

# حمله‌ی بومرنگ ناممکن کلیدمرتبط روی دور کاهشی یافته‌ی رمز قالبی Simon32/64

فهیمة عظیمة<sup>۱</sup>، نصور باقری<sup>۲</sup>

۱ کارشناسی ارشد امنیت اطلاعات، دانشگاه صنعتی مالک اشتر تهران، fahimeh.azimy@gmail.com

۲ استادیار دانشکده مهندسی برق، دانشگاه تربیت دبیر شهید رجائی، Nbagheri@srutu.edu

تاریخ دریافت: ۹۴/۱۲/۲۲ تاریخ پذیرش: ۹۵/۲/۱۵

## چکیده

در دهه‌ی گذشته حملات کلیدمرتبط از جهت نظری و عملی مورد مطالعه قرار گرفته‌اند و آسیب‌ناپذیری در برابر حملات کلیدمرتبط به‌عنوان یکی از اهداف امنیت در طراحی رمزهای قالبی در نظر گرفته شده‌است. ارزیابی رمزها در مقابل انواع حملات، منجر به شناسایی آسیب‌پذیری آن‌ها و بهبود طرح‌های رمزنگاری می‌شود. حمله‌ی بومرنگ ناممکن کلیدمرتبط، از ترکیب حملات بومرنگ و تفاضلی ناممکن کلیدمرتبط ساخته می‌شود. انعطاف‌پذیری در انتخاب تفاضل‌های کلید، امکان حمله روی تعداد دور بیشتری از رمزهای قالبی را با استفاده از این حمله فراهم می‌سازد. خانواده‌ی رمزسبک‌وزن Simon اخیراً توسط NSA به‌صورت امن و انعطاف‌پذیر برای عملکرد مناسب در محیط‌های محدود سخت‌افزاری و در ده نسخه طراحی شده‌است. زمانبند کلید Simon در برابر حملات کلیدمرتبط، مقاوم طراحی شده‌است. در این مقاله برای اولین بار حمله‌ی بومرنگ ناممکن کلیدمرتبط روی ۲۰ دور کاهشی یافته رمز سبک‌وزن Simon32/64 انجام شده‌است.

## کلیدواژه

رمز قالبی، زمانبند کلید، حمله‌ی بومرنگ ناممکن کلیدمرتبط، Simon32/64

## مقدمه

Simon و Speck را معرفی کند [۱]. در چهار دهه‌ی اخیر آژانس امنیت ملی آمریکا سومین رمز قالبی را منتشر ساخته است، بنابراین بررسی امنیت رمز Simon در برابر انواع حملات حائز اهمیت است.

در رمزهای قالبی عملیات مشخصی روی بلوکی از داده‌ها بر اساس الگوریتم رمز تکرار می‌شود. رمزهای قالبی در دو ساختار رمز فیستل و شبکه‌های جایگشت-جایگذاری<sup>۵</sup> وجود دارند. باتوجه به اهمیت رمزهای سبک‌وزن و استفاده‌ی آن‌ها در وسایل با فضای محدود، تمرکز در این مقاله روی رمز Simon از رمزهای سبک‌وزن با ساختار فیستل است [۴-۲].

امروزه روش‌های گوناگونی برای تحلیل و بررسی رمزها وجود دارد که رمزها را از جنبه‌های متفاوتی بررسی می‌کنند [۵]. یکی از نیرومندترین و گسترده‌ترین حملات روی رمزهای متقارن، حمله تفاضلی<sup>۶</sup> می‌باشد که اولین بار توسط بیهام<sup>۷</sup> و شمیر<sup>۸</sup> روی رمز FEAL انجام شد [۶]. ایده‌ی اصلی حملات تفاضلی، مطالعه‌ی

تاکنون مطالعات فراوانی در زمینه‌ی رمزنگاری صورت گرفته و همزمان با ایجاد رمزهای مختلف، حملات وسیعی برای به‌دست آوردن کلید، گسترش یافته است. از مهم‌ترین طرح‌های اولیه رمزنگاری، رمزهای کلیدمتقارن<sup>۱</sup>، رمزهای کلیدعمومی نامتقارن<sup>۲</sup> و توابع چکیده‌ساز<sup>۳</sup> می‌باشند. رمزهای کلیدمتقارن، شامل رمزهای قالبی و رمزهای رشته‌ای می‌شوند. رمزهای سبک‌وزن به طراحی رمزهایی می‌پردازند که برای قرار گرفتن و اجرا روی وسایل سخت‌افزاری کوچک مانند برچسب‌های RFID، حسگرهای شبکه و کارت‌های هوشمند بدون اتصال استفاده می‌شوند. رمزهای استاندارد متقارنی مانند AES نمی‌توانند در وسایل کوچک کم‌هزینه، استفاده شوند. در جامعه‌ی رمزنگاری، اخیراً رمزهای سبک‌وزن برای محیط‌های محدود مناسب شمرده شدند و باتوجه به کاربرد و گسترش این‌گونه وسایل، امنیت در این رمزها اهمیت ویژه‌ای پیدا می‌کند. اهمیت رمزنگاری سبک‌وزن و کاربرد آن‌ها باعث شده‌است که اخیراً<sup>۴</sup> NSA دو خانواده‌ی رمز بسیار سبک‌وزن

5 Substitution-permutation Network

6 Differential Cryptanalysis

7 Biham

8 Shamir

1 Symmetric or Secret-Key Algorithm

2 Public-Key Algorithm

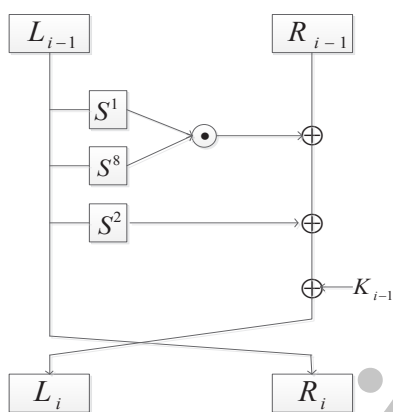
3 Hash Function

4 The National Security Agency

ادامه به معرفی و بیان مفاهیم رمز Simon پرداخته می‌شود. سپس حمله‌ی بومرنگ ناممکن کلیدمرتبط بیان می‌شود. در بخش بعد به بیان حمله‌ی بومرنگ ناممکن کلیدمرتبط<sup>۱۳</sup> روی نسخه‌ی Simon32/64 می‌پردازیم. در پایان، نتیجه‌گیری در بخش ۵ آورده می‌شود.

### معرفی رمز سبک‌وزن Simon

رمز قالبی Simon در ده نسخه با ساختار فیستل برای کاربرد بهینه در محیط‌های محدود سخت‌افزاری طراحی شده‌است. این رمز با کلمات  $n$ -بیتی (بلوک  $2n$ -بیتی) و کلید  $m$ -بیتی با  $Simon_{2n/mn}$  مشخص می‌شود که  $n \in \{16, 24, 32, 48, 64\}$  و  $m \in \{2, 3, 4\}$  می‌تواند باشد. تابع رمز Simon از سه عملیات XOR، AND منطقی و شیفت چرخشی به چپ استفاده می‌کند. در شکل (۱) ساختار یک دور از این رمز نشان داده شده‌است.



شکل ۱. ساختار یک دور رمز Simon.

تابع رمزنگاری:

$$Round_K(L_i, R_i) = (R_{i-1} \oplus ((1 \lll L_{i-1} \odot 8 \lll L_{i-1}) \oplus (2 \lll L_{i-1})) \oplus K_{i-1}, L_{i-1}) \quad (1)$$

تابع رمزگشایی:

$$Round_K^{-1}(L_i, R_i) = (R_{i-1}, L_{i-1} \oplus ((1 \lll R_{i-1} \odot 8 \lll R_{i-1}) \oplus (2 \lll R_{i-1})) \oplus K_{i-1}) \quad (2)$$

زمانبند کلید Simon از دو عملیات XOR و شیفت چرخشی به راست استفاده می‌کند و بر اساس  $m$  دارای سه ساختار متفاوت است. هر دنباله زیرکلید از این زمانبند کلید، منحصراً یک کلید مخفی را تولید می‌کند و نیز از هر کلید مخفی یک دنباله زیرکلید مشخص تولید می‌شود.

اگر  $m=2$ :

$$K_i = (K_{i-1} \ggg 3 \oplus K_{i-2}) \oplus (K_{i-1} \ggg 4) \oplus (C \oplus (Z_j)_i) \quad (3)$$

انتشار تفاضل متن‌های اصلی از طریق فرآیند رمزنگاری است که در همین رابطه مفهوم دنباله‌ی تفاضلی ارائه شده‌است. دنباله‌ی تفاضلی، احتمال انتشار تفاضل ورودی به تفاضل خروجی را توصیف می‌کند. در صورتی که احتمال وجود چنین دنباله‌ای در رمز به میزان قابل توجهی از توزیع تصادفی بیشتر باشد، این اطلاعات می‌تواند برای تمایز رمز از جایگشت تصادفی استفاده شود و تعدادی از بیت‌های کلید مخفی کشف شود. در این حمله، ابتدا مهاجم چند جفت متن اصلی را توسط تابع رمزنگاری، رمز نموده و جفت‌های متن رمز شده را با هدف برآورده شدن انتشار دنباله‌ی تفاضلی جستجو می‌کند. معمولاً زیرکلیدهای دور، مستقیماً قبل یا بعد از تفاضل تعیین می‌شوند و سپس تجزیه‌تحلیل روی دورهای بیشتر گسترش می‌یابد [۷].

یکی از انواع حملات روی رمزهای قالبی، حملات کلیدمرتبط<sup>۹</sup> است که مهاجم می‌تواند عملیات رمز را روی کلیدهای مختلف اما ناشناخته بررسی کند. در حمله‌ی کلیدمرتبط هر چند کلیدها برای مهاجم ناشناخته هستند اما روابط ریاضی بین آن‌ها شناخته شده‌است. با شناخت روابط بین کلیدها مهاجم با استفاده از نقاط ضعف الگوریتم زمانبندی کلید<sup>۱۰</sup> و الگوریتم رمزنگاری، کلید مخفی را به دست می‌آورد [۸-۹]. در دهه‌ی گذشته حملات کلیدمرتبط از جهت نظری و عملی مورد مطالعه قرار گرفته‌اند [۱۰-۱۱] و آسیب‌ناپذیری در برابر حملات کلیدمرتبط به‌عنوان یکی از اهداف امنیت در طراحی رمزهای قالبی مدرن در نظر گرفته شده‌است [۱۲]. استفاده از حملات کلیدمرتبط همراه با حملات دیگری مانند حمله‌ی تفاضلی و بومرنگ پیچیدگی این حمله را کاهش می‌دهد. با توجه به کاهش احتمال گسترش دنباله‌ی تفاضلی روی تعداد دورهای بیشتر رمز، نوعی حمله‌ی تفاضلی به‌نام بومرنگ<sup>۱۱</sup> توسط واگنر<sup>۱۲</sup> [۱۳] به‌وجود آمد. در حمله‌ی بومرنگ، دو دنباله‌ی تفاضلی مستقل با احتمال زیاد جایگزین یک دنباله‌ی تفاضلی در سرتاسر رمز، با احتمال کم می‌شوند. ایده‌ی اصلی در این حمله به‌دست آوردن چهار حالت داخلی در میانه رمز است. در این حمله تفاضل‌ها یک مستطیل در میانه‌ی رمز تشکیل می‌دهند. این چهارتایی به‌عنوان تفاضل ورودی روی نیمه دیگر رمز محسوب می‌شود، در نتیجه دنباله‌ی تفاضلی کوچکتر با احتمال بیشتر، جایگزین دنباله‌ی تفاضلی بزرگتر با احتمال کمتر می‌شود [۱۳].

با توجه به اهمیت رمزهای سبک‌وزن برای استفاده در محیط‌های محدود و کاربرد و گسترش این‌گونه وسایل با فضای کم، امنیت در این رمزها اهمیت ویژه‌ای پیدا می‌کند. در این مقاله به بررسی یک نوع از حملات کلیدمرتبط که جزء حملات پرکاربرد می‌باشد، روی رمز قالبی سبک‌وزن Simon می‌پردازیم. در ادامه این مقاله، در

13 Related-key Impossible Boomerang Attack

9 Related-key Attack  
10 Key Schedule  
11 Boomerang Attack  
12 Wagner

تفاضلی، عامل مهمی در طراحی رمزهای قالبی در نظر گرفته می‌شود. با این حال، امنیت در برابر حملات خطی و تفاضلی برای تضمین امنیت رمزهای قالبی کافی نمی‌باشد و ممکن است در مقابل انواع دیگری از حملات آسیب‌پذیر باشند. تجزیه‌تحلیل رمزهای جدید منجر به بهبود ارزیابی امنیت رمزهای قالبی و طراحی رمزهای امن‌تر می‌شود. حملات تفاضلی ناممکن و حملات نوع-بومرنگ (شامل بومرنگ، بومرنگ تقویت شده، مستطیلی و انواع کلیدمرتبط آن‌ها) در تحلیل امنیت تعداد زیادی از رمزهای قالبی استفاده شده‌است. در ادامه به معرفی حمله‌ی بومرنگ ناممکن کلیدمرتبط و انجام آن روی نسخه‌ی Simon32/64 می‌پردازیم. در جدول (۱) مهم‌ترین حملات انجام شده روی رمز Simon32/64 آورده شده‌است.

اگر  $m=3$ :  

$$K_i = (K_{i-1} \ggg 3 \oplus K_{i-3}) \oplus (K_{i-1} \ggg 4) \oplus (C \oplus (Z_j)_i) \quad (۴)$$

اگر  $m=4$ :  

$$K_i = ((K_{i-1} \ggg 3 \oplus K_{i-3}) \oplus K_{i-4}) \oplus ((K_{i-1} \ggg 3 \oplus K_{i-3}) \ggg 4) \oplus (C \oplus (Z_j)_i) \quad (۵)$$

که ثابت  $C = 0x\text{ff} \dots \text{fc}$  و  $(Z_j)_i$  کم‌ارزشترین بیت (بیت  $i$ -ام) یکی از دنباله ثابت‌های  $Z_0, Z_1, Z_2, Z_3, Z_4$  را نشان می‌دهد. عبارت  $(C \oplus (Z_j)_i)$  برای جلوگیری از حملات چرخشی و حملات جانبی در زمانبند کلید به کار برده می‌شود. جزئیات بیشتر در مورد ساختار این رمز در [۱] بیان شده‌است.

حملات خطی و تفاضلی عمومی‌ترین ابزارهای حمله روی رمزهای قالبی می‌باشند. امنیت قابل اثبات در برابر حملات خطی و

جدول ۱. مهم‌ترین حملات انجام شده روی رمز Simon32/64.

Simon32/64 (Round=32)					
مرجع	سال	پیچیدگی داده‌ای	پیچیدگی زمانی	تعداد دور حمله شده	نام حمله
[۷]	۲۰۱۳	$2^{11}$	-	۱۱	حمله‌ی خطی
[۱۴]	۲۰۱۳	$2^{11}$	-	۱۲	حمله‌ی خطی
[۷]	۲۰۱۳	$2^{16.6}$	$2^{5.6}$	۱۳	حمله‌ی تفاضلی ناممکن
[۱۵]	۲۰۱۳	$2^{10}$	$2^{5.1}$	۱۳	حمله‌ی تفاضلی ناممکن
[۱۵]	۲۰۱۳	$2^{16.6}$	$2^{14.7}$	۱۴	حمله‌ی کلیدمرتبط تفاضلی
[۱۶]	۲۰۱۳	$2^{12.161}$	$2^{22.182}$	۱۴	حمله‌ی تفاضلی ناممکن
[۱۶]	۲۰۱۳	$2^{16.481}$	$2^{16.481}$	۱۶	حمله‌ی تفاضلی
[۱۵]	۲۰۱۳	$2^{11.2}$	$2^{4.6}$	۱۸	حمله‌ی تفاضلی
[۷]	۲۰۱۳	$2^{10.86}$	$2^{52.55}$	۱۸	حمله‌ی مستطیلی کلیدمرتبط
[۱۷]	۲۰۱۴	$2^{11}$	$2^{51}$	۱۸	حمله‌ی مکعبی پویا
[۱۸]	۲۰۱۴	$2^{11}$	$2^{61.14}$	۱۸	حمله‌ی تفاضلی ناممکن
[۱۹]	۲۰۱۴	$2^{11}$	$2^{11}$	۱۹	حمله‌ی تفاضلی
[۲۰]	۲۰۱۴	$2^{11}$	$2^{22.52}$	۱۹	حمله‌ی تفاضلی ناممکن
[۲۰]	۲۰۱۴	$2^{11}$	$2^{22.52}$	۱۹	حمله‌ی تفاضلی ناممکن
[۲۱]	۲۰۱۴	$2^{11}$	$2^{22}$	۲۰	حمله‌ی پوش خطی
[۲۲]	۲۰۱۴	$2^{11}$	$2^{22}$	۲۱	حمله‌ی تفاضلی
[۱۸]	۲۰۱۴	$2^{11}$	$2^{56.66}$	۲۰	حمله‌ی خطی همبستگی صفر
[۲۳]	۲۰۱۴	$2^{11}$	$2^{55.25}$	۲۱	حمله‌ی تفاضلی
[۲۴]	۲۰۱۴	$2^{10.56}$	$2^{55.56}$	۲۱	حمله‌ی پوش خطی
[۱۸]	۲۰۱۴	$2^{11}$	$2^{21}$	۲۱	حمله‌ی جدائی‌ناپذیر
[۲۵]	۲۰۱۵	-	$2^{61.57}$	۱۸	حمله‌ی ملاقات در میانه
[۲۶]	۲۰۱۵	$2^{11}$	$2^{58.919}$	۱۹	حمله‌ی تفاضلی ناممکن
[۲۷]	۲۰۱۵	$2^{11.19}$	-	۲۳	حمله‌ی پوش خطی
[بخش ۴]	۲۰۱۶	$2^{11}$	$2^{21.68}$	۲۰	حمله‌ی بومرنگ ناممکن کلیدمرتبط

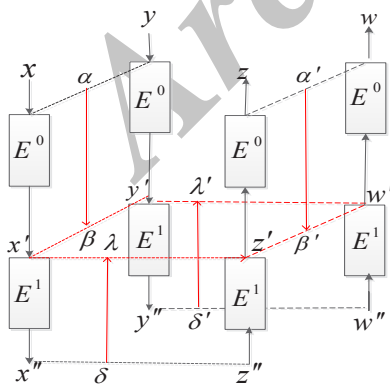
## حمله‌ی بومرنگ ناممکن

انعطاف‌پذیری در انتخاب تفاضل‌های کلید امکان شکست دورهای بیشتری از رمز قالبی با استفاده از حمله‌ی بومرنگ تفاضلی ناممکن را فراهم می‌سازد. زمانی که یک تفاضل ناممکن ساخته می‌شود، انتخاب تفاضل زیرکلید برای  $E^0$  معمولاً باعث یک تفاضل معین در زیرکلید  $E^1$  می‌شود و بالعکس. اما زمانی که یک تمایزگر بومرنگ ناممکن کلیدمرتبط ساخته می‌شود، انعطاف‌پذیری بیشتری در انتخاب تفاضل‌های زیرکلید برای  $E^0$  و  $E^1$  داریم: می‌توان از یک تفاضل زیرکلید برای  $E^0$  و یک تفاضل زیرکلید کاملاً نامرتبط برای  $E^1$  استفاده کرد. حتی برای انعطاف‌پذیری بیشتر می‌توان از دو تفاضل زیرکلید متفاوت برای  $E^0$  یا  $E^1$  به‌کار برد. این انعطاف‌پذیری در انتخاب تفاضل‌های کلید، امکان شکستن دورهای بیشتری از رمزهای قالبی با استفاده از حمله‌ی بومرنگ ناممکن را فراهم می‌سازد. در [۳۱] نشان می‌دهند که حداکثر طول تمایزگرهای بومرنگ ناممکن با تمایزگرهای تفاضلی ناممکن روی رمزهای معین برابر است ولی حمله‌ی بومرنگ ناممکن با احتمال بیشتری روی آن‌ها امکان‌پذیر (عملی) است.

### تمایزگر بومرنگ ناممکن

در [۲۸] بیان می‌شود که مانند یک تمایزگر بومرنگ، یک تمایزگر بومرنگ ناممکن رمز قالبی  $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$  را به‌صورت دو زیررمز  $E^0 \circ E^1$  در نظر می‌گیرد. چنین تمایزگری از چهار تفاضل مرتبط ساخته می‌شود، دو تفاضل برای  $E^0$  و دو تفاضل برای  $E^1$  استفاده می‌شود و همه‌ی این تفاضل‌ها احتمال ۱ دارند. یک تمایزگر بومرنگ ناممکن در شکل (۲) نشان داده شده‌است. یک تمایزگر بومرنگ ناممکن شامل:

- یک تفاضل  $\Delta\alpha \rightarrow \Delta\beta$  با احتمال ۱ برای  $E^0$
- یک تفاضل  $\Delta\alpha' \rightarrow \Delta\beta'$  با احتمال ۱ برای  $E^0$
- یک تفاضل  $\Delta\delta \rightarrow \Delta\gamma$  با احتمال ۱ برای  $(E^1)^{-1}$
- یک تفاضل  $\Delta\delta' \rightarrow \Delta\gamma'$  با احتمال ۱ برای  $(E^1)^{-1}$



شکل ۲. تمایزگر بومرنگ ناممکن [۲۸].

که  $\delta, \alpha, \alpha', \beta, \beta', \gamma, \gamma', \delta'$  و  $\delta$  بیت‌های  $n$ -بیتی هستند و  $\beta, \beta', \gamma$  و  $\gamma'$  شرط  $\beta \oplus \beta' \oplus \gamma \oplus \gamma' \neq 0$  را برآورده می‌کنند.

حمله‌ی بومرنگ ناممکن در سال ۲۰۰۸ توسط جیگیانگ لو<sup>۱۴</sup> در پایان‌نامه‌ی دکتری وی پیشنهاد شده‌است [۲۸]. این حمله یک توسعه‌ی جدید از حملات تفاضلی است. در این حمله با ترکیب ایده‌های حملات تفاضلی ناممکن و بومرنگ، تمایزگر بومرنگ ناممکن ساخته می‌شود. مشابه یک حمله‌ی بومرنگ، یک رمز قالبی  $E$  به‌صورت دو زیررمز  $E^0 \circ E^1$  در نظر گرفته می‌شود. دو (یا بیشتر) تفاضل با احتمال ۱ برای  $E^0$  و دو (یا بیشتر) تفاضل با احتمال ۱ برای  $E^1$  استفاده می‌شود که XOR تفاضل‌های میانه‌ی این تفاضل‌ها برابر با صفر است. حمله‌ی تفاضلی ناممکن اولین‌بار توسط بیهام و کلر<sup>۱۵</sup> روی ۵-دور کاهش‌یافته‌ی رمز AES-128 ارائه شد. در این حمله، تفاضل‌هایی جستجو می‌شوند که احتمال وقوع صفر دارند [۲۹]. در [۲۸] حمله‌ی بومرنگ ناممکن برای شکستن ۶-دور AES-128، ۷-دور AES-192 و ۷-دور AES-256 در سناریوی حمله تک کلیدی ۸-دور AES-192 و ۹-دور AES-256 در سناریوی حمله‌ی کلیدمرتبط با دو کلید استفاده شده است.

در انجام حملات تفاضلی، مطلوب است که تفاضل تا جای ممکن روی بیشترین تعداد دور برقرار شود. البته با افزایش تعداد دور، تفاضل احتمال کمتری پیدا می‌کند. حمله‌ی بومرنگ بر اساس چنین ایده‌ای شکل گرفته است و از دو تفاضل کوتاه‌تر با احتمال بیشتر به‌جای یک تفاضل با احتمال کمتر روی تعداد دور بیشتر استفاده می‌کند [۳۰]. در حملات تفاضلی ناممکن تفاضل‌ها هرگز و تحت هیچ شرایطی انجام نمی‌شوند. حمله‌ی بومرنگ ناممکن از ترکیب حملات بومرنگ و تفاضلی ناممکن ایجاد شده‌است. حمله‌ی بومرنگ ناممکن بر اساس تمایزگر بومرنگ ناممکن ساخته می‌شود [۲۸].

همان‌طور که در [۲۸] ذکر شده‌است، یک رمز قالبی مقاوم نسبت به حمله‌ی نوع-بومرنگ لزوماً در مقابل حمله‌ی بومرنگ ناممکن مقاوم نمی‌باشد. در تمایزگر نوع-بومرنگ، خروجی یک دور میانه‌ی رمز با توزیع یکنواخت و مستقل از دورهای قبلی در نظر گرفته می‌شود. در حالی که، در تمایزگر بومرنگ ناممکن اغلب توزیع یکنواخت و استقلال از دورهای قبلی در نظر گرفته نمی‌شود. بنابراین به‌نظر می‌رسد یک تمایزگر بومرنگ ناممکن از تمایزگر نوع-بومرنگ مناسب‌تر است [۲۸]. در واقع، امتیاز حمله‌ی بومرنگ ناممکن نسبت به حملات بومرنگ، مشابه حملات تفاضلی ناممکن نسبت به حملات تفاضلی است. با آنکه همیشه می‌توان یک تفاضل ناممکن را از یک تمایزگر ناممکن بومرنگ روی تعداد دور یکسان به‌دست آورد، این مورد برای انواع آن‌ها در سناریوی حمله کلیدمرتبط درست نمی‌باشد. همان‌طور که در [۲۸] بیان شده‌است،

14 Jiqiang Lu  
15 Keller

چهارتائی‌هایی که شرایط زیر را برآورده سازند چهارتائی درست نامیده می‌شوند.

$$E_{K_a}^a(x) \oplus E_{K_a}^a(y) = \alpha \quad (9)$$

$$E_{K_a}^a(z) \oplus E_{K_a}^a(w) = \alpha' \quad (10)$$

$$(E_{K_b}^b)^{-1}(x'') \oplus (E_{K_b}^b)^{-1}(y'') = \delta \quad (11)$$

$$(E_{K_b}^b)^{-1}(z'') \oplus (E_{K_b}^b)^{-1}(w'') = \delta' \quad (12)$$

اگر یک چهارتائی وجود داشته باشد که معادلات ۹-۱۲ را برآورده سازد، حدس زیرکلید  $(K_a, K_b)$  باید نادرست باشد و می‌تواند حذف شود. بنابراین با تعداد کافی از جفت‌های متن اصلی انتخابی، زیرکلید درست در  $E^a$  و  $E^b$  با حذف حدس‌های نادرست پیدا می‌شود.

### حمله‌ی بومرنگ ناممکن کلیدمرتبط

در حمله‌ی کلیدمرتبط، دشمن نه‌تنها قادر به رمزنگاری و رمزگشایی با کلید  $K$  است، همچنین می‌تواند از کلیدهای مرتبط استفاده کند. در حمله‌ی کلیدمرتبط نگاهت رابطه توسط دشمن انتخاب می‌شود. در اولین حمله‌ی کلیدمرتبط یک روش نگاهت ساده به‌کار رفته است: چرخش [۳۲] و فیلپ‌های بیت [۳۳]. در سناریوی حمله‌ی کلیدمرتبط [۳۴]، فرض می‌شود مهاجم تفاضل مشخصی بین یک یا چندین جفت کلید می‌شناسد. در تمایزگر بومرنگ ناممکن کلیدمرتبط، رمز قالبی  $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$  به‌صورت دو زیررمز  $E^0 \circ E^1$  در نظر گرفته می‌شود. معمولاً، چنین تمایزگری در سناریوی حمله‌ی کلیدمرتبط شامل چهار کلید  $K_A, K_B, K_C, K_D$  است و از چهار تفاضل کلیدمرتبط ساخته شده‌است. دو تفاضل برای  $E^0$  و دو تفاضل برای  $E^1$  در نظر گرفته می‌شود که باید احتمال ۱ داشته باشند [۲۸].  $E^a$  تعداد دوره‌های قبل از  $E^0$  و  $E^b$  تعداد دوره‌های بعد از  $E^1$  را نشان می‌دهد. بنابراین، تمایزگر بومرنگ ناممکن کلیدمرتبط شامل موارد زیر است:

- یک تفاضل کلیدمرتبط  $\Delta\alpha \rightarrow \Delta\beta$  با احتمال ۱ برای  $E^0$  تحت کلید  $K_B$  و  $K_A$
- یک تفاضل کلیدمرتبط  $\Delta\alpha' \rightarrow \Delta\beta'$  با احتمال ۱ برای  $E^0$  تحت کلید  $K_D$  و  $K_C$
- یک تفاضل کلیدمرتبط  $\Delta\delta \rightarrow \Delta\gamma$  با احتمال ۱ برای  $E^1$  تحت کلید  $K_A$  و  $K_C$
- یک تفاضل کلیدمرتبط  $\Delta\delta' \rightarrow \Delta\gamma'$  با احتمال ۱ برای  $E^1$  تحت کلید  $K_B$  و  $K_D$

که  $\theta, \mu, \mu', \alpha, \alpha', \beta, \beta', \gamma, \gamma', \delta, \delta'$  و  $\theta$  بلوک‌های  $n$ -بیتی هستند و  $\beta, \beta', \gamma, \gamma'$  شرط  $\beta \oplus \beta' \oplus \gamma \oplus \gamma' \neq 0$  را برآورده می‌کنند. برای برآورده شدن این شرط می‌تواند دو تفاضل موجود در  $E^0$  یا  $E^1$  را تاجائیکه شرط برقرار باشد، کاملاً یکسان در نظر

چهارتائی‌هایی که شرایط زیر را برآورده سازند چهارتائی درست نامیده می‌شوند.

$$\begin{aligned} z \oplus w = \alpha, x \oplus y = \alpha & - \\ z' \oplus w' = \beta, x' \oplus y' = \beta & - \\ y' \oplus w' = \gamma, x' \oplus z' = \gamma & - \\ y'' \oplus w'' = \delta, x'' \oplus z'' = \delta & - \end{aligned}$$

و تعداد چهارتائی‌های درست موردانتظار با شروع  $m$  جفت متن اصلی برابر است با:

$$\binom{mq}{2} \cdot 2^{-n+1} \cdot q^2 \cdot 2^{-n} = m^2 \cdot 2^{-n} \cdot (pq)^2 \quad (6)$$

بنابراین اگر  $pq < 2^{-n/2}$  باشد، دشمن می‌تواند چهارتائی‌های درست را برای  $E$  شمارش و از جایگشت تصادفی تشخیص دهد.

**قضیه:** اثبات مبنای نظری حمله‌ی بومرنگ ناممکن

باتوجه به [۲۸]، فرض کنید که  $X$  و  $X'$  بلوک‌های  $n$ -بیتی هستند و  $K$  یک کلید برای رمز قالبی  $n$ -بیتی  $E^1 \circ E^0 = E$  است. فرض کنید که  $\Delta\alpha \rightarrow \Delta\beta$  و  $\Delta\alpha' \rightarrow \Delta\beta'$  تفاضل‌هایی با احتمال ۱ برای  $E_K^0, E_K^1, \Delta\delta \rightarrow \Delta\gamma$  و  $\Delta\delta' \rightarrow \Delta\gamma'$  تفاضل‌هایی با احتمال ۱ برای  $(E_K^1)^{-1}$  می‌باشد که  $\beta \oplus \beta' \oplus \gamma \oplus \gamma' \neq 0$ . در نتیجه دو معادله‌ی زیر نمی‌تواند برقرار باشد:

$$E_K(X) \oplus E_K(X') = \delta \quad (7)$$

$$E_K(X \oplus \alpha) \oplus E_K(X' \oplus \alpha) = \delta' \quad (8)$$

بر اساس این قضیه در [۲۸] بیان می‌شود که تمایزگری به فرم نشان داده شده در شکل (۲) نمی‌تواند هرگز رخ دهد و تمایزگر بومرنگ ناممکن نامیده می‌شود. این تمایزگر را می‌توان به‌صورت  $(\Delta\delta, \Delta\delta') \leftrightarrow (\Delta\alpha, \Delta\alpha')$  نشان داد و تا زمانی که شرط  $\beta \oplus \beta' \oplus \gamma \oplus \gamma' \neq 0$  برقرار است ممکن است دو تفاضل برای  $E^0$  یا  $E^1$  مشابه باشند.

### حمله‌ی کشف کلید

در حمله‌ی بومرنگ ناممکن یک رمز قالبی  $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$  به‌صورت چهار زیررمز  $E = E^a \circ E^0 \circ E^1 \circ E^b$  در نظر گرفته می‌شود که  $E^0 \circ E^1$  دوره‌های تمایزگر بومرنگ ناممکن با تفاضل  $(\Delta\delta, \Delta\delta') \leftrightarrow (\Delta\alpha, \Delta\alpha')$  را نشان می‌دهد.  $E^a$  تعداد دوره‌های قبل از  $E^0$  و  $E^b$  تعداد دوره‌های بعد از  $E^1$  را نشان می‌دهد. در حمله‌ی بومرنگ ناممکن در سناریوی حمله‌ی متن اصلی انتخابی، برای مشخص کردن یک حدس از زیرکلیدهای استفاده شده در  $E^a$  و  $E^b$ ، این شرط بررسی می‌شود که آیا شرایط تفاضل مورد نیاز تمایزگر بومرنگ ناممکن توسط چهارتائی کاندید متشکل از دو جفت متن اصلی برآورده می‌شود یا خیر.

به‌طور خاص، فرض کنید که  $K_a$  یک حدس برای زیرکلید استفاده شده در  $E^a$  و  $K_b$  یک حدس برای زیرکلید استفاده شده در  $E^b$  است، سپس مهاجم بررسی می‌کند که آیا یک چهارتائی کاندید از جفت متن اصلی-متن رمز شده شناخته شده‌ی

گرفت. یک تمایزگر بومرنگ ناممکن کلیدمرتبط در شکل (۳) نشان داده شده‌است.

در حمله‌ی تفاضلی ناممکن کلیدمرتبط، دنباله‌ی تفاضلی زیرکلیدها با کمترین پیچیدگی جستجو می‌شود. در Simon32/64 با کلید ۴ کلمه‌ای می‌توان در دنباله‌ی تفاضلی زیرکلیدها از مسیری با سه زیرکلید ۰ متوالی استفاده نمود. در حمله‌ی تفاضلی ناممکن دنباله مشخصه‌ی تفاضلی در قسمتی از رمز با احتمال ۰ وجود ندارد و می‌توان از دو مسیر ناپیوسته در دو جهت برای رسیدن به تناقض استفاده نمود. درحالی‌که در این حمله برای اضافه کردن تفاضل‌های کلید، دنباله‌ی زیرکلید پیوسته است. در حمله‌ی بومرنگ ناممکن در دو زیررمز  $E^0$  و  $E^1$  مسیره‌های تفاضلی باید با احتمال ۱ به تناقض برسند. با توجه به اینکه اضافه کردن تفاضل زیرکلیدها برای رسیدن به احتمال ۱ منجر به افزایش پیچیدگی و کاهش تعداد دور مورد حمله می‌شود، از دنباله‌ی تفاضلی زیرکلید با سه ۰ متوالی استفاده می‌کنیم. در حمله‌ی بومرنگ ناممکن می‌توان در دو جهت از دو مشخصه‌ی تفاضلی ناپیوسته‌ی زیرکلید با سه زیرکلید ۰ متوالی برای افزایش تعداد دور مورد حمله استفاده نمود. در جدول (۲)، دنباله تفاضل زیرکلیدهای استفاده شده در حمله‌ی بومرنگ ناممکن کلیدمرتبط روی Simon32/64 آورده شده‌است.

جدول ۲. دنباله زیرکلیدهای استفاده شده در حمله بومرنگ ناممکن کلیدمرتبط روی رمز Simon32/64.

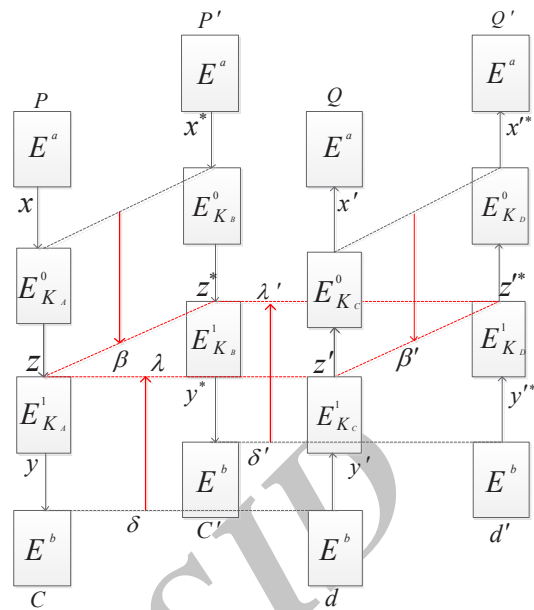
مشخصه‌ی تفاضلی زیرکلید Simon32/64			
$\Delta K_5$	6	$\nabla K_{13}$	0
$\Delta K_6$	0	$\nabla K_{14}$	0
$\Delta K_7$	0	$\nabla K_{15}$	0
$\Delta K_8$	0	$\nabla K_{16}$	6
$\Delta K_9$	6		
$\Delta K_{10}$	2,3		
$\Delta K_{11}$	0,14		
$\Delta K_{12}$	5,6,8,9,10		

بر اساس دنباله زیرکلیدهای یافته شده، تفاضل ورودی به‌گونه‌ای انتخاب می‌شود که حمله روی تعداد دور بیشتر و مشخصه‌ی دنباله‌ی تفاضلی با احتمال کمتر از  $2^{-32}$  ایجاد شود. در تفاضل ورودی از تفاضل کوتاه‌شده استفاده می‌نمائیم. در تفاضل‌های کوتاه‌شده هر بایت در تجزیه‌تحلیل می‌تواند تفاضل صفر یا غیرصفر داشته باشد. به‌صورت کلی تر بردار تفاضل کوتاه‌شده به‌صورت زیر تعریف می‌شود:

رشته  $\Delta$  شامل  $n$  بایت  $(\Delta_0, \Delta_1, \dots, \Delta_{n-1})$  را در نظر می‌گیریم. سپس بردار تفاضل  $X = (X_0, X_1, \dots, X_{N-1})$  متناظر  $\Delta$  به فرم زیر تعریف می‌شود:

$$X_i = \begin{cases} 0 & \text{if } \Delta_i = 0 \\ 1 & \text{otherwise} \end{cases} \quad (13)$$

شکل ۳. تمایزگر بومرنگ ناممکن کلیدمرتبط.



### حمله‌ی بومرنگ ناممکن کلیدمرتبط روی Simon32/64

نسخه‌ی ۳۲-بیتی رمز Simon از کلید ۶۴-بیتی با  $m=4$  استفاده می‌کند. هر دنباله زیرکلید، منحصراً کلید مخفی مشخصی را تولید می‌کند و بنابراین انتخاب زیرکلیدهای  $K_0, K_1, K_2, K_3$  در هر قسمت از دنباله‌ی زیرکلیدها نتیجه‌ی یکسانی می‌دهد. در ادامه جستجوی مشخصه‌ی زیرکلید و متن اصلی و سپس روال حمله بیان شده‌است.

#### جستجوی مشخصه‌ی تفاضلی ناممکن کلیدمرتبط

الگوریتم ماتسوئی روشی برای یافتن بهترین مسیر تفاضلی در تعداد دور داده شده‌است. در این روش بهترین مشخصه‌ی دور  $r$  با توجه به بهترین احتمالات مشخصه‌های دورهای  $1, \dots, r-1$  و تعداد مشخصه‌های دور  $r$  ساخته می‌شود. در این الگوریتم بازگشتی، تنها در صورتی مشخصه‌ای گسترش می‌یابد که ضرب احتمال آن در احتمال دورهای باقیمانده از بهترین احتمال همه‌ی دورهای قبلی بزرگتر باشد. در این روش برای هر مشخصه‌ی  $r-1$  اگر  $p_r \cdot p_{n-r}^{best} \geq p_n^*$  برقرار باشد، سپس یک دور گسترش می‌یابد [۳۵]. در [۳۶] الگوریتم ماتسوئی به‌عنوان مناسب‌ترین روش برای جستجوی مشخصه‌ی تفاضلی با حالت ۶۴-بیتی بیان شده و روی رمز DES آورده شده‌است.



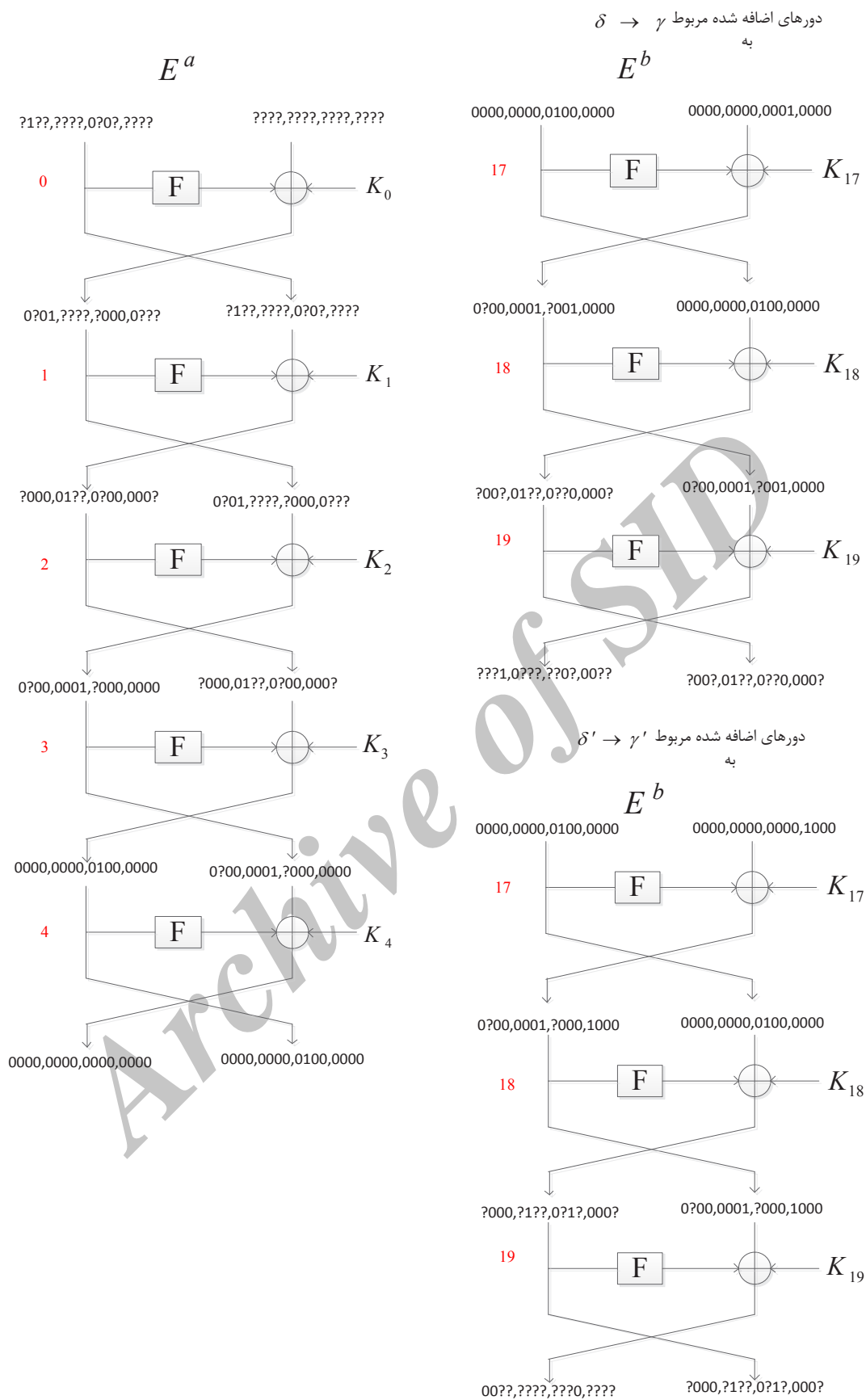
در رمز Simon به علت ویژگی جذب AND منطقی، بیت‌های نامشخص را بر اساس  $L_{((i+7) \bmod n), ((i-7) \bmod n)}$  معین می‌کنیم. در جدول (۳)، مشخصه‌ی بومرنگ ناممکن کلیدمرتبط روی ۱۲- دور رمز Simon32/64 نشان داده شده‌است. در جدول (۳) تفاضل‌های  $\alpha \rightarrow \beta$  و  $\delta \rightarrow \gamma$  روی زیررمزهای  $E^0$  و  $E^1$  آورده شده‌است. همان‌طور که دیده می‌شود، بیت‌های ۵ و ۱۲ سمت راست ورودی با احتمال ۱ متناقض می‌باشند. تفاضل‌های کلیدمرتبط  $\Delta\alpha \rightarrow \Delta\beta$  و  $\Delta\alpha' \rightarrow \Delta\beta'$  برای  $E^0$  هر دو یکسان در نظر گرفته شده‌اند. برای برقرارشدن شرط  $\beta \oplus \beta' \oplus \gamma \oplus \gamma' = 0$  مقادیر  $\gamma$  و  $\gamma'$  به‌گونه‌ای انتخاب شده‌اند که در بیت ۹ سمت چپ به تناقض می‌رسند و در نهایت شرط برقرار می‌شود؛ تناقض بین  $\gamma$  و  $\gamma'$  در جدول (۴) آورده شده‌است. دورهای اضافه‌شده به مشخصه‌ی ۱۲- دوری در شکل (۳) مشاهده می‌شود.

در حملات تفاضلی، تجزیه‌تحلیل کامل دو متن در نظر گرفته می‌شود ولی در تفاضل کوتاه‌شده، تفاضل‌ها به‌صورت جزئی تعیین می‌شوند و برخی از بیت‌ها به‌جای کل بلوک پیش‌بینی می‌شوند. در جستجوی دنباله‌ی تفاضلی ناممکن می‌توان از تفاضل‌های کوتاه‌شده استفاده کرد و در نتیجه انتشار به‌طور موثرتری مورد بررسی قرار می‌گیرد [۳۷]. برای بیان دنباله‌ی مشخصه‌ی تفاضلی ناممکن از تفاضل‌های کوتاه‌شده استفاده می‌کنیم که بر اساس ویژگی جذب AND منطقی ارائه‌شده در [۷] بیان می‌شوند.

ویژگی جذب Simon: به‌علت چرخش ۱ بیت و ۸ بیت موقعیت به سمت چپ در تابع دور Simon، عملیات AND منطقی با احتمال  $2^{-2}$  یک بیت فعال  $\Delta L_i$  را جذب می‌کند اگر و فقط اگر  $L_{((i+7) \bmod n), ((i-7) \bmod n)} = 0$  در دنباله‌ی تفاضلی ارائه‌شده بر اساس [۷]، تفاضل  $\Delta_{i,[j]}$  بیانگر تفاضل کوتاه‌شده است که بیت  $i$  فعال و مقادیر  $j$  نامشخص است.

جدول ۳. مشخصه‌ی ۱۲ دوری بومرنگ ناممکن کلیدمرتبط روی رمز Simon32/64.

دور	تفاضل سمت چپ ورودی	تفاضل سمت راست ورودی	تفاضل زیرکلید
0	$E^0$	0000000000000000	0000000001000000
1	$E^0$	0000000000000000	0000000000000000
2	$E^0$	0000000000000000	0000000000000000
3	$E^0$	0000000000000000	0000000000000000
4	$E^0$	0000000000000000	0000000001000000
5	$E^0$	0000000001000000	0000000000000000
6	$E^0$	0?000001?0001100	0000000001000000
7	$E^0$	?100?????0?1?????	0?000001?0001100
	$E^0$	????????????????	?100?????0?1?????
8	$E^1$	??0?010????0000?	???1?0???0?0?0?
9	$E^1$	0??00001??0?0000	??0?010????0000?
10	$E^1$	000?000001?00000	0??00001??0?0000
11	$E^1$	0000000000010000	000?000001?00000
	$E^1$	0000000001000000	0000000000010000



شکل ۴. دورهای قبل و بعد از مشخصه‌ی بومرنگ ناممکن کلیدمرتبط ۱۲-دور رمز Simon32/64.



جدول ۴. جدول بررسی تناقض بین  $\gamma'$  و  $\gamma$ .

		تفاضل سمت چپ ورودی	تفاضل سمت راست ورودی	تفاضل زیرکلید
$E^1$	$\delta'$	0000000001000000	0000000000001000	/
$E^1$		0000000000001000	0000?000001?0000	0000000001000000
$E^1$		0000?000001?0000	00??00001??0?000	0000000000000000
$E^1$		00??00001??0?000	??0?01?????0000	0000000000000000
$E^1$	$\gamma'$	0??0?01?????0000	????1?????0?0??	0000000000000000
$E^1$	$\gamma$	??0?010????0000?	???1?0????0?0?0?	0000000000000000
$E^1$		0??00001??0?0000	?0?010????0000?	0000000000000000
$E^1$		000?000001?00000	0??00001??0?0000	0000000000000000
$E^1$		0000000000010000	000?000001?00000	0000000001000000
$E^1$	$\delta$	0000000001000000	0000000000010000	/

**روال حمله بومرنگ ناممکن کلیدمرتبط روی رمز Simon32/64**

بعد از جستجوی مشخصه، روال حمله و پیچیدگی را در ادامه بیان می‌کنیم.

۱- همهی  $2^{32}$  متن اصلی را در نظر گرفته و آن‌ها را درون  $2^2$  ساختار قرار می‌دهیم که هر کدام شامل دو مجموعه‌ای با  $2^{29}$  متن اصلی است. ۴ ساختار بیان شده به شکل  $(x_1, x_2, \dots, x_{29})$  و  $(x_1, x_2, \dots, x_{29})$  می‌باشند که  $x_i$  ( $1 \leq i \leq 2$ ) مقادیر معین و  $?$  همهی مقادیر ممکن را می‌گیرند. هر ساختار در حدود  $2^{58}$  جفت متن اصلی تولید می‌کند که تفاضلی به شکل زیر دارند:

$$(0?1????? 0?0?????, ??????????????????)$$

بنابراین در مجموع  $2^{60}$  جفت متن اصلی با تفاضلی به این شکل می‌توانیم به دست بیاوریم.  $2^2$  ساختار  $S_i$  ( $i = 1, 2, 3, 4$ ) انتخاب می‌کنیم که یک ساختار  $S_i$  مجموعه‌ای از  $2^{29}$  متن اصلی  $P_{i,l}$  با ۳ بیت معین است و ۲۹ بیت باقیمانده هر مقدار ممکن را دریافت می‌کنند ( $l = 1, 2, \dots, 2^{29}$ ). در یک سناریوی حمله‌ی متن اصلی - انتخابی، همهی متن‌های رمز شده برای  $2^{29}$  متن اصلی در هر  $2^2$  ساختار را با کلیدهای  $K_A, K_B, K_C, K_D$  که  $K_A \oplus K_B = K_C \oplus K_D = (K_3 = \Delta_6, K_2 = 0, K_1 = 0, K_0 = 0)$  ساختار  $K_A \oplus K_C = K_B \oplus K_D = (K_3 = \Delta_6, K_2 = 0, K_1 = 0, K_0 = 0)$  رمزنگاری می‌کنیم. متن‌های رمز شده برای متن اصلی  $P_{i,l}$  که با کلیدهای  $K_A, K_B, K_C, K_D$  رمزنگاری شدند را به ترتیب با  $C_{i,l}, C_{i,l}^*, C_{i,l}, C_{i,l}^*$  مشخص می‌کنیم.

۲- برای جفت متن اصلی  $P_{i,l}$  مقدار  $\Delta F(L_0) \oplus R_0$  را محاسبه کرده و بررسی می‌کنیم که برابر با  $0?01,????,?000,0???$  می‌باشد یا خیر و متن‌هایی با این ویژگی را حفظ می‌کنیم.

۳- برای متن‌های اصلی باقیمانده ۹ بیت از زیرکلید باقیمانده  $\Delta F(L_1) \oplus R_1$  را محاسبه کرده و بررسی می‌کنیم که

آیا برابر با  $0000,01??,0?00,000?$  می‌باشد یا خیر.

۴- برای متن‌های اصلی باقیمانده ۱۴ بیت از زیرکلیدهای  $K_0^g = \{0,1,2,3,7,8,9,15\}$  و  $K_1^g = \{6,7,8,13,14,15\}$  را حدس می‌زنیم. برای هر جفت باقیمانده  $\Delta F(L_2) \oplus R_2$  را محاسبه کرده و بررسی می‌کنیم که آیا برابر با  $0?00,0001,?000,0000$  می‌باشد یا خیر.

۵- برای متن‌های اصلی باقیمانده ۱۳ بیت از زیرکلیدهای  $K_1^g = \{4,5,6,12,13,14\}$ ,  $K_2^g = \{0,1,5,7,14,15\}$ ,  $K_0^g = \{12\}$  را حدس می‌زنیم. برای هر جفت باقیمانده  $\Delta F(L_3) \oplus R_3$  را محاسبه کرده و بررسی می‌کنیم که آیا برابر با  $0000,0000,0100,0000$  می‌باشد یا خیر.

۶- برای متن‌های اصلی باقیمانده ۳ بیت از زیرکلیدهای  $K_1^g = \{11\}$  و  $K_2^g = \{13\}$ ,  $K_3^g = \{15\}$  را حدس می‌زنیم. برای هر جفت باقیمانده  $\Delta F(L_4) \oplus R_4$  را محاسبه کرده و بررسی می‌کنیم که آیا برابر با  $0000,0000,0000,0000$  می‌باشد یا خیر.

۷- مقدار  $(R_5 \oplus L_4), (R_5 \oplus L_4) \oplus \Delta F(L_4)$  را از طریق دورهای ۴- و با زیرکلیدهای زیر

$$(K_0^g \oplus \Delta_2, K_1^g \oplus \Delta_{2,4,5,6}, K_2^g \oplus \Delta_{4,6}, K_3^g \oplus \Delta_{5,6})$$

رمزگشایی نموده و آن را با  $\bar{P}_{i,l}$  نشان می‌دهیم. آن را در  $S_i$  پیدا می‌کنیم. متن‌های رمز شده  $\bar{P}_{i,l}$  تحت کلیدهای  $K_A, K_B, K_C, K_D$  را به ترتیب با  $\bar{C}_{i,l}, \bar{C}_{i,l}^*, \bar{C}_{i,l}, \bar{C}_{i,l}^*$  نمایش می‌دهیم.

۸- همهی  $(C_{i,l}, C_{i,l}^*)$  و  $(\bar{C}_{i,l}^*, \bar{C}_{i,l}^*)$  را تا خروجی دور ۱۹ رمزگشایی می‌کنیم؛ سپس  $C_{i,l} \oplus C_{i,l}^*$  را به دست آورده و جفت‌هایی که مقدار تفاضل سمت راست آن‌ها  $\Delta F(C_{i,l}(R_{20}) \oplus C_{i,l}^*(R_{20})) \oplus (C_{i,l}(L_{20}) \oplus C_{i,l}^*(L_{20}))$  و برابر با  $(0?00,0001,?001,0000)$  می‌باشد را حفظ می‌کنیم. در ادامه  $\bar{C}_{i,l}^* \oplus \bar{C}_{i,l}^*$  را به دست آورده و جفت‌هایی که مقدار تفاضل آن‌ها  $\Delta F(\bar{C}_{i,l}^*(R_{20}) \oplus \bar{C}_{i,l}^*(R_{20})) \oplus (\bar{C}_{i,l}^*(L_{20}) \oplus \bar{C}_{i,l}^*(L_{20}))$  در سمت راست برابر با  $(0?00,0001,?000,1000)$  می‌باشد را حفظ می‌کنیم.

۹- بر اساس زیرکلیدهای  $K_0^g, K_1^g, K_2^g, K_3^g$  حدس زده شده، ۸ بیت

کلید ۶۴-بیتی حدس زده شده کلید کاربر ۲۰ دور رمز Simon32/64 باشد در این صورت مراحل تمام می‌شود.

### تجزیه تحلیل پیچیدگی حمله

حمله به  $2^{32}$  متن اصلی انتخابی نیاز دارد که پیچیدگی زمانی آن برابر با  $2^{59.68}$  رمزنگاری ۲۰-دور رمز Simon32/64 است. در مرحله‌ی (۱)، جفت متن‌های رمز شده‌ی متناظر برای همه‌ی جفت متن‌های اصلی را به دست می‌آوریم. برای هر جفت متن رمز شده بررسی تفاضل‌هایی به شکل  $(????10?????00??)$ ،  $(????01??0??0000?)$  برای خروجی کشف کلید مشخصه اول و تفاضل به شکل  $(????0000?1??0?1?000?)$ ،  $(00?????????0????)$  برای خروجی کشف کلید مشخصه دوم را حفظ می‌کنیم. جفت متن‌های رمز شده‌ای که شرط در هیچ دو گروه را برآورده نمانند، حذف می‌شوند. تعداد  $2^{46} \times 2^{-14} = 2^{46}$  جفت تقریباً برای گروه اول و  $2^{48} \times 2^{-12} = 2^{48}$  جفت تقریباً برای گروه دوم باقی می‌ماند. پیچیدگی زمانی این مرحله برابر است با:

$$2 \times 2^{32} \times 2^4 \times \frac{1}{20} \approx 2^{32.68}$$

در مرحله‌ی (۲)، تعداد جفت‌های باقیمانده باتوجه به ۷ بیت شرط، برابر با  $2^{39} \times 2^{-7} = 2^{46}$  در گروه اول و  $2^{48} \times 2^{-7} = 2^{41}$  در گروه دوم می‌باشد. پیچیدگی زمانی این مرحله برابر است با:

$$2 \times 2^{46} \times \frac{1}{20} + 2 \times 2^{48} \times \frac{1}{20} \approx 2^{44.68}$$

در مرحله‌ی (۳-۷)، تعداد جفت‌های باقیمانده باتوجه به ۲۲ بیت شرط، برابر با  $2^{17} \times 2^{-8-7-5-2} = 2^{17}$  در گروه اول و  $2^{19} \times 2^{-8-7-5-2} = 2^{19}$  در گروه دوم می‌باشد. در حدود  $2^{17}$  جفت متن اصلی برای هر حدس از ۳۹ بیت زیرکلیدهای  $K_0^g, K_1^g, K_2^g, K_3^g$  در گروه اول و  $2^{19}$  جفت متن اصلی در گروه دوم باقی می‌ماند که تفاضل آن‌ها تحت کلیدهای حدس زده شده در خروجی دور پنجم به صورت  $(0000000000000000)$  می‌باشد. بنابراین در حدود  $2^{37} \approx \frac{2^{19 \times 2}}{2} = 2^{37}$  چهارتایی کاندید برای هر حدس از زیرکلیدهای  $K_0^g, K_1^g, K_2^g, K_3^g$  تولید می‌شود. در مرحله‌ی (۸) بررسی می‌شود که تفاضل بین  $(C_{i,l}, C'_{i,l})$  در چهارتایی کاندید به شکل  $(0?00,0001,?001,0000)$  و تفاضل بین  $(\bar{C}'_{i,l}, \bar{C}_{i,l})$  در چهارتایی کاندید به شکل  $(0?00,0001,?000,1000)$  باشد. که تعداد چهارتایی‌های باقیمانده برابر با  $2^{37} \times 2^{-9} + 2^{37} \times 2^{-12} \approx 2^{25}$  می‌شود. پیچیدگی زمانی این مرحله برابر است با:

$$2 \times 2^{19} \times 2^{39} \times \frac{1}{2} \times \frac{1}{20} \approx 2^{53.68}$$

در مرحله‌ی (۹)، هر جفت  $(T_{i_1, l_1}, T'_{i_2, l_2})$  شرط را با احتمال  $2^{-7}$  و  $(\bar{T}_{i_1, l_1}, \bar{T}'_{i_2, l_2})$  شرط را با احتمال  $2^{-7}$  در چهارتایی کاندید ملاقات می‌کنند، بنابراین در حدود  $2^{25} \times 2^{-14} = 2^{11}$  چهارتایی

زیرکلیدهای  $\{0,1,5,7,11,13,14,15\} = K_{19}$  را محاسبه کرده و همه‌ی  $C'_{i,l}$  و  $C_{i,l}$  باقیمانده را تا خروجی دور ۱۸ رمزگشایی می‌کنیم؛ آن‌ها را به ترتیب با  $T'_{i,l}$  و  $T_{i,l}$  نشان می‌دهیم. در تفاضل مربوط به  $\delta' \rightarrow \gamma'$  و بر اساس زیرکلیدهای  $K_0^g, K_1^g, K_2^g, K_3^g$  حدس زده شده، ۸ بیت زیرکلیدهای  $\{0,1,5,7,10,12,14,15\} = K_{19}$  را محاسبه کرده و همه‌ی  $\bar{C}'_{i,l}$  و  $\bar{C}_{i,l}$  را برای به دست آوردن مقادیر متناظر خروجی دور ۱۸ رمزگشایی می‌کنیم؛ آن‌ها را با به ترتیب با  $\bar{T}'_{i,l}$  و  $\bar{T}_{i,l}$  نشان می‌دهیم. مقادیر  $(T_{i,l}, T'_{i,l}, \bar{T}_{i,l}, \bar{T}'_{i,l})$  را در یک جدول هش ذخیره می‌کنیم. چهارتایی‌های  $(T_{i_1, l_1}, \bar{T}_{i_1, l_1}, T'_{i_2, l_2}, \bar{T}'_{i_2, l_2})$  انتخاب می‌کنیم. سپس  $T_{i_1, l_1} \oplus T'_{i_2, l_2}$  را به دست آورده و تنها جفت‌هایی که تفاضل  $(0000,0000,0100,0000)$  در  $\Delta F(R_{19}) \oplus L_{19}$  دارند را حفظ می‌کنیم. سپس  $\bar{T}_{i_1, l_1} \oplus \bar{T}'_{i_2, l_2}$  را به دست آورده و تنها آن‌هایی که  $\Delta F(R_{19}) \oplus L_{19}$  برابر با  $(0000,0000,0100,0000)$  دارند را حفظ می‌کنیم. که  $1 \leq i_1 \leq i_2 \leq 2^2$  و  $1 \leq l_1 \leq l_2 \leq 2^{29}$  است. اگر ۶ یا بیشتر چهارتایی  $(T_{i_1, l_1}, \bar{T}_{i_1, l_1}, T'_{i_2, l_2}, \bar{T}'_{i_2, l_2})$  این مرحله را عبور دهد، مرحله‌ی بعد را با چهارتایی‌هایی که شرط را برآورده کردند انجام می‌دهیم؛ در غیر این صورت، مرحله‌ی (۳-۶) را با حدس دیگری تکرار می‌کنیم.

۱۰- بر اساس زیرکلیدهای  $K_0^g, K_1^g, K_2^g, K_3^g$  حدس زده شده، ۲ بیت زیرکلیدهای  $\{13,15\} = K_{18}$  را محاسبه کرده و برای هر چهارتایی باقیمانده  $(T_{i_1, l_1}, \bar{T}_{i_1, l_1}, T'_{i_2, l_2}, \bar{T}'_{i_2, l_2})$  همه‌ی  $T_{i_1, l_1}$  و  $T'_{i_2, l_2}$  را برای به دست آوردن مقدار خروجی دور ۱۷ رمزگشایی کرده و بررسی می‌کنیم که آیا  $\Delta F(R_{18}) \oplus L_{18}$  برابر با  $0000,0000,0001,0000$  می‌باشد یا خیر. اگر شرط برقرار نباشد این مرحله را با چهارتایی دیگر امتحان می‌کنیم؛ در تفاضل مربوط به  $\delta' \rightarrow \gamma'$  و بر اساس زیرکلیدهای  $K_0^g, K_1^g, K_2^g, K_3^g$  حدس زده شده، ۲ بیت زیرکلیدهای  $\{13,15\} = K_{18}$  را محاسبه کرده و همه‌ی  $\bar{T}_{i_1, l_1}$  و  $\bar{T}'_{i_2, l_2}$  را برای به دست آوردن خروجی دور ۱۷ رمزگشایی می‌کنیم و بررسی می‌کنیم که آیا  $\Delta F(R_{18}) \oplus L_{18}$  برابر با  $0000,0000,0000,1000$  می‌باشد یا خیر. اگر شرط برقرار نباشد این مرحله را با چهارتایی دیگر امتحان می‌کنیم. اگر ۶ یا بیشتر چهارتایی این مرحله را عبور دهد، مرحله‌ی بعد را انجام می‌دهیم؛ در غیر این صورت، مرحله‌ی (۳-۶) را با حدس دیگری تکرار می‌کنیم.

۱۱- مقادیر  $K_0 = \{0 \sim 15\}$ ،  $K_1 = \{0 \sim 9, 11, 13 \sim 15\}$ ،  $K_2 = \{0, 1, 5, 7, 11, 13 \sim 15\}$  و  $K_3 = \{15\}$  حدس زده شده‌اند. جستجوی جامع برای ۲۵ بیت کلید باقیمانده انجام می‌شود. اگر

حمله به کار ببریم و تعداد دور حمله شده نسبت به حالت تفاضلی ناممکن را افزایش دهیم. الگوریتم رمز قالبی AES، از قوی ترین و پرکاربردترین الگوریتم های رمزنگاری با ساختار جایگشت-جایگذاری می باشد. با وجود اینکه حملات خطی و تفاضلی روی دورهای محدود این رمز انجام شده اند؛ اما حمله ی بومرنگ کلیدمرتبط روی دور کامل AES-256 صورت گرفته است [۳۸]. حمله ی خطی روی ۲۳ دور از رمز Simon32/64 و حمله ی کلیدمرتبط ارائه شده در این مقاله روی ۲۰ دور از آن، نشان می دهد که زمانبند کلید این رمز قالبی در برابر حملات کلیدمرتبط مقاوم تر طراحی شده است و ادعای طراحان آن مبنی بر مقام بودن زمانبند کلید آن اثبات می شود. حمله ی بومرنگ ناممکن کلیدمرتبط را می توان برای ارزیابی امنیت رمزهایی با ساختار جایگشت-جایگذاری و نیز بررسی نقاط ضعف الگوریتم زمانبند کلید آن ها به کار برد.

### مرجع ها

- [1]. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., and Wingers, L.. "The SIMON and SPECK Families of Lightweight Block Ciphers." IACR Cryptology ePrint Archive, 2013, 404, 2013.
- [2]. Abdelraheem, M. A. A. Cryptanalysis of Some Lightweight Symmetric Ciphers (Doctoral dissertation, The Technical University of Denmark), December 2012.
- [3]. Knudsen, L. R., and Robshaw, M. The block cipher companion. Springer Science & Business Media, 2011.
- [4]. Borghoff, J. Cryptanalysis of Lightweight Ciphers (Doctoral dissertation, The Technical University of Denmark), 2010.
- [5]. "Cryptography," 9 Jun 2013. [Online]. Available: <http://en.wikipedia.org/wiki/Cryptography>. [Accessed 1 March 2016].
- [6]. Biham, E., and Shamir, A. "Differential cryptanalysis of Feal and N-hash." In Advances in Cryptology—EUROCRYPT'91 (pp. 1-16). Springer Berlin Heidelberg, January 1991.
- [7]. Abed, F., List, E., Lucks, S., and Wenzel, J. "Differential and linear cryptanalysis of reduced-round SIMON." Cryptology ePrint Archive, Report 2013/526, 2013.
- [8]. Biham, E. "New types of cryptanalytic attacks using related keys." Journal of Cryptology, 7(4), 229-246, 1994.
- [9]. Knudsen, L. R. "Cryptanalysis of LOKI 91." In Advances in Cryptology—AUSCRYPT'92 (pp. 196-208). Springer Berlin Heidelberg, January 1993.
- [10]. Bellare, M., and Kohno, T. "A theoretical treatment of related-key attacks: RKA-PRPs, RKA-

کاندید به صورت  $(T_{i_1, l_1}, \bar{T}_{i_1, l_1}^*, T'_{i_2, l_2}, \bar{T}_{i_2, l_2}^*)$  بعد از این مرحله برای هر حدس از زیرکلیدهای  $K_0^g, K_1^g, K_2^g, K_3^g$  باقی می ماند. پیچیدگی زمانی این مرحله برابر است با:

$$2 \times 2^{25} \times 2^{39} \times \frac{1}{2} \times \frac{1}{20} \approx 2^{59.68}$$

در مرحله ی (۱۰) و (۱۱)، هر جفت  $(T_{i_1, l_1}, T'_{i_2, l_2})$  شرط را با احتمال  $2^{-2}$  و  $(\bar{T}_{i_1, l_1}, \bar{T}_{i_2, l_2}^*)$  شرط را با احتمال  $2^{-2}$  در چهارتایی کاندید ملاقات می کنند، بنابراین در حدود  $2^{11} \times 2^{-4} = 2^7$  چهارتایی کاندید به صورت  $(T_{i_1, l_1}, \bar{T}_{i_1, l_1}^*, T'_{i_2, l_2}, \bar{T}_{i_2, l_2}^*)$  بعد از این مرحله برای هر حدس از زیرکلیدهای  $K_0^g, K_1^g, K_2^g, K_3^g$  باقی می ماند. برای ۲۵ بیت باقیمانده از کلید جستجوی جامع انجام می شود، در نتیجه پیچیدگی زمانی این مرحله برابر است با:

$$2 \times 2^{11} \times 2^{39} \times \frac{1}{2} \times \frac{1}{20} + 2^{25} \approx 2^{45.68}$$

بنابراین، حمله ی بومرنگ ناممکن کلیدمرتبط با پیچیدگی زمانی  $2^{59.68}$  رمزنگاری ۲۰-دور رمز Simon32/64 انجام می شود.

### نتیجه گیری

در این مقاله، برای اولین بار یک حمله ی بومرنگ ناممکن کلیدمرتبط روی ۲۰-دور کاهش یافته ی رمز قالبی Simon32/64 را ارائه کردیم. تاکنون تنها دو حمله ی کلیدمرتبط روی Simon32/64 ارائه شده است؛ ابتدا عابد و همکارانش<sup>۱۶</sup> در [۱۵] روی ۱۴-دور از این نسخه حمله ی تفاضلی کلیدمرتبط و سپس در [۷] یک حمله ی مستطیلی کلیدمرتبط روی ۱۸-دور آن انجام داده اند.

همان طور که بیان کردیم، یک رمز قالبی مقاوم نسبت به حمله ی نوع-بومرنگ لزوماً در مقابل حمله ی بومرنگ ناممکن مقاوم نمی باشد. حمله ی بومرنگ ناممکن (کلیدمرتبط) انتخاب های مختلفی برای تفاضل ها (کلیدمرتبط) و متن های اصلی مورد نیاز ایجاد می کند. در تمایزگر نوع-بومرنگ، خروجی یک دور میانه ی رمز با توزیع یکنواخت و مستقل از دورهای قبلی در نظر گرفته می شود. در حالی که، در تمایزگر بومرنگ ناممکن اغلب توزیع یکنواخت و استقلال از دورهای قبلی در نظر گرفته نمی شود. بنابراین به نظر می رسد یک تمایزگر بومرنگ ناممکن از تمایزگر نوع-بومرنگ مناسب تر است. در حمله ی کلیدمرتبط با توجه به اینکه از ارتباط بین کلیدها مطلع هستیم با عملیات XOR، عبارت  $(C \oplus (Z_j)_i)$  از ساختار زمانبند کلید حذف می شود و پیچیدگی ساختار زمانبند برای تولید زیرکلیدها کاهش می یابد. انعطاف پذیری در انتخاب تفاضل های کلید امکان شکست دورهای بیشتری از رمز قالبی با استفاده از حمله ی بومرنگ تفاضلی ناممکن را فراهم می سازد. بنابراین ما با استفاده از ویژگی حملات بومرنگ توانستیم دو دنباله مسیر زیرکلید متفاوت را برای انجام

- Linear Cryptanalysis of Reduced-round SIMON.”, 2014.
- [25]. Song, L., Hu, L., Ma, B., and Shi, D. “Match Box Meet-in-the-Middle Attacks on the SIMON Family of Block Ciphers.” In *Lightweight Cryptography for Security and Privacy* (pp. 140-151). Springer International Publishing, 2015.
- [26]. Chen, Z., Wang, N., and Wang, X. “Impossible Differential Cryptanalysis of Reduced Round SIMON.”, 2015.
- [27]. Chen, H., and Wang, X. “Improved linear hull attack on round-reduced simon with dynamic key-guessing techniques.” *Cryptology ePrint Archive, Report 2015/666*, July 2015. <http://eprint.iacr.org/2015/666>. Pdf, 2015.
- [28]. Lu, J. *Cryptanalysis of block ciphers* (Doctoral dissertation, Royal Holloway, University of London), July 2008. <http://www.rhul.ac.uk/mathematics/techreports>
- [29]. Biham, E., and Keller, N. “Cryptanalysis of reduced variants of Rijndael.” In *3rd AES Conference*, New York, USA, April 2000.
- [30]. Wagner, D. “The boomerang attack.” In *Fast Software Encryption* (pp. 156-170). Springer Berlin Heidelberg, January 1999.
- [31]. Choy, J., and Yap, H. “Impossible boomerang attack for block cipher structures.” In *Advances in Information and Computer Security* (pp. 22-37). Springer Berlin Heidelberg, 2009.
- [32]. Biham, E. “New types of cryptanalytic attacks using related keys.” *Journal of Cryptology*, 7(4), 229-246, 1994.
- [33]. Kelsey, J., Schneier, B., and Wagner, D. “Related-key cryptanalysis of 3-way, biham-des, cast, des-x, newdes, rc2, and tea.” *Information and Communications Security*, 233-246, 1997.
- [34]. Biham, E. “New types of cryptanalytic attacks using related keys.” *Journal of Cryptology*, 7(4), 229-246, 1994.
- [35]. Matsui, M. “On correlation between the order of S-boxes and the strength of DES.” In *Advances in Cryptology—EUROCRYPT’94* (pp. 366-375). Springer Berlin Heidelberg, January 1995.
- [36]. Biryukov, A., and Nikolić, I. “Search for related-key differential characteristics in DES-like ciphers.” In *Fast Software Encryption* (pp. 18-34). Springer Berlin Heidelberg, January 2011.
- [37]. Biham, E., Biryukov, A., and Shamir, A. “Miss in the Middle Attacks on IDEA and Khufu.” In *Fast Software Encryption* (pp. 124-138). Springer Berlin Heidelberg, January 1999.
- [38]. Biryukov, A., and Khovratovich, D. “Related-key cryptanalysis of the full AES-192 and AES-256.” In *Advances in Cryptology—ASIACRYPT 2009* (pp. 1-18). Springer Berlin Heidelberg, 2009.
- PRFs, and applications.” In *Advances in Cryptology—EUROCRYPT 2003* (pp. 491-506). Springer Berlin Heidelberg, 2003.
- [11]. Biryukov, A., and Khovratovich, D. “Related-key cryptanalysis of the full AES-192 and AES-256.” In *Advances in Cryptology—ASIACRYPT 2009* (pp. 1-18). Springer Berlin Heidelberg, 2009.
- [12]. Daemen, J., and Rijmen, V. “The design of Rijndael: AES-the advanced encryption standard.” Springer Science & Business Media, 2013.
- [13]. Wagner, D. “The boomerang attack.” In *Fast Software Encryption* (pp. 156-170). Springer Berlin Heidelberg, January 1999.
- [14]. Alizadeh, J., Bagheri, N., Gauravaram, P., Kumar, A., and Sanadhya, S. K. “Linear Cryptanalysis of Round Reduced SIMON.” *IACR Cryptology ePrint Archive*, 2013, 663, 2013.
- [15]. Abed, F., List, E., Lucks, S., and Wenzel, J. “Differential Cryptanalysis of Reduced-Round Simon.” Available: [citeseerx.ist.psu.edu](http://citeseerx.ist.psu.edu), 2013.
- [16]. Alkhzaimi, H., and Lauridsen, M. M. “Cryptanalysis of the SIMON Family of Block Ciphers.” *IACR Cryptology ePrint Archive*, 2013, 543, 2013.
- [17]. Ahmadian, Z., Rasoolzadeh, S., Salmasizadeh, M., and Aref, M. R. “Automated Dynamic Cube Attack on Block Ciphers: Cryptanalysis of SIMON and KATAN.”, 2014.
- [18]. Wang, Q., Liu, Z., Varici, K., Sasaki, Y., Rijmen, V., and Todo, Y. “Cryptanalysis of Reduced-round SIMON32 and SIMON48.” In *Progress in Cryptology-INDOCRYPT 2014* (pp. 143-160). Springer International Publishing, 2014.
- [19]. Biryukov, A., Roy, A., and Velichkov, V. “Differential analysis of block ciphers SIMON and SPECK.” In *Fast Software Encryption* (pp. 546-570). Springer Berlin Heidelberg, March 2014.
- [20]. Boura, C., Naya-Plasencia, M., and Suder, V. “Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon (Full Version).”, 2014.
- [21]. Alizadeh, J., Alkhzaimi, H. A., Aref, M. R., Bagheri, N., Gauravaram, P., Kumar, A., and Sanadhya, S. K. “Cryptanalysis of SIMON variants with connections.” In *Radio Frequency Identification: Security and Privacy Issues* (pp. 90-107). Springer International Publishing, 2014.
- [22]. Wang, N., Wang, X., Jia, K., and Zhao, J. “Improved differential attacks on reduced SIMON versions.” *Cryptology ePrint Archive, Report 2014/448*, 2014.
- [23]. Wang, N., Wang, X., Jia, K., and Zhao, J. “Differential Attacks on Reduced SIMON Versions with Dynamic Key-guessing Techniques.”, 2014.
- [24]. Abdelraheem, M. A. A., Alizadeh, J., Alkhzaimi, H. A., Aref, M. R., Bagheri, N., Gauravaram, P., and Lauridsen, M. M. “Improved