دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۳، جلد ۲۲، شماره ۲ (۸۷-۹۴)
https://monadi.isc.org.ir

ارائه‌شده در بیست و یکمین کنفرانس بین‌المللی انجمن رمز ایران در دانشگاه تربیت مدرس و پژوهشگاه ارتباطات و فناوری اطلاعات، ۲۵ و ۲۶ مهرماه ۱۴۰۳

بررسی حمله تحلیل توان روی رمز قالبی SPEEDY و مقاوم‌سازی آن با استفاده از روش نقاب‌گذاری مبتنی بر دامنه (DOM)★

کیوان خورمهر، جوادعلیزاده* و محسن جهانبانی

آزمایشگاه مساف، دانشکده رایانه، شبکه و ارتباطات، دانشگاه جامع امام حسین (ع)، تهران، ایران

اطلاعات مقاله

کلمات کلیدی:
حمله تحلیل توان
رمز قالبی SPEEDY
مقاوم‌سازی
روش DOM

نوع مقاله: پژوهشی

چکیده

حملات کانال جانبی مانند حمله تحلیل توان یک تهدید برای امنیت کاربردهای یک رمز قالبی روی سخت‌افزار هستند. حمله تحلیل توان را می‌توان به سه روش ساده، مبتنی بر تفاضلات داده‌ها و مبتنی بر همبستگی داده‌ها انجام داد. در این مقاله امنیت رمز قالبی SPEEDY در برابر حمله تحلیل توان مورد بررسی قرار می‌گیرد. برای این منظور ابتدا در بخش اول مقاله نشان داده می‌شود که لایه غیرخطی رمز قالبی SPEEDY در برابر حمله تحلیل توان نشت دارد. به طوری که با پیاده‌سازی سخت‌افزاری آن و استفاده از ۱۰۰۰ نمونه ورودی، می‌توان حمله کشف کلید انجام داد. در بخش دوم مقاله به موضوع مقاوم‌سازی رمز قالبی SPEEDY در برابر حمله تحلیل توان پرداخته شده و با استفاده از روش نقاب‌گذاری مبتنی بر دامنه یا DOM، یک روش پیاده‌سازی امن برای این رمز پیشنهاد می‌شود. با استفاده از ابزار سیلور و روش آزمون T نشان داده می‌شود که نسخه مقاوم‌سازی رمز قالبی SPEEDY، ضعف‌ها و نشتی‌های مربوط به نسخه اصلی در برابر حمله تحلیل توان را ندارد

© ۱۴۰۳ انجمن رمز ایران

۱ مقدمه

برای تأمین امنیت اطلاعات لازم است تا ویژگی‌های مهم مانند محرمانگی، دست‌نخوردگی، دسترس‌پذیری، احراز اصالت و انکارناپذیری پیام تأمین شود. الگوریتم‌های رمزنگاری نقش مهمی در تأمین برخی از این ویژگی‌ها دارند. از میان الگوریتم‌های رمزنگاری، رمزهای قالبی به دلیل اینکه قابلیت اثبات امنیتی دارند و همچنین کاربردهای متنوعی که دارند، در مقایسه با رمزهای دنباله‌ای بیشتر مورد توجه قرار گرفته‌اند. برای استفاده امن از یک الگوریتم رمز قالبی، لازم است تا از امنیت و مقاومت آن در برابر حملات شناخته شده اطمینان حاصل شود. حملات روی الگوریتم‌های رمزنگاری را می‌توان در دو دسته کلی حملاتی که از ضعف‌های خود الگوریتم استفاده می‌کنند و حملاتی که از ضعف‌های مربوط به پیاده‌سازی نرم‌افزاری یا سخت‌افزاری این الگوریتم‌ها استفاده می‌کنند، دسته‌بندی کرد. حملاتی مانند حمله تفاضلی یا حمله خطی جزو حملات دسته اول و حملاتی مانند حملات کانال جانبی از نوع تحلیل توان جزو حملات دسته دوم قرار می‌گیرند. برای مقاوم‌سازی رمز قالبی در برابر حملات دسته اول لازم است تا از مؤلفه‌ها و معماری طراحی امن در طراحی رمزهای قالبی استفاده شود. همچنین برای اطمینان از امنیت یک سامانه رمزنگاری در برابر حملات کانال جانبی از نوع تحلیل توان، لازم است تا الگوریتم‌های رمزنگاری با استفاده از روش‌های مقاوم‌سازی به‌صورت امن پیاده‌سازی شوند. از روش‌های مقاوم‌سازی شناخته شده برای پیاده‌سازی‌های سخت‌افزاری

★از کمیته علمی بیست و یکمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.
*نویسنده مسئول.
آدرس‌های رایانامه: khoormehr@ihu.ac.ir (کیوان خورمهر)، jaalizadeh@ihu.ac.ir (جوادعلیزاده)، mjahanbani@ihu.ac.ir (محسن جهانبانی)
© ۱۴۰۳ تمامی حقوق متعلق به انجمن رمز ایران است.

الگوریتم‌های رمز قالبی می‌توان به روش‌های مخفی‌سازی، نقاب‌گذاری، پیاده‌سازی آستانه‌ای و نقاب‌گذاری مبتنی بر دامنه (DOM) اشاره کرد.

در سال ۲۰۲۱، الگوریتم رمز قالبی SPEEDY توسط لیندر و همکارانش در کنفرانس CHES معرفی شد [۱]. این الگوریتم با هدف ارائه تأخیر پایین و کارآیی بالا در بستر سخت‌افزار طراحی شده است. در طراحی رمز قالبی SPEEDY، میزان فضا و انرژی مصرفی نسبت به کارآیی و سرعت آن در اولویت دوم قرار داشته و طراحان تلاش کرده‌اند تا با تمرکز روی طراحی یک جعبه جانشانی شش بیتی مناسب بتوانند به هدف تأخیر پایین دست پیدا کنند.

تاکنون امنیت رمز قالبی SPEEDY در برابر حملات مبتنی بر وجود ضعف در خود الگوریتم، مانند حمله تفاضلی بررسی شده است [۲] که نشان داده می‌شود هفت دور این الگوریتم آسیب‌پذیر است. در این مقاله امنیت پیاده‌سازی سخت‌افزاری الگوریتم رمز قالبی SPEEDY در برابر حمله تحلیل توان مورد بررسی و رسیدگی قرار می‌گیرد. بعد از اینکه نشان داده می‌شود رمز قالبی SPEEDY در برابر حمله تحلیل توان ناامن است، از یک روش نقاب‌گذاری مبتنی بر دامنه برای مقاوم‌سازی این رمز قالبی استفاده می‌شود. برای توضیح موارد ذکر شده، بقیه مطالب این مقاله به صورت زیر سازمان‌دهی شده است.

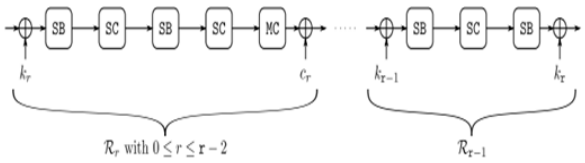
در بخش ۱.۲، ابتدا رمز قالبی SPEEDY و مفاهیم مورداستفاده در رابطه با حمله تحلیل توان و مقاوم‌سازی در برابر این حمله معرفی می‌شوند. در بخش ۳ نشان داده می‌شود که لایه غیرخطی رمز قالبی SPEEDY در برابر حمله تحلیل توان نشتی دارد و می‌تواند باعث آسیب‌پذیری این الگوریتم در برابر حمله ذکر شده شود. در این بخش روش اعمال حمله تحلیل توان روی رمز قالبی SPEEDY جهت کشف کلید نیز توصیف می‌شود. در بخش ۴، الگوریتم رمز SPEEDY با استفاده از روش نقاب‌گذاری مبتنی بر دامنه مقاوم‌سازی می‌شود. در بخش ۵ نسخه مقاوم‌سازی شده با استفاده از ابزار سیلور و روش آزمون T مورد ارزیابی قرار می‌گیرد. در نهایت جمع‌بندی و نتیجه‌گیری مقاله در بخش ۶ ارائه می‌شود.

۲ مفاهیم پایه

در این بخش مفاهیم پایه موردنیاز برای درک رمز قالبی SPEEDY و حمله تحلیل توان روی آن توصیف می‌شود. همچنین روش مقاوم‌سازی مبتنی بر دامنه نیز برای امن‌سازی یک رمز قالبی در برابر حمله تحلیل توان معرفی می‌شود.

۱.۲ معرفی رمز قالبی SPEEDY

رمز قالبی SPEEDY از خانواده رمزهای با تأخیر کم است که در سال ۲۰۲۱ معرفی شد. این الگوریتم از یک جعبه جانشانی شش بیتی استفاده می‌کند و می‌تواند قالب‌های پیام و کلیدهای با اندازه متفاوت را پشتیبانی کند. به عنوان نمونه SPEEDY-r-6l معرف الگوریتم SPEEDY با تعداد



شکل ۱. تابع دور الگوریتم رمز SPEEDY [۱]

جدول ۱. تابع دور الگوریتم رمز SPEEDY [۱]

x_0x_1	$x_2x_3x_4x_5$															
	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f
0.	08	00	09	03	38	10	29	13	0c	0d	04	07	30	01	20	23
1.	1a	12	18	32	3e	16	2c	36	1c	1d	14	37	34	05	24	27
2.	02	06	0b	0f	33	17	21	15	0a	1b	0e	1f	31	11	25	35
3.	22	26	2a	2e	3a	1e	28	3c	2b	3b	2f	3f	39	19	2d	3d

دور r و طول کلید $6l$ می‌باشد. در این رمز قالبی حالت را می‌توان به صورت یک آرایه $6 \times l$ از بیت‌ها در نظر گرفت که در آن مقدار l برابر با ۳۲ است. برای مثال متن ورودی ۱۹۲ بیتی به یک ماتریس 6×32 تبدیل شده و عملیات رمزنگاری روی آن انجام می‌شود. در هر دور، ماتریس حالت با کلید دور XOR شده و وارد جعبه جانشانی، تبدیل جابجا کننده ستونی و تبدیل مخلوط‌کننده ستونی شده و در نهایت با عدد ثابت دور XOR می‌شود. در دور آخر سه عملیات پایانی یعنی جابجاکننده ستونی و مخلوط‌کننده ستونی و XOR با عدد ثابت دور حذف می‌شوند و به جای آن‌ها عمل XOR با کلید دوم دور آخر انجام می‌شود. فرایند رمزگذاری با استفاده از رمز SPEEDY در شکل ۱ خلاصه شده است.

با توجه به شکل ۱ جعبه جانشانی شش بیتی بر روی هر ردیف از ماتریس حالت اعمال می‌شود که معادله آن به صورت معادله (۱) می‌باشد.

$$(y_{[i,0]}, y_{[i,1]}, y_{[i,2]}, y_{[i,3]}, y_{[i,4]}, y_{[i,5]}) = S(x_{[i,0]}, x_{[i,1]}, x_{[i,2]}, x_{[i,3]}, x_{[i,4]}, x_{[i,5]}) \quad (۱)$$

جدول جستجوی این جعبه جانشانی را می‌توان مطابق جدول ۱ در نظر گرفت.

بعد از تبدیل جعبه جانشانی، ماتریس حالت وارد تبدیل جابجاکننده ستونی یا همان SC می‌شود که خروجی این تبدیل طبق رابطه (۲) محاسبه می‌شود.

$$y_{[i.j]} = x_{[i+j.j]} \quad (۲)$$

سپس عملیات مخلوط‌کننده ستونی یا همان MC نیز بر روی هر ستون انجام می‌شود. به طوری که هفت بیت ورودی به طور خاص انتخاب و با هم XOR می‌شوند تا یک بیت جدید به عنوان خروجی تولید شود. این رابطه در معادله (۳) نشان داده شده است. این عملیات همچنین می‌تواند به عنوان ضرب هر ستون توسط یک ماتریس چرخشی نیز در نظر گرفته شود.

$$y_{[i.j]} = x_{[i.j]} \oplus x_{[i+1.j]} \oplus x_{[i+5.j]} \oplus x_{[i+9.j]}$$

$$\oplus x_{[i+۱۵.j]} \oplus x_{[i+۲۱.j]} \oplus x_{[i+۲۶.j]} \quad (۳)$$

کلید دور ۱۹۲ بیتی k_r و ثابت ۱۹۲بیتی C_r نیز به ترتیب با کل ماتریس حالت XOR می‌شوند. همچنین کلید اصلی [۱] ۱۹۲ بیتی الگوریتم SPEEDY به عنوان کلید دور صفرم $(k_۰)$ درنظر گرفته می‌شود و رابطه کلید دور rام با کلید دور $r+۱$ام به صورت معادله (۴) می‌باشد [۱].

$$k_{r+۱} = PB(k_r) \quad (۴)$$

۲.۲ توصیف حمله تحلیل توان

حمله تحلیل توان مصرفی یک نوع حمله کانال جانبی است که به دنبال به دست آوردن اطلاعات مخفی الگوریتم رمز قالبی با استفاده از ثبت توان مصرفی تراشه در حال انجام عملیات رمزنگاری است. این تحلیل از این حقیقت که توان لحظه‌ای مصرفی تراشه، به اطلاعات در حال پردازش و عملیات در حال اجرا بستگی دارد، بهره می‌برد. این حمله شامل سه نوع حمله تحلیل توان ساده، حمله تحلیل توان تفاضلی و حمله تحلیل توان همبستگی است [۳]. در حمله تحلیل توان همبستگی با استفاده از معادله (۵) همبستگی بین ماتریس توان‌های اندازه‌گیری شده از تراشه هنگام اجرای عملیات رمزنگاری و ماتریس توان‌های فرضی (که با استفاده از وزن همینگ داده‌ها پس از XOR با کلید و عبور از جعبه جانشانی رمز تشکیل می‌شود) به دست می‌آید. ستونی که بیشترین مقدار این ماتریس در آن قرار دارد، برابر یک بایت از کلید خواهد بود.

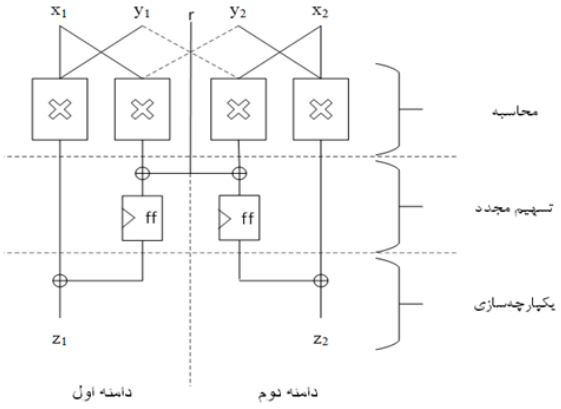
$$r_{ij} = \frac{\sum_d^D (h_{di} - \tilde{h}_i) \cdot (t_{di} - \tilde{t}_j)}{\sqrt{\sum_d^D (h_{di} - \tilde{h}_i)^۲ \cdot \sum_{d=۱}^D (t_{di} - \tilde{t}_j)^۲}} \quad (۵)$$

در معادله (۵)، h ماتریس توان فرضی است که با استفاده از وزن همینگ داده‌ها به ازای کلیدهای فرضی متفاوت به دست می آید. t ماتریس توان‌های اندازه‌گیری شده است. $\tilde{t}_j$ و $\tilde{h}_j$ نیز به ترتیب مقادیر میانگین ماتریس‌های t و h هستند. D نیز تعداد نمونه‌های توان است که به ازای متن‌های اصلی مختلف (D متن اصلی مختلف) به دست می‌آید.

۳.۲ معرفی روش مقاوم‌سازی DOM

یکی از روش‌های مقاوم‌سازی الگوریتم‌های رمزنگاری در برابر حملات پیاده‌سازی، روش نقاب‌گذاری دامنه‌گرا است. این روش تعداد سهم‌های ورودی را از $td+۱$ سهم به $d+۱$ سهم کاهش می‌دهد و با این کار مساحت پیاده‌سازی نیز کم می‌شود. در این روش، به‌ازای تعداد سهم‌ها، دامنه‌هایی وجود دارند که هر کدام از این دامنه‌ها با استفاده از عدد تصادفی از یکدیگر مستقل می‌شوند. در شکل ۲ پیاده‌سازی نقاب‌گذاری دامنه‌گرا مرتبه اول برای یک درگاه AND دو ورودی نشان داده شده است [۴]. همان‌طور که در این شکل مشاهده می‌شود، این روش شامل سه مرحله است. مرحله اول، محاسبه [۲] است که در آن سهم‌ها با یکدیگر ضرب می‌شوند. از آنجا که خروجی‌های این مرحله حاصل‌ضرب ورودی‌هایی از دو دامنه متفاوت

[1] Master key [2] Calculation



شکل ۲. نقاب‌گذاری دامنه‌گرا برای درگاه AND دو ورودی با درجه امنیت مرتبه اول

است، ممکن است باعث نشتی شوند، زیرا دو دامنه با این ضرب به هم وابسته می‌شوند. بنابراین، نیاز به یک تازه‌سازی وجود دارد تا دو دامنه از هم مستقل شوند. تازه‌سازی به معنای XOR کردن خروجی‌های ذکر شده با یک عدد تصادفی است که این عمل در مرحله بعد، یعنی مرحله تسهیم مجدد انجام می‌شود. برای جلوگیری از وقوع خطای گذرا یا گلیچ در این مرحله، از ثبات استفاده می‌شود. در مرحله آخر نیز جمع یا یکپارچه‌سازی در هر دامنه انجام می‌شود تا سهم‌های خروجی شکل بگیرند.

۴.۲ معرفی ابزار SILVER و روش آزمون T

برای ارزیابی نشتی یک الگوریتم رمز یا مقاومت آن در برابر حمله تحلیل توان باید میزان نشتی این الگوریتم در برابر حمله تحلیل توان سنجیده شود. برای این منظور از ابزارها و روش‌های خاص مانند ابزار سیلور و آزمون T استفاده می‌شود که در این مقاله نیز به کار برده شده‌اند.

آزمون آماری T یکی از روش‌های تشخیص تفاوت آماری بین دو گروه است که با استفاده از ویژگی‌هایی مانند میانگین و واریانس انجام می‌شود. برای ارزیابی مقاومت پیاده‌سازی الگوریتم‌های رمزنگاری می‌توان از این آزمون استفاده کرد. ابتدا چند بار متن آشکار ثابت به الگوریتم داده شده و توان مصرفی اندازه‌گیری و ذخیره می‌شود. سپس این فرایند با متون آشکار تصادفی تکرار می‌شود. با مقایسه داده‌های حاصل از این دو مرحله با آزمون T می‌توان تشخیص داد که آیا تمایزی بین این دو گروه وجود دارد یا نه. در صورت عدم وجود تمایز، اطلاعات مفیدی برای مهاجم نشت نمی‌کند. اما در صورت وجود تمایز، آن نقطه مستعد حمله تحلیل توان است.

این آزمون به‌وسیله رابطه (۶) انجام می‌شود. اگر مقدار حاصل از این رابطه کمتر از ۴/۵ یا بیشتر از ۴/۵− باشد، بین دو گروه تمایزی وجود ندارد، اما اگر خارج از این بازه باشد بین دو گروه تمایز وجود دارد.

$$t = \frac{(\mu_۰ - \mu_۱)}{\sqrt{\frac{s_۰^۲}{n_۰} + \frac{s_۱^۲}{n-۱}}} \quad (۶)$$

در رابطه (۶)، μ_0 و μ_1 به ترتیب میانگین گروه اول و دوم، s_0^2 و s_1^2 به ترتیب واریانس گروه اول و دوم، n_0 و n_1 به ترتیب تعداد اعضای گروه اول و دوم هستند و t حاصل این آزمون است. این آزمون T مرتبه اول است. برای انجام آزمون با مراتب بالاتر کافی است طبق [۵] به جای میانگین و واریانس، گشتاور مرکزی یا استاندارد را قرار داد.

یکی دیگر از روش‌های نرم‌افزاری برای ارزیابی مقاومت پیاده‌سازی در برابر حمله تحلیل توان که در سال ۲۰۲۰ توسط نیچل و همکاران معرفی شد، ابزاری به نام SILVER است [۶]. این ابزار که با زبان C نوشته شده است، با استفاده از مفاهیمی مانند نمودارهای تصمیم دودویی کاهش مرتبه یافته [1] و استقلال آماری توزیع‌های احتمال، سعی در کشف نشتی پیاده‌سازی‌ها دارد. SILVER برای ارزیابی پیاده‌سازی‌هایی با مساحت کمتر از 5 KGE مناسب است. بنابراین می‌توان از آن برای ارزیابی یک جعبه جانشانی که معمولاً مساحتی کمتر از این مقدار دارد، استفاده کرد. این ابزار در سیستم عامل لینوکس قابل استفاده است و برای استفاده از آن نیاز به تهیه لیست توصیف مدار می‌باشد. برای تهیه لیست توصیف مدار نیز می‌توان از نرم‌افزار Design Compiler استفاده کرد.

۳ ارزیابی میزان نشت الگوریتم رمز SPEEDY

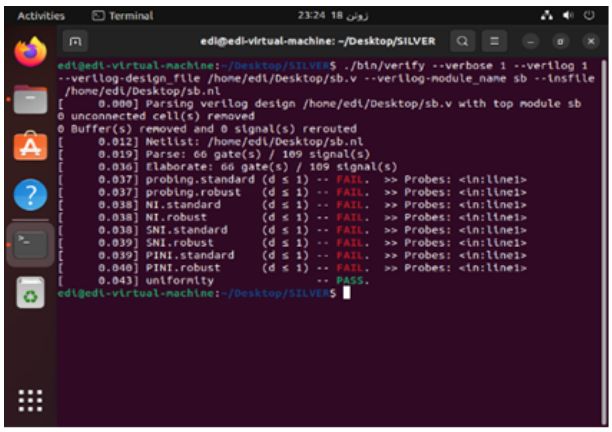
براي بررسی میزان ضعف الگوریتم SPEEDY در برابر حمله تحلیل توان، از سه روش استفاده می‌شود. ابتدا با پیاده‌سازی سخت‌افزاری جعبه جانشانی به‌وسیله کد VHDL، میزان نشت اطلاعات با استفاده از ابزار SILVER مورد بررسی قرار می‌گیرد. سپس با پیاده‌سازی نرم‌افزاری الگوریتم روی میکرو، نشت اطلاعات از طریق اندازه‌گیری توان مصرفی مطالعه و بررسی شده و نشان داده می‌شود که چگونه می‌توان با استفاده از حمله تحلیل توان، کلید رمز قالبی SPEEDY را به دست آورد.

۱.۳ ارزیابی جعبه جانشانی رمز SPEEDY با ابزار SILVER و آزمون T

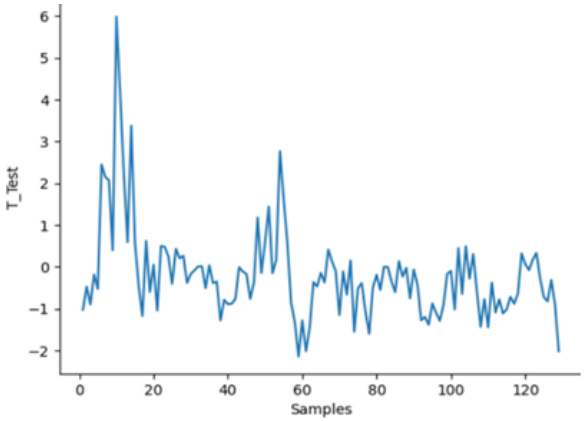
برای ارزیابی جعبه جانشانی رمز SPEEDY با استفاده از ابزار SILVER، ابتدا کد VHDL جعبه جانشانی با استفاده از نرم‌افزار ISE پیاده‌سازی می‌شود. سپس، لیست توصیف مدار از این کد با در نظر گرفتن عدم وجود برخی درگاه‌ها در نرم‌افزار Design Compiler ساخته می‌شود. پس از آن، با تغییر ورودی‌های این لیست به گونه‌ای که این ورودی‌ها قابل خواندن توسط ابزار SILVER باشند، لیست ویرایش می‌شود. در نهایت، لیست ویرایش شده به عنوان فایل ورودی به ابزار SILVER داده می‌شود تا پردازش شود. نتیجه ارزیابی جعبه جانشانی امن در شکل ۳ آمده است.

همان‌طور که در شکل ۳ مشاهده می‌شود جعبه جانشانی الگوریتم SPEEDY در برابر حمله تحلیل توان امن نیست. همچنین برای اطمینان بیشتر از این موضوع آزمون T نیز با ۵۰۰۰۰ نمونه توان اجرا شد. برای این منظور از برد هدف CW305 برای ثبت اثرهای توان استفاده شد. همان طور که در شکل ۴ مشاهده می‌شود، از آنجا که مقدار آزمون از کران

[1] Reduced Ordered Binary Decision Diagrams



شکل ۳. نتیجه ارزیابی جعبه جانشانی رمز SPEEDY با ابزار SILVER



شکل ۴. نتیجه آزمون T بر روی جعبه جانشانی رمز SPEEDY

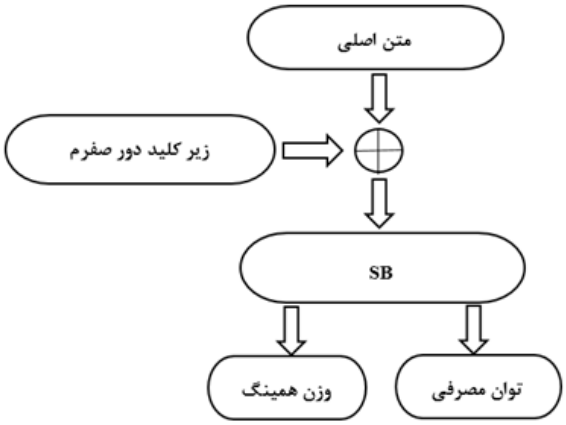
۴/۵ عبور کرده است، لذا در این جعبه جانشانی نشتی وجود دارد.

با توجه به توضیحات ارائه شده، مشخص است که لایه غیرخطی رمز قالبی SPEEDY در برابر حمله تحلیل توان دارای نشت اطلاعات است و بنابراین انتظار می‌رود که حمله تحلیل توان برای کشف کلید این الگوریتم رمز موفقیت‌آمیز باشد. در بخش بعد این حمله توضیح داده می‌شود.

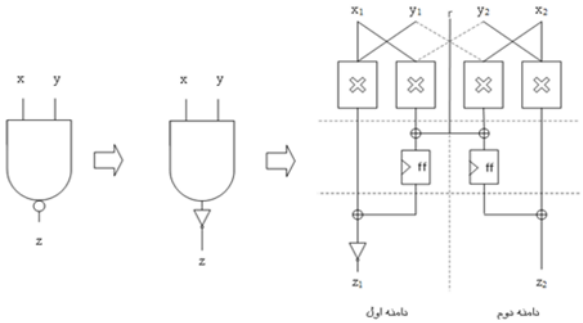
۲.۳ حمله تحلیل توان روی رمز قالبی SPEEDY

اجرای حمله تحلیل توان بر روی الگوریتم SPEEDY ابتدا باید بستر اجرای حمله ایجاد شود. برای اجرای این حمله از برد Chipwisperer که یک برد تخصصی برای ارزیابی نشت اطلاعات است استفاده می‌شود. بدین منظور بعد از پیاده‌سازی الگوریتم بر روی میکرو برد هدف، میزان توان مصرفی الگوریتم با فرکانس نمونه‌برداری ۴ برابر فرکانس کاری میکرو یعنی 29.538459 MS/s اندازه‌گیری می‌شود (بر طبق قضیه نایکوئیست فرکانس نمونه برداری حداقل باید دو برابر فرکانس کاری میکرو باشد که در اینجا برای دقت بیشتر ثبت اثر توان [2] ۴ برابر فرکانس کاری میکرو در نظر گرفته می‌شود). نقطه میانی مورد نظر برای اجرای حمله مانند شکل

[2] Power trace



شکل ۵. نقطه میانی الگوریتم SPEEDY برای اجرای حمله



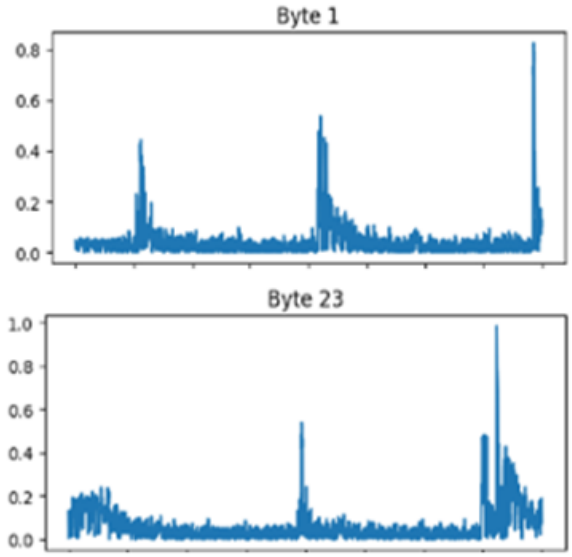
شکل ۶. نمایش میزان توان مصرفی یک جعبه جانشانی از الگوریتم اسپیدی در حالت پیاده‌سازی نرم‌افزاری

۵ می باشد که در آن از خروجی جعبه جانشانی دور اول برای به دست آوردن زیر کلید دور صفرم که همان کلید اصلی است، استفاده می‌شود.

برای نمایش بهتر نشت اطلاعات از طریق توان مصرفی در خروجی جعبه جانشانی دور اول، در شکل ۶ میزان توان مصرفی اجرای یک جعبه جانشانی از الگوریتم رمز در حالت پیاده‌سازی نرم‌افزاری ارائه شده است.

بعد از ثبت نمونه‌های توان به ازای متن‌های پیام گوناگون حمله همبستگی به‌ازای ۵۰۰ و ۱۰۰۰ نمونه توان اجرا شد. با توجه به این حمله به ازای ۵۰۰ نمونه توان ۱۰ بایت از ۲۴ بایت از زیرکلید دور صفرم به دست می‌آید. همچنین به ازای ۱۰۰۰ نمونه توان ۱۷ بایت از زیرکلید دور صفرم به دست می‌آید. همان طور که انتظار می‌رفت، می‌توان با افزایش تعداد نمونه‌های توان، تعداد بیشتری از بایت‌های زیر کلید دور صفرم که همان کلید اصلی الگوریتم است را به دست آورد. در شکل ۷ به عنوان نمونه مقادیر به دست آمده برای همبستگی دو بایت از زیر کلید دور صفرم نشان داده شده است که تقریباً مقدار آنها نزدیک به یک است.

در بخش بعد از روش DOM استفاده می‌شود تا یک پیاده‌سازی سخت‌افزاری برای رمز قالبی SPEEDY طوری ارائه شود که در برابر



شکل ۷. مقادیر به دست آمده برای همبستگی بایت اول و بیست و سوم زیرکلید دور صفرم

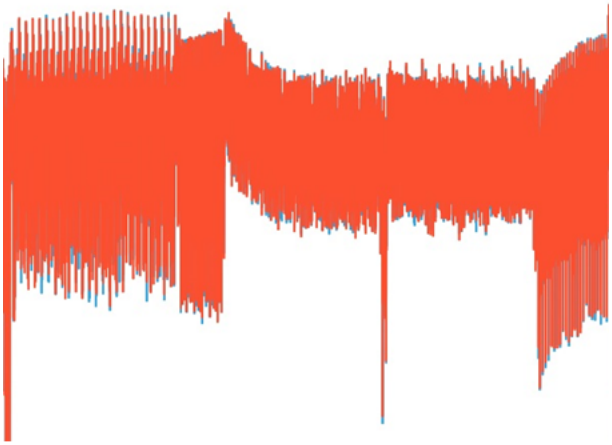
حمله تحلیل توان مقاوم باشد.

۴ مقاوم‌سازی پیاده‌سازی سخت‌افزاری رمز قالبی SPEEDY با استفاده از روش DOM

برای مقاوم‌سازی جعبه جانشانی رمز SPEEDY به روش نقاب‌گذاری مبتنی بر دامنه مرتبه اول، تمامی درگاه‌های موجود باید به درگاه AND دو ورودی تبدیل شوند. زیرا این روش برای درگاه AND دو ورودی طراحی شده است. ابتدا، تمامی درگاه‌های NAND موجود در جعبه جانشانی به درگاه‌های AND و NOT تبدیل شدند که نتیجه آن ۳۰ درگاه AND و ۳۶ درگاه NOT بود. سپس، درگاه‌های AND سه ورودی و چهار ورودی به درگاه AND دو ورودی تبدیل شدند که در این مرحله ۶۳ درگاه AND دو ورودی به دست آمد. در نهایت، به جای درگاه‌های AND دو ورودی، طرح DOM قرار داده شد. نحوه اعمال روش DOM بر روی درگاه $NAND$ دو ورودی در شکل ۸ نشان داده شده است.

مقاوم‌سازی جعبه جانشانی با استفاده از کد VHDL و سنتز در نرم‌افزار Design Compiler منجر به افزایش مساحت از 29.5 GE به 2519 GE شد. تأخیر اجرای جعبه جانشانی مقاوم‌سازی شده به ۴/۵ کلاک افزایش یافت، در حالی که جعبه جانشانی مقاوم‌سازی نشده در کمتر از یک کلاک انجام می‌شد. همچنین، جعبه جانشانی مقاوم‌سازی شده از ۶۳ بیت تصادفی و ۲۵۲ درگاه AND دو ورودی استفاده می‌کند.

بعد از انجام تغییرات روی جعبه جانشانی رمز SPEEDY، لازم است تا با استفاده از روش‌ها و ابزارهای معرفی شده، نسخه جدید مورد تحلیل و ارزیابی قرار بگیرد. این کار در بخش بعد توضیح داده می‌شود.



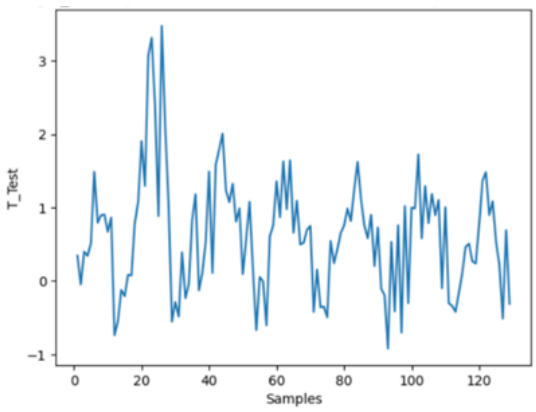
شکل ۸. اعمال روش نقاب گذاری دامنه گرا مرتبه اول بر روی درگاه NAND دو ورودی

۵ ارزیابی نسخه مقاوم‌سازی شده پیاده‌سازی رمز قالبی SPEEDY

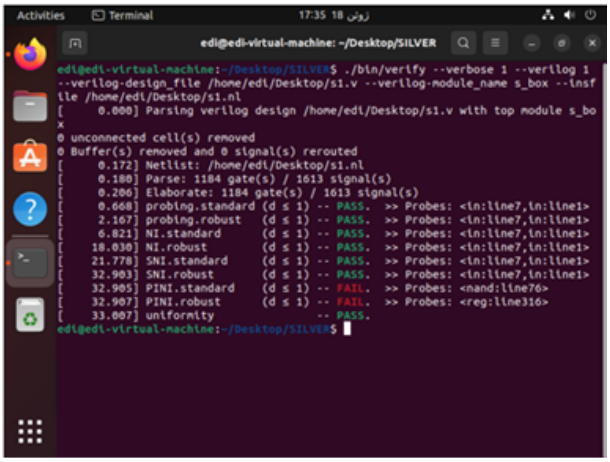
برای ارزیابی طرح ارائه شده در بخش قبل، ابتدا کد VHDL طرح مقاوم‌سازی شده تبدیل به فایل بیتی شده و سپس در تراشه FPGA برد CW305 که XC7A100TFTG256 نام دارد قرار داده می‌شود. در مرحله بعد به وسیله زبان پایتون، متن آشکار ثابت و عدد تصادفی تولید می‌شود (پایتون از الگوریتم Mersenne Twister که یک الگوریتم با دوره بالاست برای تولید عدد شبه‌تصادفی بهره می‌برد) و به تراشه FPGA برای استفاده در جعبه جانشانی مقاوم‌سازی شده، داده شد. این فرآیند برای ۲۵۰۰۰ بار تکرار شد و در هر بار تکرار، توان مصرفی تراشه توسط برد Chipwhisperer اندازه‌گیری و به عنوان گروه اول ذخیره شد. سپس متن آشکار تصادفی و عدد تصادفی تولید و به تراشه FPGA برای استفاده در جعبه جانشانی مقاوم‌سازی شده داده شد. این فرآیند نیز برای ۲۵۰۰۰ بار تکرار شد و توان مصرفی تراشه در هر بار تکرار توسط برد Chipwhisperer اندازه‌گیری و به عنوان گروه دوم ذخیره شد. سپس آزمون T بر روی این دو گروه انجام گرفت که نتیجه آن در شکل ۹ آمده است.

همان طور که در شکل ۹ مشخص است، طرح مقاوم‌سازی شده در تعداد ۵۰۰۰۰ نمونه توان به دلیل اینکه مقدار آزمون بین ۴٫۵− و ۴٫۵ است دارای نشتی نیست. این امر نشان می‌دهد که روش مقاوم‌سازی ارائه شده در این مقاله برای مقاومت رمز قالبی SPEEDY در برابر حمله تحلیل توان موثر می‌باشد.

به منظور اطمینان بیشتر از صحت اجرای مقاوم‌سازی جعبه جانشانی علاوه بر روش آزمون T از روش مبتنی بر ابزار SILVER نیز استفاده می‌شود. در اینجا نیز کد VHDL جعبه مقاوم‌سازی تهیه شده و به همان روش ذکر شده وارد ابزار SILVER می‌شود. خروجی SILVER برای جعبه جانشانی مقاوم شده مطابق شکل ۱۰ است که نشان می‌دهد نشتی



شکل ۹. نمودار آزمون T با ۵۰۰۰۰ نمونه برای جعبه جانشانی مقاوم شده رمز SPEEDY



شکل ۱۰. نتیجه ارزیابی جعبه جانشانی امن شده رمز SPEEDY با استفاده از ابزار SILVER

جعبه جانشانی رمز SPEEDY برطرف شده است.

۶ نتیجه‌گیری

در این مقاله، امنیت رمز قالبی SPEEDY و پیاده‌سازی سخت‌افزاری آن در برابر حمله تحلیل توان مورد مطالعه و بررسی قرار گرفت. برای این منظور ابتدا لایه غیرخطی از جهت وجود نشت در برابر تحلیل توان مصرفی مورد ارزیابی قرار گرفت و نشان داده شد که دارای نشت است. با استفاده از این نشت می‌توان حمله تحلیل توان روی خود الگوریتم رمز قالبی SPEEDY اعمال کرده و کلید این الگوریتم رمز را به دست آورد. بعد از این کار، تلاش شد تا با استفاده از راهکاری مانند نقاب‌گذاری مبتنی بر دامنه، یک روش پیاده‌سازی امن برای رمز قالبی SPEEDY ارائه شود که در برابر حمله تحلیل توان مقاوم باشد. روش پیاده‌سازی جدید با استفاده از ابزار SILVER و روش آزمون T مورد بررسی قرار گرفت و نشان داده شد که نشتی مربوط به پیاده‌سازی پایه و بدون نقاب‌گذاری رمز قالبی SPEEDY را ندارد.

۷ تشکر و قدردانی

بخش‌های مربوط به ارزیابی جعبه جانشانی رمز قالبی SPEEDY و پیاده‌سازی آن با روش DOM از پایان‌نامه آقای رضا نادعلیزاده با عنوان «ارائه یک روش پیاده‌سازی امن مرتبه اول رمز قالبی SPEEDY در برابر حمله تحلیل توان» و تحت راهنمایی آقایان دکتر جوادعلیزاده و دکتر محسن جهانبانی تهیه شده است.

مراجع

[1] Leander, Gregor, Moos, Thorben, Moradi, Amir, and Rasoolzadeh, Shahram. The speedy family of block ciphers-engineering an ultra low-latency cipher from gate level for secure processor architectures. *Cryptology ePrint Archive*, 2021.

[2] Boura, Christina, David, Nicolas, Heim Boissier, Rachelle, and Naya-Plasencia, María. Better steady than speedy: full break of speedy-7-192. in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 36–66. Springer, 2023.

[3] Mangard, Stefan, Oswald, Elisabeth, and Popp, Thomas. *Power analysis attacks: Revealing the secrets of smart cards*, vol. 31. Springer Science & Business Media, 2008.

[4] Moradi, Amir, Poschmann, Axel, Ling, San, Paar, Christof, and Wang, Huaxiong. Pushing the limits: A very compact and a threshold implementation of aes. in *Advances in Cryptology–EUROCRYPT 2011: 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings 30*, pp. 69–88. Springer, 2011.

[5] Schneider, Tobias and Moradi, Amir. Leakage assessment methodology: A clear roadmap for side-channel evaluations. in *Cryptographic Hardware and Embedded Systems–CHES 2015: 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings 17*, pp. 495–513. Springer, 2015.

[6] Knichel, David, Sasdrich, Pascal, and Moradi, Amir. Silver–statistical independence and leakage verification. in *Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part I 26*, pp. 787–816. Springer, 2020.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2024, Volume 22, Number 2 (pp. 87–94)
https://monadi.isc.org.ir

Presented at the ISCISC 2024 in Tarbiat Modares University & Research Institute for Information and Communication Technology, Tehran, Iran

Investigation of power analysis attack on the SPEEDY block cipher and countermeasure using domain-oriented masking (DOM) method★

Keivan Khoormehr, Javad Alizadeh * and Mohsen Jahanbani

Masaf Laboratory, Faculty of Computer, Network, and Communications, Imam Hossein Comprehensive University, Tehran

ARTICLE INFO.

Keywords:
Power analysis attack
SPEEDY block cipher
Countermeasure
DOM method

Type: Research paper

ABSTRACT

Side-channel attacks, particularly power analysis attacks, pose a significant threat to the security of block cipher applications in hardware. These attacks can be executed using three primary methods: Simple Power Analysis (SPA), Differential Power Analysis (DPA), and Correlation Power Analysis (CPA). This paper examines the vulnerability of the SPEEDY block cipher to such power analysis attacks. In the first section, we demonstrate that the non-linear layer of the SPEEDY block cipher is susceptible to information leakage when subjected to power analysis attacks. By implementing the cipher in hardware and utilizing 1000 input samples, we establish that key-recovery attacks are feasible. The second section focuses on countermeasures to enhance the security of the SPEEDY block cipher against power analysis attacks. We propose a secure implementation method that employs Domain-Oriented Masking (DOM). Using the SILVER tool and the T-test method, we show that the secured version of the SPEEDY block cipher effectively mitigates the vulnerabilities and information leakages present in the original version when exposed to power analysis attacks.

© 2024 ISC

★ The ISCISC 2024 Program Committee effort is highly acknowledged for reviewing this paper.
* Corresponding author
Email addresses: khoormehr@ ihu.ac.ir (Keivan Khoormehr), jaalizadeh@ ihu.ac.ir (Javad Alizadeh), mjahanbani@ ihu.ac.ir (Mohsen Jahanbani)
© 2024 ISC. All rights reserved.