Round-Reduced SIMON32 and SIMON48 and SIMON64

S. Ahmad Oskoueian, N. Bagheri*

*Shahid Rajaee Teacher Training University

(Received: 30/05/2015, Accepted: 31/10/2016)

ABSTRACT

On June 2013, Beaulieu and et.al from the U.S National Security Agency proposed a family of block ciphers, SIMON. This family of block ciphers is classified as lightweight block ciphers that comes in a variety of widths and key sizes. SIMON offers excellent performance on hardware and software platforms from which hardware performance is optimal. The main purpose of this paper is to provide improved differential attacks proposed on this family of block ciphers. Getting help from the new ideas and viewpoints about methods and key-guessing policies, we improve differential attack on 22-round SIMON32, 23-round SIMON48 and 29-round SIMON64. This attack adds one round to the latest differential cryptanalysis presented before this paper submission.

Keywords: SIMON, Differential Cryptanalysis, Lightweight Block Ciphers

*Corresponding Author Email: Nbagheri@srttu.edu