حمله‌ی بومرنگ ناممکن کلیدمرتبط روی دور کاهش‌یافته‌ی رمز قالبی Simon32/64

فهیمه عظیمی [۱]، نصور باقری [۲]

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

۲استادیار دانشکده مهندسی برق، دانشگاه تربیت دبیر شهید رجائی، Nbagheri@srttu.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 درنظر 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 اخیرًا توسط NSA به‌صورت امن و انعطاف‌پذیر برای عملکرد مناسب درمحیط‌های محدود سخت‌افزاری و در ده نسخه طراحی شده‌است. زمانبند کلید Simon در برابر حملات کلیدمرتبط، مقاوم طراحی شده‌است. در این مقاله برای اولین‌بار حمله‌ی بومرنگ ناممکن کلیدمرتبط روی ۲۰ دور کاهش‌یافته رمز سبک‌وزن Simon32/64انجام شده‌است.

کلیدواژه

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

مقدمه

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 [۱]، رمزهای کلیدعمومی نامتقارن [۲] و توابع چکیده‌ساز [۳] 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 بدون‌اتصال 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 NSA [۴] دو خانواده‌ی رمز بسیار سبک‌وزن 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 شبکه های جایگشت-جایگذاری [۵] 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 [۲-۴].

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 [۶] می‌باشد که اولین‌بار توسط بیهام [۷] و شمیر [۸] روی رمز FEAL انجام شد [۶]. ایده‌ی اصلی حملات تفاضلی، مطالعه‌ی

1 Symmetric or Secret-Key Algoritm
2 Public-Key Algoritm
3 Hash Function
4 The National Security Agency

5 Substitution-permutation Network
6 Differential Cryptanalysis
7 Biham
8 Shamir

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. درصورتی‌که 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 رمزشده 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].

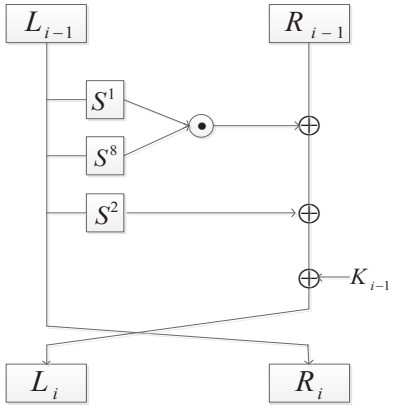
یکی از انواع حملات روی رمزهای قالبی، حملات کلیدمرتبط[۹] است که مهاجم می‌تواند عملیات رمز را روی کلیدهای مختلف اما ناشناخته بررسی کند. در حمله‌ی کلیدمرتبط هر چند کلیدها برای مهاجم ناشناخته هستند اما روابط ریاضی بین آن‌ها شناخته شده‌است. با شناخت روابط بین کلیدها مهاجم با استفاده از نقاط ضعف الگوریتم زمانبندی کلید[۱۰] و الگوریتم رمزنگاری، کلید مخفی را به‌دست می‌آورد [۹-۸]. در دهه‌ی گذشته حملات کلیدمرتبط از جهت نظری و عملی مورد مطالعه قرار گرفته‌اند [۱۱-۱۰]و آسیب‌ناپذیری در برابر حملات کلیدمرتبط به‌عنوان یکی از اهداف امنیت در طراحی رمزهای قالبی مدرن درنظر گرفته شده‌است [۱۲]. استفاده از حملات کلیدمرتبط همراه با حملات دیگری مانند حمله‌ی تفاضلی و بومرنگ پیچیدگی این حمله را کاهش می‌دهد. باتوجه به کاهش احتمال گسترش دنباله‌ی تفاضلی روی تعداد دورهای بیشتر رمز، نوعی حمله‌ی تفاضلی به‌نام بومرنگ[۱۱] توسط واگنر[۱۲] [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 چهارتائی 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].

باتوجه به اهمیت رمزهای سبک‌وزن برای استفاده در محیط‌های محدود و کاربرد وگسترش 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 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[۱۳] روی نسخه‌ی Simon32/64 می‌پردازیم. در پایان، نتیجه‌گیری در بخش ۵ آورده می‌شود.

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

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 Simon2n/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 :

$$Round_K(L_i,R_i) = \left(R_{i-1} \oplus \left((1 \lll L_{i-1} \odot 8 \lll L_{i-1}) \oplus (2 \lll L_{i-1})\right) \oplus K_{i-1}, L_{i-1}\right) \quad (۱)$$

تابع رمزگشایی :

$$Round_K^{-1}(L_i,R_i) = \left(R_{i-1}, L_{i-1} \oplus \left((1 \lll R_{i-1} \odot 8 \lll R_{i-1}) \oplus (2 \lll R_{i-1})\right) \oplus K_{i-1}\right) \quad (۲)$$

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 :

$$K_i = (K_{i-1} \ggg 3 \oplus K_{i-2}) \oplus (K_{i-1} \ggg 4) \oplus (C \oplus (Z_j)_i) \quad (۳)$$

13 Related-key Impossible Boomerang Attack

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 = 0Xff….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 به‌کار 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 تفاضلی، عامل مهمی در طراحی رمزهای قالبی درنظر گرفته می‌شود. با این‌حال، 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.

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

Simon32/64 (Round=32)						
	نام حمله	تعداد دور حمله شده	پیچیدگی زمانی	پیچیدگی داده‌ای	سال	مرجع
۱	حمله‌ی خطی	۱۱	-	$2^{۲۳}$	۲۰۱۳	[۷]
۲	حمله‌ی خطی	۱۲	-	$2^{۳۱}$	۲۰۱۳	[۱۴]
۳	حمله‌ی تفاضلی ناممکن	۱۳	$2^{۵۰,۱}$	$2^{۲۹,۶}$	۲۰۱۳	[۷]
۴	حمله‌ی تفاضلی ناممکن	۱۳	$2^{۵۰,۱}$	$2^{۳۰}$	۲۰۱۳	[۱۵]
۵	حمله‌ی کلیدمرتبط تفاضلی	۱۴	$2^{۴۳,۷}$	$2^{۲۹,۶}$	۲۰۱۳	[۱۵]
۶	حمله‌ی تفاضلی ناممکن	۱۴	$2^{۴۴,۱۸۳}$	$2^{۴۳,۲۹۱}$	۲۰۱۳	[۱۶]
۷	حمله‌ی تفاضلی	۱۶	$2^{۴۶,۴۸۱}$	$2^{۴۹,۴۸۱}$	۲۰۱۳	[۱۶]
۸	حمله‌ی تفاضلی	۱۸	$2^{۴۶}$	$2^{۳۱,۲}$	۲۰۱۳	[۱۵]
۹	حمله‌ی مستطیلی کلیدمرتبط	۱۸	$2^{۵۴,۵۵}$	$2^{۲۰,۸۲}$	۲۰۱۳	[۷]
۱۰	حمله‌ی مکعبی پویا	۱۸	$2^{۵۱}$	$2^{۳۲}$	۲۰۱۴	[۱۷]
۱۱	حمله‌ی تفاضلی ناممکن	۱۸	$2^{۶۱,۱۴}$	$2^{۳۲}$	۲۰۱۴	[۱۸]
۱۲	حمله‌ی تفاضلی	۱۹	$2^{۴۲}$	$2^{۳۱}$	۲۰۱۴	[۱۹]
۱۳	حمله‌ی تفاضلی ناممکن	۱۹	$2^{۶۲,۵۶}$	$2^{۳۲}$	۲۰۱۴	[۲۰]
۱۴	حمله‌ی تفاضلی ناممکن	۱۹	$2^{۶۲,۵۶}$	$2^{۳۲}$	۲۰۱۴	[۲۰]
۱۵	حمله‌ی پوش خطی	۲۰	$2^{۴۶}$	$2^{۳۱}$	۲۰۱۴	[۲۱]
۱۶	حمله‌ی تفاضلی	۲۱	$2^{۴۶}$	$2^{۳۱}$	۲۰۱۴	[۲۲]
۱۷	حمله‌ی خطی همبستگی صفر	۲۰	$2^{۵۶,۹۶}$	$2^{۳۲}$	۲۰۱۴	[۱۸]
۱۸	حمله‌ی تفاضلی	۲۱	$2^{۵۵,۲۵}$	$2^{۳۱}$	۲۰۱۴	[۲۳]
۱۹	حمله‌ی پوش خطی	۲۱	$2^{۵۵,۵۶}$	$2^{۳۰,۵۶}$	۲۰۱۴	[۲۴]
۲۰	حمله‌ی جدائی‌ناپذیر	۲۱	$2^{۶۳}$	$2^{۳۱}$	۲۰۱۴	[۱۸]
۲۱	حمله‌ی ملاقات در میانه	۱۸	$2^{۶۲,۵۷}$	-	۲۰۱۵	[۲۵]
۲۲	حمله‌ی تفاضلی ناممکن	۱۹	$2^{۵۸,۹۱۶}$	$2^{۳۲}$	۲۰۱۵	[۲۶]
۲۳	حمله‌ی پوش خطی	۲۳	-	$2^{۳۱,۱۶}$	۲۰۱۵	[۲۷]
۲۴	حمله‌ی بومرنگ ناممکن کلیدمرتبط	۲۰	$2^{۶۳,۶۸}$	$2^{۳۲}$	۲۰۱۶	[بخش ۴]

حمله‌ی بومرنگ نامکن

حمله‌ی بومرنگ نامکن در سال ۲۰۰۸ توسط جیگیانگ لو[14] در پایان‌نامه‌ی دکتری وی پیشنهاد شده‌است [۲۸]. این حمله یک توسعه‌ی جدید از حملات تفاضلی است. در این حمله با ترکیب ایده‌های حملات تفاضلی نامکن و بومرنگ، تمایزگر بومرنگ نامکن ساخته می‌شود. مشابه یک حمله‌ی بومرنگ، یک رمز قالبی E به‌صورت دو زیررمز $E^0 \circ E^1$ درنظر 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 نامکن اولین‌بار توسط بیهام و کلر[15] 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 نامکن برای شکستن ۶-دور AES-128، ۷-دور AES-192 و ۷-دور AES-256 در سناریوی حمله تک کلیدی و ۸-دور AES-192 و ۹-دور AES-256 در سناریوی حمله‌ی کلیدمرتبط با دو کلید استفاده شده است.

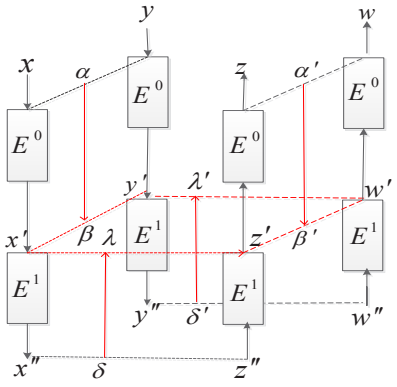
در انجام حملات تفاضلی، مطلوب است که تفاضل تا جای ممکن روی بیشترین تعداد دور برقرار شود. البته با افزایش تعداد دور، تفاضل احتمال کمتری پیدا می‌کند. حمله‌ی بومرنگ بر اساس چنین ایده‌ای شکل گرفته است و از دو تفاضل کوتاهتر با احتمال بیشتر به‌جای یک تفاضل با احتمال کمتر روی تعداد دور بیشتر استفاده می‌کند [۳۰].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

همان‌طور که در [۲۸]ذکر شده‌است، یک رمز قالبی مقاوم نسبت به حمله‌ی نوع-بومرنگ لزوماً در مقابل حمله‌ی بومرنگ نامکن مقاوم نمی‌باشد. در تمایزگر نوع-بومرنگ، خروجی یک دور میانه‌ی رمز با توزیع یکنواخت و مستقل از دورهای قبلی درنظر گرفته می‌شود. درحالی‌که، در تمایزگر بومرنگ نامکن اغلب توزیع یکنواخت و استقلال از دورهای قبلی درنظر گرفته نمی‌شود. بنابراین به‌نظر می‌رسد یک تمایزگر بومرنگ نامکن از تمایزگر نوع-بومرنگ مناسب‌تر است [۲۸]. در واقع، امتیاز حمله‌ی بومرنگ نامکن نسبت به حملات بومرنگ، مشابه حملات تفاضلی نامکن نسبت به حملات تفاضلی است. با آنکه همیشه می‌توان یک تفاضل نامکن را از یک تمایزگر نامکن بومرنگ روی تعداد دور یکسان به‌دست آورد، این مورد برای انواع آن‌ها در سناریوی حمله کلیدمرتبط درست نمی‌باشد. همان‌طور که در [۲۸]بیان شده‌است، انعطاف‌پذیری در انتخاب تفاضل‌های کلید امکان شکست دورهای بیشتری از رمز قالبی با استفاده از حمله‌ی بومرنگ تفاضلی نامکن را فراهم می‌سازد. زمانی‌که یک تفاضل نامکن ساخته می‌شود، انتخاب تفاضل زیرکلید برای E^0 معمولا باعث یک تفاضل معین در زیرکلید E^1 می‌شود و بالعکس. اما زمانی‌که یک تمایزگر بومرنگ نامکن 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 نامکن را فراهم می سازد. در [۳۱]نشان می‌دهند که حداکثر طول تمایزگرهای بومرنگ نامکن با تمایزگرهای تفاضلی نامکن روی رمزهای معین برابر است ولی حمله‌ی بومرنگ نامکن با احتمال بیشتری روی آن‌ها امکان‌پذیر (عملی) است.

تمایزگر بومرنگ نامکن

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

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



شکل ۲. تمایزگر بومرنگ نامکن [۲۸].

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

14 Jiqiang Lu
15 Keller

چهارتائی‌هایی که شرایط زیر را برآورده سازند چهارتائی درست نامیده می شوند.

- $z \oplus w = \alpha, x \oplus y = \alpha$
- $z' \oplus w' = \beta, x' \oplus y' = \beta$
- $y' \oplus w' = \gamma, x' \oplus z' = \gamma$
- $y'' \oplus w'' = \delta, x'' \oplus z'' = \delta$

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

$$\binom{mp}{2}.2^{-n+1}.q^2.2^{-n} = m^2.2^{-n}.(pq)^2 \quad (۶)$$

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 $E = E^0 \circ E^1$ است. فرض کنید که $\Delta\alpha \to \Delta\beta$ و $\Delta\alpha' \to \Delta\beta'$ تفاضل‌هایی با احتمال ۱ برای E_K^0، $\Delta\delta \to \Delta\gamma$ و $\Delta\delta' \to \Delta\gamma'$ تفاضل‌های 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:

$$E_K(X) \oplus E_K(X') = \delta \quad (۷)$$

$$E_K(X \oplus \alpha) \oplus E_K(X' \oplus \alpha) = \delta' \quad (۸)$$

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 $(\Delta\alpha, \Delta\alpha') \nrightarrow (\Delta\delta, \Delta\delta')$ نشان داد و تا زمانی‌که 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 $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ به‌صورت چهار زیررمز $E = E^a \circ E^0 \circ E^1 \circ E^b$ درنظر گرفته می‌شود که $E^0 \circ E^1$ دورهای تمایزگر بومرنگ ناممکن با تفاضل $(\Delta\alpha, \Delta\alpha') \nrightarrow (\Delta\delta, \Delta\delta')$ را نشان می‌دهد. E^a تعداد دورهای قبل از E^0 و E^b تعداد دورهای 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 رمزشده شناخته شده‌ی (((x,y),(z,w)),((x'',y''),(z'',w''))) چهار شرط زیر را برآورده می‌سازد:

$$E_{K_a}^a(x) \oplus E_{K_a}^a(y) = \alpha \quad (۹)$$

$$E_{K_a}^a(z) \oplus E_{K_a}^a(w) = \alpha' \quad (۱۰)$$

$$(E_{K_b}^b)^{-1}(x'') \oplus (E_{K_b}^b)^{-1}(y'') = \delta \quad (۱۱)$$

$$(E_{K_b}^b)^{-1}(z'') \oplus (E_{K_b}^b)^{-1}(w'') = \delta' \quad (۱۲)$$

اگر یک چهارتائی وجود داشته باشد که معادلات ۱۲-۹ 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.

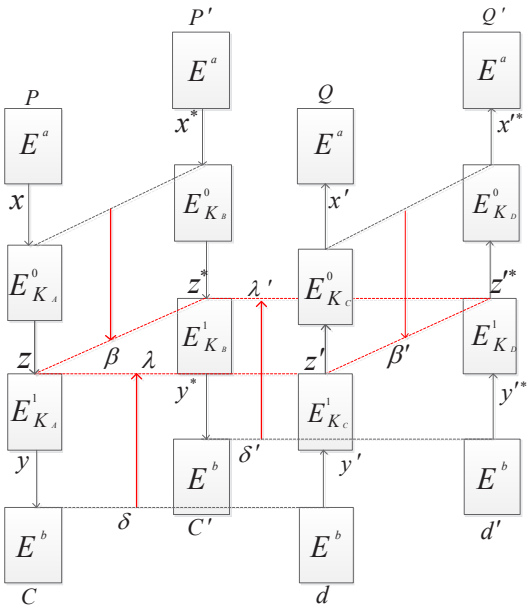
حمله‌ی بومرنگ ناممکن کلیدمرتبط

در حمله‌ی کلیدمرتبط، دشمن نه‌تنها قادر به رمزنگاری و رمزگشایی با کلید K است، همچنین می‌تواند از کلیدهای مرتبط استفاده کند. در حمله‌ی کلیدمرتبط نگاشت رابطه توسط دشمن انتخاب می‌شود. در اولین حمله‌ی کلیدمرتبط یک روش نگاشت ساده به‌کار رفته است: چرخش [۳۲]و فیلیپ‌های 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 $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ به‌صورت دو زیررمز $E^0 \circ E^1$ درنظر 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 $(E^1)^{-1}$ درنظر گرفته می‌شود که باید احتمال ۱ داشته باشند [۲۸]. E^a تعداد دورهای قبل از E^0 و E^b تعداد دورهای بعد از E^1 را نشان می‌دهد. بنابراین، تمایزگر بومرنگ ناممکن کلیدمرتبط شامل موارد زیر است:

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

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

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



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 باتوجه به بهترین احتمالات مشخصه‌های دورهای 1,…,r-1 و تعداد مشخصه‌های دور r ساخته می‌شود. در این الگوریتم بازگشتی، تنها درصورتی 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 $p_r . p_{n-r}^{best} \geq p_n^*$ برقرار باشد، سپس یک دور گسترش می‌یابد [۳۵]. در [۳۶]الگوریتم ماتسویی به‌عنوان مناسب‌ترین روش برای جستجوی مشخصه‌ی تفاضلی با حالت ۶۴-بیتی بیان شده و روی رمز DES آورده 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 مسیرهای تفاضلی باید با احتمال ۱ به تناقض برسند. باتوجه 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			
ΔK_5	6	∇K_{13}	0
ΔK_6	0	∇K_{14}	0
ΔK_7	0	∇K_{15}	0
ΔK_8	0	∇K_{16}	6
ΔK_9	6		
ΔK_{10}	2,3		
ΔK_{11}	0,14		
ΔK_{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 کلی‌تر بردار تفاضل کوتاه‌شده به‌صورت زیر تعریف می‌شود:

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

$$X_i = \begin{cases} 0 & \text{if } \Delta_i = 0 \\ 1 & \text{otherwise} \end{cases} \qquad (۱۳)$$

در حملات تفاضلی، تجزیه‌تحلیل کامل دو متن درنظر 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 ΔL_i را جذب می‌کند اگر و فقط اگر $L_{((i+7)mod\ n),((i-7)modn)} = 0$.

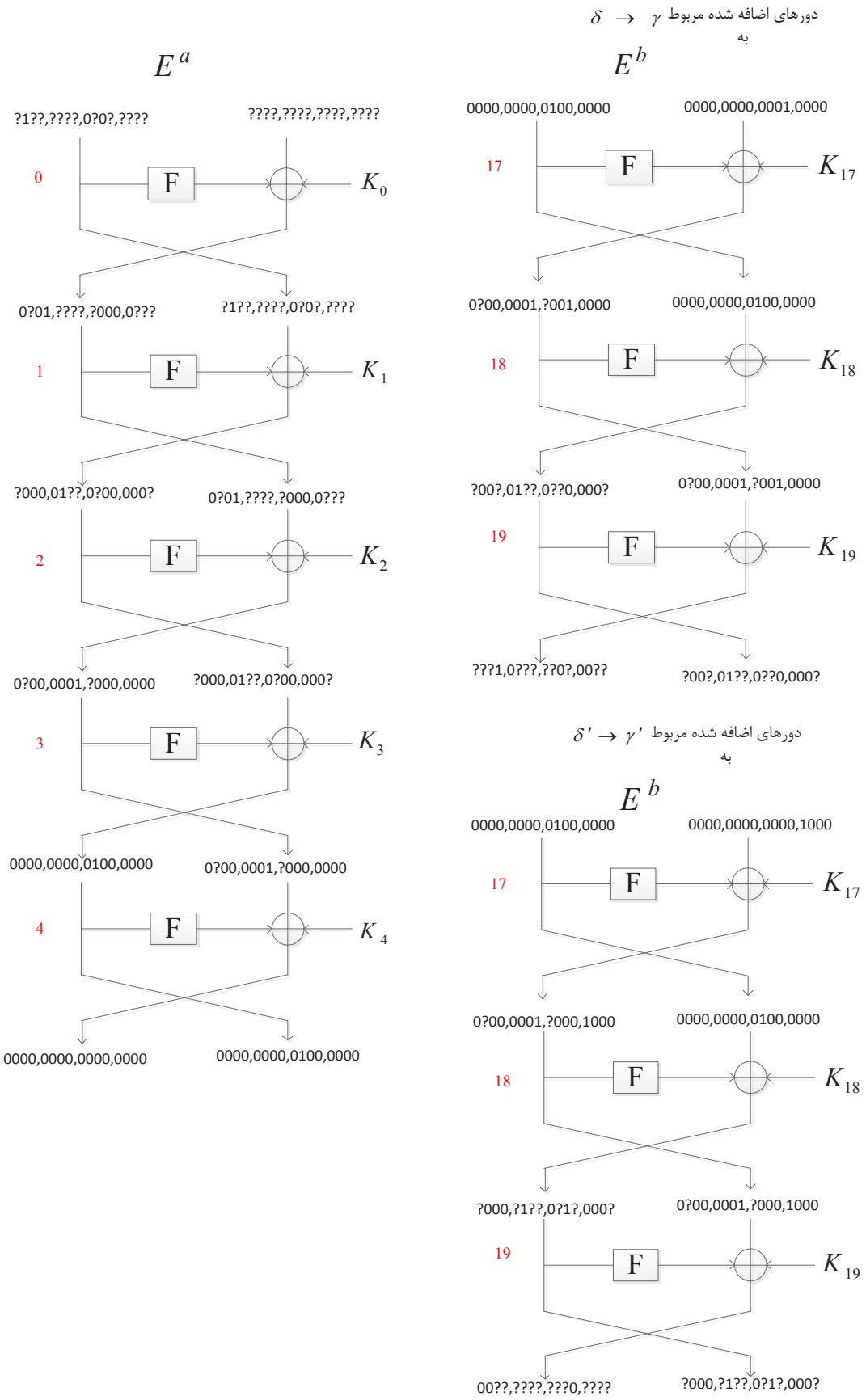
در دنباله‌ی تفاضلی ارائه‌شده بر اساس [۷]، تفاضل $\Delta_{i,[j]}$ بیانگر تفاضل کوتاه‌شده است که بیت i فعال و مقادیر j نامشخص است.

در رمز Simon به‌علت ویژگی جذب AND منطقی، بیت‌های نامشخص را بر اساس $L_{((i+7)mod\ n),((i-7)modn)}$ معین می‌کنیم. در جدول (۳)، مشخصه‌ی بومرنگ ناممکن کلیدمرتبط روی ۱۲-دور رمز Simon32/64 نشان داده شده‌است.

در جدول (۳) تفاضل‌های $\alpha \to \beta$ و $\delta \to \gamma$ 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 $\Delta\alpha \to \Delta\beta$ و $\Delta\alpha' \to \Delta\beta'$ برای E^0 هر دو یکسان درنظر گرفته شده‌اند. برای برقرارشدن شرط $\beta \oplus \beta' \oplus \gamma \oplus \gamma' \neq 0$ مقادیر γ و γ' به‌گونه‌ای انتخاب شده‌اند که در بیت ۹ سمت چپ به تناقض می‌رسند و در نهایت شرط برقرار می‌شود؛ تناقض بین γ و γ' در جدول (۴) آورده شده‌است. دورهای اضافه‌شده به مشخصه‌ی ۱۲-دوری در شکل (۳) مشاهده می‌شود.

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	0000000001000000
1	E^0	0000000000000000	0000000000000000	0000000000000000
2	E^0	0000000000000000	0000000000000000	0000000000000000
3	E^0	0000000000000000	0000000000000000	0000000000000000
4	E^0	0000000000000000	0000000000000000	0000000001000000
5	E^0	0000000001000000	0000000000000000	0000000000001100
6	E^0	0?000001?0001100	0000000001000000	0100000000000001
7	E^0	?100????0?1??00?	0?000001?0001100	0000011101100000
	E^0	????????????????	?100????0?1??00?	/
8	E^1	??0?010????0000?	???1?0????0?0?0?	0000000000000000
9	E^1	0??00001??0?0000	??0?010????0000?	0000000000000000
10	E^1	000?000001?00000	0??00001??0?0000	0000000000000000
11	E^1	0000000000010000	000?000001?00000	0000000001000000
	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 γ و γ'.

		تفاضل سمت چپ ورودی	تفاضل سمت راست ورودی	تفاضل زیرکلید
E^1	δ'	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	γ'	0??0?01?????0000	????1??????0?0??	0000000000000000
E^1	γ	??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	δ	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 درنظر گرفته و آن‌ها را درون 2^2 ساختار قرار می‌دهیم که هر کدام شامل دو مجموعه‌ای با 2^{29} متن اصلی است. ۴ ساختار بیان‌شده به شکل (?1?????? x_1?x_2????? , ????????????????) و (?0?????? x_1?x_2????? , ????????????????) می‌باشند که x_i $(2 \le i \le 1)$ 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:

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

بنابراین در مجموع 2^{60} جفت متن اصلی با تفاضلی به این شکل می‌توانیم به‌دست 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 رمزشده برای 2^{29} متن اصلی در هر 2^2 ساختار را با کلیدهای K_A, K_B, K_C, K_D که $K_A \oplus K_B = K_C \oplus K_D =$ $(K_3 = \Delta_6, K_2 = 0, K_1 = 0, K_0 = 0)$ $K_A \oplus K_C = K_B \oplus K_D =$ $(K_3 = \Delta_6, K_2 = 0, K_1 = 0, K_0 = 0)$ رمزنگاری می‌کنیم.

متن‌های رمزشده برای متن اصلی $P_{i,l}$ که با کلیدهای K_A, K_B, K_C, K_D رمزنگاری شدند را به‌ترتیب 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 ?000,0??? ,0?01 می‌باشد یا خیر و متن‌هایی با این ویژگی را حفظ می‌کنیم.

۳- برای متن‌های اصلی باقیمانده ۹ بیت از زیرکلید $K_0^g = \{0,1,2,3,4,5,9,10,11\}$ را حدس می‌زنیم. برای هر جفت باقیمانده $\Delta F(L_1) \oplus R_1$ را محاسبه کرده و بررسی می‌کنیم که آیا برابر با ?000,01??,0?00,000 می‌باشد یا خیر.

۴- برای متن‌های اصلی باقیمانده ۱۴ بیت از زیرکلیدهای $K_1^g = \{0,1,2,3,7,8,9,15\}$ و $K_0^g = \{6,7,8,13,14,15\}$ 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 $K_2^g = \{13\}$ و $K_1^g = \{11\}$, $K_3^g = \{15\}$ 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 $(L_5 \oplus (\Delta F(L_4) \oplus R_4)), (R_5 \oplus L_4)$ را از طریق دورهای ۰-۴ 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 رمزشده‌ی $\bar{P}_{i,l}$ تحت کلیدهای K_A, K_B, K_C, K_D را به‌ترتیب 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 ۱۹رمزگشایی می‌کنیم؛ سپس $C_{i,l} \oplus C'_{i,l}$ را به‌دست آورده و جفت‌هایی که مقدار تفاضل سمت راست آن‌ها $\oplus$ $\Delta F(C_{i,l}(R_{20}) \oplus C'_{i,l}(R_{20}))$ $(C_{i,l}(L_{20}) \oplus C'_{i,l}(L_{20}))$ و برابر با (0?00,0001,?001,0000) می‌باشد را حفظ می‌کنیم. در ادامه $\bar{C}'^*_{i,l} \oplus \bar{C}^*_{i,l}$ را به‌دست آورده و جفت‌هایی که مقدار تفاضل آن‌ها $\oplus$ $\Delta F(\bar{C}^*_{i,l}(R_{20}) \oplus \bar{C}'^*_{i,l}(R_{20}))$ $(\bar{C}^*_{i,l}(L_{20}) \oplus \bar{C}'^*_{i,l}(L_{20}))$ در سمت راست برابر با (0?00,0001,?000,1000) می‌باشد را حفظ می‌کنیم.

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

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

۱۰- بر اساس زیرکلیدهای $K_0^g, K_1^g, K_2^g, K_3^g$ حدس‌زده شده، ۲ بیت زیرکلیدهای $K_{18}=\{13,15\}$ را محاسبه کرده و برای هر چهارتائی 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 به‌دست آوردن مقدار خروجی دور ۱۷رمزگشایی 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 چهارتائی دیگر امتحان می‌کنیم؛ در تفاضل مربوط به $\delta' \to \gamma'$ و بر اساس زیرکلیدهای $K_0^g, K_1^g, K_2^g, K_3^g$ حدس‌زده شده، ۲ بیت زیرکلیدهای $K_{18}=\{13,15\}$ را محاسبه کرده و همه‌ی $\bar{T}^*_{i_1,l_1}$ و $\bar{T}'^*_{i_2,l_2}$ را برای به‌دست 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 چهارتائی دیگر امتحان می‌کنیم. اگر ۶ یا بیشتر چهارتائی این مرحله را عبور دهد، مرحله‌ی بعد را انجام می‌دهیم؛ درغیراین‌صورت، مرحله‌ی (۶-۳) را با حدس دیگری تکرار می‌کنیم.

۱۱- مقادیر $K_0=\{0\sim15\}$، $K_1=\{0\sim9,11,13\sim15\}$، $K_2=\{0,1,5,7,11,13\sim15\}$ و $K_3=\{15\}$ حدس‌زده شده‌اند. جستجوی جامع برای ۲۵ بیت کلید باقیمانده انجام می‌شود. اگر کلید ۶۴-بیتی حدس‌زده شده کلید کاربر ۲۰ دور رمز Simon32/64 باشد در این‌صورت 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 رمزشده‌ی متناظر برای همه‌ی جفت متن‌های اصلی را به‌دست می‌آوریم. برای هر جفت متن رمزشده بررسی تفاضل‌هایی به شکل (???10?????0?00?? , ??00?01??0??0000?) برای خروجی کشف کلید مشخصه‌ی اول و تفاضل به شکل (?000?1??0?1?000? , 00??????????0????) برای خروجی کشف کلید مشخصه‌ی دوم را حفظ می‌کنیم. جفت متن‌های رمزشده‌ای که شرط در هیچ دو گروه را برآورده نسازند، حذف می‌شوند. تعداد $2^{60} \times 2^{-14} = 2^{46}$ جفت تقریباً برای گروه اول و $2^{60} \times 2^{-12} = 2^{48}$ جفت تقریباً برای گروه دوم باقی‌می‌ماند. 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 $2^{46} \times 2^{-7} = 2^{39}$ 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 (۷-۳)، تعداد جفت‌های باقیمانده باتوجه به ۲۲ بیت شرط، برابر با $2^{39} \times 2^{-8-7-5-2} = 2^{17}$ در گروه اول و $2^{41} \times 2^{-8-7-5-2} = 2^{19}$ 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 باقی‌می‌ماند که تفاضل آن‌ها تحت کلیدهای حدس‌زده شده در خروجی دور پنجم به‌صورت (0000000000000000 , 0000000001000000) می‌باشد. بنابراین در حدود $\binom{2^{19}}{2} \approx \frac{2^{19\times2}}{2} = 2^{37}$ چهارتائی 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 چهارتائی کاندید به شکل (0?00,0001,?001,0000) وتفاضل بین $(\bar{C}'^*_{i,l}, \bar{C}^*_{i,l})$ در چهارتائی کاندید به شکل (0?00,0001,?000,1000) باشد. که تعداد چهارتائی‌های 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 چهارتائی کاندید ملاقات می‌کنند، بنابراین در حدود $2^{25} \times 2^{-14} = 2^{11}$ چهارتائی

کاندید به‌صورت $(T_{i_1,l_1}, \bar{T}^{*}_{i_1,l_1}, T'_{i_2,l_2}, \bar{T}'^{*}_{i_2,l_2})$ بعد از این مرحله برای هر حدس از زیرکلیدهای $K_0^g, K_1^g, K_2^g, K_3^g$ باقی‌می‌ماند. 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 مرحله‌ی (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 چهارتائی کاندید ملاقات می‌کنند، بنابراین در حدود $2^{11} \times 2^{-4} = 2^{7}$ چهارتائی کاندید به‌صورت $(T_{i_1,l_1}, \bar{T}^{*}_{i_1,l_1}, T'_{i_2,l_2}, \bar{T}'^{*}_{i_2,l_2})$ بعد از این مرحله برای هر حدس از زیرکلیدهای $K_0^g, K_1^g, K_2^g, K_3^g$ باقی‌می‌ماند. برای ۲۵ بیت باقیمانده از کلید جستجوی جامع انجام می‌شود، 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، حمله‌ی بومرنگ ناممکن کلیدمرتبط با پیچیدگی زمانی $2^{59.68}$ رمزنگاری ۲۰-دور رمز Simon32/64 انجام می‌شود.

نتیجه گیری

در این مقاله، برای اولین‌بار یک حمله‌ی بومرنگ ناممکن کلیدمرتبط روی ۲۰-دور کاهش‌یافته‌ی رمز قالبی Simon32/64 را ارائه کردیم. تاکنون تنها دو حمله‌ی کلیدمرتبط روی Simon32/64 ارائه‌شده است؛ ابتدا عابد و همکارانش[16] در [۱۵]روی ۱۴-دور از این نسخه حمله‌ی تفاضلی کلیدمرتبط و سپس در [۷]یک حمله‌ی مستطیلی کلیدمرتبط روی ۱۸-دور آن انجام داده‌اند.

همان‌طور که بیان کردیم، یک رمز قالبی مقاوم نسبت به حمله‌ی نوع-بومرنگ لزوماً در مقابل حمله‌ی بومرنگ ناممکن مقاوم نمی‌باشد. حمله‌ی بومرنگ ناممکن (کلیدمرتبط) انتخاب‌های مختلفی برای تفاضل‌ها (کلیدمرتبط) و متن‌های اصلی مورد نیاز ایجاد می‌کند. در تمایزگر نوع-بومرنگ، خروجی یک دور میانه‌ی رمز با توزیع یکنواخت و مستقل از دورهای قبلی درنظر گرفته می‌شود. درحالی‌که، در تمایزگر بومرنگ ناممکن اغلب توزیع یکنواخت و استقلال از دورهای قبلی درنظر گرفته نمی‌شود. بنابراین به‌نظر می‌رسد یک تمایزگر بومرنگ ناممکن از تمایزگر نوع-بومرنگ مناسب‌تر است. در حمله‌ی کلیدمرتبط باتوجه به اینکه از ارتباط بین کلیدها مطلع هستیم با عملیات XOR، عبارت $(C \oplus (Z_j)_i)$ از ساختار زمانبند کلید حذف می‌شود و پیچیدگی ساختار زمانبند برای تولید زیرکلیدها کاهش می‌یابد. انعطاف‌پذیری در انتخاب تفاضل‌های کلید امکان شکست دورهای بیشتری از رمز قالبی با استفاده از حمله‌ی بومرنگ تفاضلی ناممکن را فراهم می‌سازد. بنابراین ما با استفاده از ویژگی حملات بومرنگ توانستیم دو دنباله مسیر زیرکلید متفاوت را برای انجام حمله به‌کار ببریم و تعداد دور حمله شده نسبت به حالت تفاضلی ناممکن را افزایش دهیم. الگوریتم رمز قالبی AES، از قوی‌ترین و پرکاربردترین الگوریتم‌های رمزنگاری با ساختار جایگشت-جایگذاری می‌باشد. با وجود اینکه حملات خطی و تفاضلی روی دورهای محدود این رمز انجام شده‌اند؛ اما حمله‌ی بومرنگ کلیدمرتبط روی دور کامل AES-256 صورت گرفته است [۳۸]. حمله‌ی خطی روی ۲۳ دور از رمز Simon32/64 و حمله‌ی کلیدمرتبط ارائه‌شده در این مقاله روی ۲۰ دور از آن، نشان می‌دهد که زمانبند کلید این رمز قالبی در برابر حملات کلیدمرتبط مقاوم‌تر طراحی شده‌است و ادعای طراحان آن مبنی بر مقام بودن زمانبند کلید آن اثبات می‌شود. حمله‌ی بومرنگ ناممکن کلیدمرتبط را می‌توان برای ارزیابی امنیت رمزهایی با ساختار جایگشت-جایگذاری و نیز بررسی نقاط ضعف الگوریتم زمانبند کلید آن‌ها به‌کار برد.

16 Abed et al

مرجع‌ها

[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-

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 201 5. 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, 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., Varıcı, 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