فصلنامه علمی مطالعات قدرت نرم
دوره ۱۳، شماره ۲، شماره پیاپی (۳۳)، تابستان ۱۴۰۲، ص ۲۰۰ ـ ۱۷۵
مقاله پژوهشی DOR:20.1001.1.23225580.1402.13.2.11.5

بررسی و تبیین جنگ الکترونیک و استراتژی‌های مقابله با آن (مطالعه موردی سامانه‌های رمزنگاری در زیرساخت‌های کشور)

سید حمیدرضا موسوی[۱]

تاریخ دریافت: ۱۴۰۲/۰۳/۱۰ تاریخ پذیرش: ۱۴۰۲/۰۶/۲۵

چکیده:

اساسی‌ترین جنبه بررسی و تبیین دیدگاه صاحب نظران نظامی غرب در باب جنگ‌های آینده نه تنها جنگ های فیزیکی با ادوات انفجاری نیست بلکه مبتنی بر ادوات بدون وزن است که می‌تواند قدرت مقابله را برای کشور ایران افزایش دهد. یکی از این جنگ‌ها، جنگ الکترونیک و مباحث پیرامون آن از جمله کدگذاری و تحلیل الکترومغناطیسی به عنوان جنگی نوین در عرصه بین‌المللی است. جنگ الکترونیک یعنی هر عملی است که شامل استفاده از طیف الکترومغناطیسی یا انرژی هدایت شده برای کنترل طیف، حمله به دشمن یا جلوگیری از حمله دشمن است. اصولا در این نوع جنگ دو هدف دنبال می‌شود اول به هم ریختن سیستم‌های الکترونیکی حریف و دوم استخراج داده و نفوذ به کانالهای رادیویی است. جنگ الکترونیک را می‌توان از طریق هوا، دریا، زمین، یا فضا توسط سیستم‌های سرنشین دار و بدون سرنشین استفاده کرد و می‌تواند انسان، ارتباطات، رادار یا دارایی‌های دیگر (نظامی و غیرنظامی) را هدف قرار دهد. در این مقاله سعی شده است یکی از روش‌های مقابله با حملات مبتنی بر جنگ الکترونیک با رویکرد مقاوم کردن سامانه‌های زیر ساخت کشور از جمله نیروگاههای تولید برق، سامانه های پدافندی و استراتژیک کشور با مقاوم سازی سامانه‌های رمز نگاری تبیین کرد. مشکل اصلی در مدیریت زیرساختهای کشور عدم وجود ارتباط با مراکز دیگری با استفاده ازخطوط ایمن غیر بیسیم یا نوری است. لذا پروسه جنگ رادیویی به خاطر وجود کانالهای رادیویی بسیار کاراتر است. که شامل ارتباطات رادیویی، ایجاد اختلال در ارتباطات رادیویی دشمن و شنود(استراق سمع) گفتگوهای دشمن است. در این مقاله سعی شده است ارتباط موجود بین زیر ساختها را به طوری ایمن کرد که حتی در صورت نفوذ دشمن به کانالهای جانبی نتوانند به محتوی اصلی داده‌ها دسترسی پیدا کنند. نتایج شبیه سازی‌های استقامت بالای ۹۹,۷ درصد در الگوریتم AES 256 را نشان می‌دهد.

واژگان اصلی: رمزنگاری، جنگ الکترونیک، زیرساخت، جنگ مدرن.

۱. استادیار، دانشکده مهندسی برق و کامپیوتر، واحد زنجان، دانشگاه آزاد اسلامی، زنجان، ایران (نویسنده مسئول)
hamidrezaznu@gmail.com

مقدمه

اگر نگاهی به تاریخ جهان بیندازیم با جنگ‌های بی‌شماری روبه‌رو خواهیم شد؛ جنگ‌هایی که اگر اتفاق نمی‌افتادند یا نتیجه نبردها تغییر می‌یافت، سرنوشت بشر تغییر داده می‌شد و در دنیای متفاوتی زندگی می‌کردیم. بشر همواره به‌دنبال سلطه‌گری بر انسان‌ها و اراضی خارج از قلمروی خود بوده است و حتی پیشرفت علم نیز نتوانست افساری برای جهان‌خواهی فرمان‌روایان بسازد.

درواقع علم در رسیدن فرمان‌روایان به اهدافشان سرعت نیز بخشیده است. زمانی‌که مغول‌ها به جنگ با خوارزمشاهیان پرداختند، دیوارهای بلند شهرهای خوارزمشاهیان مانند سدی در برابر مغول‌ها ایستادگی کردند؛ اما علم تولید منجنیق توانست به مغول‌ها برای فتح شهرهای آن زمان کمک فراوانی کند. منجنیق‌ها دستگاه‌هایی برای پرتاب سنگ‌های بزرگ به دژها و دیوارهای بلند بودند تا فتح شهری مستحکم، امکان‌پذیر شود. این دستگاه‌ها به حالتی بودند که امکان جداسازی قطعات آن‌ها برای حمل ساده‌تر وجود داشت و هنگام استفاده از آن‌ها، افرادی آموزش‌دیده شروع به نصب و راه‌اندازی منجنیق‌ها می‌کردند؛ اما استفاده از منجنیق‌ها به افرادی باهوش در زمینه ریاضی نیاز داشت تا مختصات دقیق برای پرتاب سنگ‌ها را بررسی کنند(سازدار و همکاران، ۱۳۹۲: ۲۹).

در سال ۲۰۲۲ جنگ اوکراین آغاز شد. اگرچه قبل از آن برآوردها از آغاز یک درگیری کوتاه با پیروزی احتمالی مسکو حکایت داشت اما گذشت زمان ابعاد این منازعه را پیچیده تر کرده است(زبردست، ۱۴۰۱). ورود آمریکا و دیگر کشورهای عضو ناتو به جنگ با مسکو و ارسال آشکار کمک های تسلیحاتی و مالی به کی یف برای دیگر کشورهای جهان نیز نکات قابل توجهی در رابطه ادوات در جنگ های مدرن را به همراه داشته است. «موسسه بین المللی مطالعات استراتژیک» (The International Institute for Strategic Studies) در گزارشی مبسوط با عنوان «درس های جنگ اوکراین» آورده است جنگ های بزرگ آزمونی برای نیروهای مسلح کشورها و بررسی اوات جدید بخصوص ادوات جن الکترونیک است و جنگ روسیه و اوکراین نیز از این قاعده مستثنی نیست. اگرچه در حال حاضر تنها دو کشور به جنگ مستقیم می پردازند اما بسیاری از کشورهای دیگر نیز در این مخاصمه از نظر سیاسی، دیپلماتیک و اقتصادی درگیر هستند و با ارائه کمک های نظامی و اطلاعاتی به کی‌یف در نبرد مشارکت دارند. غربی ها پشتیبانی نظامی قابل توجهی را با ارسال طیف گسترده ای از سلاح ها، مهمات، قطعات یدکی و آموزش نظامی به اوکراین به عمل آورده اند. به عبارت دیگر شاهد یک تلاش بین المللی برای جلوگیری از پیروزی روسیه در جنگ هستیم. گرچه نمی توان در مورد

نتیجه و مدت این جنگ با قاطعیت سخن گفت اما برخی از تحولات در اوکراین، ویژگی های کلیـدی جنگ مدرن بین دولت ها را نشان می دهد. جنگ یک رقابت بسیار پویا شامل عملی سازی اراده ها در حوزه‌های مختلف است. این جنگ خاطرنشان می کند که عنصـر اصـلی در توانمنـدی نظـامی میـزان کارآیی است؛ ضمن اینکه کمیت ها هم در میدان جنگ و هم در زرادخانه ها هنوز مهم هسـتند. علـاوه بر این دسترسی به بسیاری از سلاح های دقیق فعلی به دلیل هزینـه، پیچیـدگی و زمـان تولیـد محـدود هستند و مخفی کردن نیروها و اطلاعات از چشم ماهواره ها و پهپادها بـه شـدت دشـوار شـده اسـت (سلامی و همکاران، ۱٤۰۲، ۱۲۰). پرنده های بدون سرنشین هم نقش فزاینده ای را در جنگ زمینی ایفا می کند(اصغرزاده و میرزائـی، ۱۳۹۹: ۲۰۲). بـه طوریکـه در دنیـای کنـونی رمزنگـاری و حواشـی آن کاربردهای وسیعی در صنعت یافته است و از طرفی نیاز به دسـتیابی بـه سـرعتهای بالـاتر و از طرفـی بالابردن امنیت موجب شده است از پیاده سازی سخت افزاری آنها استفاده شود. امروزه کاربردهای نوین دیگری مانند هدایت نفرات و موشک‌ها و کشتی ها، قایق ها و زیردریایی ها با دستگاه‌های الکترونیکی به جنگ الکترونیک افزوده شده‌است(اصغرزاده و میرزائی، ۱۳۹۹: ۷۳). دستگاه جمینـگ از ایـن جملـه دستگاه‌هاست که با ایجاد چگالی از انرژی در مسیر سیگنال فرستاده می‌شود و با افزودن پارازیت (نویز) به آن، رادار را مختل می‌کند. البته می‌توان آن را شناسایی کرد. در این بـین مشـکل اصـلی در مـدیریت سامانه ها عدم وجود ارتباط با مراکز دیگری با استفاده ازخطوط ایمن غیر قابل نفوذ است. (فرحبخت و دهقانی، ۱۳۹۸: ۱۹۹) در خطوط بیسیم به سادگی دشمن می تواند عمل شنود و استراق سمع را انجـام دهد برای همین منظور در این مقاله سعی بر آن شده است تا با استفاده از رمزنگـاری سـخت افـزاری منعطف تا حد ممکن ایمنی کانال ارتباط مابین را بالا برد. برای راحتی طراحی و کاهش زمان رسیدن به بازار استفاده از ادوات قابل برنامه ریزی افزایش یافته اسـت(Brier, 2004: 16). پیـاده سـازی هـای معمولی بر روی FPGA برای کاربردهای رمزنگاری خیلی مناسب نیست زیرا اطلاعات زیـادی از آن نشت می کند(Popp, 2007: 535)، از جمله ی این اطلاعات، اطلاعات کانال جانبی است که به نحو روزافزونی که حملات کانال جانبی را ممکن می سازد. اطلاعات کانال جانبی شامل بررسی زمان اجرای پروسه، اعمال خرابی، تحلیل توان مصرفی و تحلیل الکترومغناطیسـی است(اصـغرزاده، ۱۳۹۹: ۷۳). در پیاده سازی های معمولی اعمال تمام حملات بالا ممکن است که با استفاده از روش هایی همچون اضافه کردن اتفاقی سیکلهای اضافه، یکسان سازی مصرف توان و ... سعی در کاهش این نوع حملـات شـده است ولی چندان موفقیتی حاصل نشده است(Mengard, 2002: 343),(Bevan, 2002: 327).

در مقابل پیاده سازی های ساده پیاده سازی های مقاوم با استفاده از قابلیت های جدید در FPGA های امروزی می تواند گام مثبتی در حل این ضعف ذاتی باشد به طوری که روش های جدید تاحدود خیلی زیادی غیر قابل پیش بینی و ردیابی هستند، که می توانند حملات کانال جانبی را تا حد زیادی خنثی سازند. در مورد حملات توانی FPGA هایی که تاکنون پیاده سازی شده اند، مصرف توان متفاوتی ندارند، که همین مسأله باعث آسیبپذیری آنها می شود. در این مقاله سعی بر آن شده است تا روش های مختلف مقاوم سازی با هم مقایسه شده، و در نهایت روشی جدید برای این کار ارائه شود. یک توپولوژی برای این کار پیشنهاد شده است که مبتنی بر تغییر در ساختار گیتهای پایه FPGA ها هست، که روش فوق با کمی تغییر در گیت XNOR توانسته است تا حدود خیلی زیادی سطح مقاومت را بالا ببرد، همچنین به منظور دستیابی به یک روش کاملا مورد قبول ۳ پارامتر توان مصرفی، فضای اشغالی و سرعت عملکرد سیستم همراه به عنوان پارامترهای اصلی در نظر گرفته شده اند. در پایان نیز برای آزمودن روش های پیشنهادی، الگوریتم رمزنگاری AES بر روی FPGA پیاده شده و حمله ی توانی تفاضلی به داده های توانی آن اعمال شده است.. در این مقاله در بخش دوم درباره انواع جنگ الکترونیک و رمز نگاریها در سیستم های زیرساختی بحث شده است و در بخش سوم انواع حملات و روشها مرسوم مشابه بیان گردیده است در بخش چهارم روش پیشنهاده ما که مبتی بر به هم ریخت توان مصرفی با استفاده از نحوه پیاده سازی شرح داده شده است و در نهایت در بخش پنجم نتایج حاصل از شبیه سازی آورده شده است.

۱- جنگ الکترونیک

افراد یگان جنگ الکترونیک می‌کوشند تحرک هر فرستنده‌ای را کشف، صدای هر گوینده‌ای را ضبط و هرگونه سامانه الکترونیکی تهدیدآمیز را نابود کنند . بکارگیری سایت‌های شنود متحرک مجهز به سامانه‌های رهگیری مراقب، استراق سمع، ضبط و ثبت فرستنده‌های فعال دشمن، پخش پارازیت شنود و فریب الکترونیکی اهمیت ویژه‌ای در این‌گونه عملیات دارد(سلامی و همکاران، ۱۴۰۲: ۱۲۰). تجهیزات شنود، سامانه‌های اختلالگر، جهت‌یاب‌های مختلف، رادارها و سامانه‌های کشف و رهگیری و رمزشکن از لوازم یگان جنگال است. رمزنگاری فرآیندی است که در طی آن، داده‌ها از فرم عادی خود خارج و به صورتی تبدیل می‌شوند که بدون داشتن اطلاعات لازم (کلید رمز) خواندن آن‌ها تقریباً غیرممکن است؛ بنابراین در این روش با رمز نمودن داده‌ها از دسترسی افراد غیرمجاز به داده‌ها

جلوگیری شده و محرمانگی داده به دست می‌آید. در این روش ابتدا در مبدأ عمل رمزنگاری انجام‌شده و سپس رمز شده داده‌ها به مقصد ارسال می‌گردند. حمله‌کننده‌ای که استراق سمع می‌کند و بسته‌های داده‌ها را در حین انتقال از شبکه دریافت می‌کند، رمز شده داده‌ها را به دست می‌آورد که برای او قابل‌استفاده نیست. دریافت‌کننده داده‌ها در مقصد هم داده رمز شده را دریافت می‌نماید ولی او به دلیل اینکه، اطلاعات رمزگشایی داده‌ها را دارد می‌تواند داده‌ها را رمزگشایی نموده و استفاده کند. برای رمزنگاری داده‌ها دو روش متقارن و نامتقارن وجود دارد. ایده رمزنگاری متقارن از سال‌های پیش وجود داشته است و مسئله جدیدی نیست ولی رمزنگاری نامتقارن از اصول ریاضی و الگوریتم‌های پیچیده‌ای استفاده می‌کند و روش جدیدی در رمزنگاری داده‌ها به شمار می‌آید (Tiri, 2008).

۱-۱. رمزنگاری متقارن داده‌ها

در این روش رمزنگاری، ترکیبی از جابجایی و جایگزینی داده‌ها در مراحل متعدد انجام می‌شوند تا پیچیدگی لازم برای داده‌ها به وجود آید. همچنین برای انجام عملیات رمزنگاری از یک کلید مشترک و محرمانه بین فرستنده و گیرنده انجام می‌شود. در این روش داده در مبدأ با کلید مشترک، رمز شده و به مقصد ارسال می‌گردند و در مقصد نیز داده‌ها با کلید مشترک رمزگشایی می‌شوند. در رمزنگاری متقارن فرض بر این است که حمله‌کننده از الگوریتم رمزنگاری مطلع است و تنها بر محرمانگی کلید رمزنگاری مشترک تکیه می‌شود. به‌طورکلی هر چه طول کلید بیشتر باشد مدت‌زمان بیشتری برای شکستن داده‌ها صرف می‌گردد و امنیت بیشتری به دست می‌آید. با توجه به قدرت پردازش فعلی، انتخاب کلیدهای بیشتر از ۱۲۸بیت مناسب به نظر می‌رسد. همچنین کلیدهای رمزنگاری مدتی پس از استفاده باید تعویض شوند و کلیدهای جدید حتی‌الامکان باید به‌صورت تصادفی انتخاب گردند تا حداکثر امنیت به دست آید. الگوریتم‌های رمزنگاری متقارن به ۲ دسته الگوریتم‌های بلاکی[۱] و جریانی و داده‌ها بیت به بیت رمزنگاری و یا رمزگشایی می‌شوند. الگوریتم‌های جریانی سریع‌تر از بلاکی هستند. الگوریتم‌های همانندDES[۲]، بلاکی و الگوریتم‌هایی همانند RCCL، جریانی است البته لازم به ذکر است که رمزنگاری متقارن، احراز هویت را نیز فراهم می‌آورد. درصورتی‌که داده رمز شده‌ای دریافت شد با توجه به کلید مورداستفاده می‌توان از هویت شخص ارسال‌کننده داده نیز مطمئن شد زیرا این کلیدها محرمانه فرض می‌شوند. رمزنگاری متقارن از کارایی مطلوبی برخوردار است و تأخیر کمی را در عملیات

۱ Black

۲ Data Encryption Standard

رمزنگاری و رمزگشایی داده‌ها فراهم می‌آورد؛ بنابراین از آن می‌توان برای رمزنگاری حجم بزرگی از داده‌ها استفاده نمود. از این نوع رمزنگاری در پروتکل‌های امنیتی محیط باسیم و بی‌سیم به‌طور گسترده استفاده می‌شود. الگوریتم 3DES، DES، IDEA [1]، RC4 [2] و غیره از الگوریتم‌های متقارن می‌باشند (Rührmair, 2014: 476).

۲-۱.رمزنگاری نامتقارن داده‌ها

رمزنگاری نامتقارن یا رمزنگاری کلید عمومی، بزرگ‌ترین و شاید تنهاترین انقلاب موجود در تاریخ رمزنگاری است. در این الگوریتم به‌جای جایگشت و جایگزینی داده‌ها، توابع ریاضی استفاده می‌شود و به‌جای یک کلید محرمانه مشترک، یک کلید عمومی و یک کلید خصوصی ایجاد و کلید عمومی در اختیار همه و کلید خصوصی تنها در دسترس کاربر قرار می‌گیرد. برای محرمانگی کلید خصوصی، رمز عبوری برای دسترسی پایگاه داده کلید خصوصی در نظر گرفته می‌شود. مفهوم رمزنگاری کلید عمومی، در پی تلاش برای حل دو مشکل توزیع کلید به روش امن و امضاء دیجیتال به وجود آمده و دارای دو خصوصیات مهم و اساسی زیر می‌باشند. ۱- به‌طور محاسباتی محاسبه کلید رمزگشایی از کلید رمزنگاری غیرممکن است. ۲- هر دو کلید عمومی و خصوصی را می‌توان برای رمزنگاری استفاده نمود. البته برای رمزگشایی باید کلید دیگر استفاده نمود. در این روش رمزنگاری، ابتدا کلید عمومی مقصد به روشی معتبری فراهم‌شده و سپس داده‌ها توسط کلید عمومی مقصد، رمزنگاری و به آن ارسال می‌گردند. حمله‌کننده بین مسیر مبدأ و مقصد می‌تواند کلید عمومی مقصد را به‌راحتی به دست آورد ولی با این کلید، قادر به رمزگشایی داده‌ها نخواهد بود. در مقصد، داده‌ها توسط کلید خصوصی، رمزگشایی و استفاده می‌شوند. البته عکس این روش محرمانگی داده‌ها را به وجود نمی‌آورد زیرا درصورتی‌که داده‌ها ابتدا توسط کلید خصوصی رمزنگاری شوند و سپس منتقل گردند چون همه افراد کلید عمومی را می‌دانند؛ بنابراین همه می‌توانند داده‌های رمز شده را رمزگشایی نمایند و محرمانگی داده‌ها از دست می‌رود. برای به دست آوردن کلید عمومی به روشی معتبر می‌توان از گواهی دیجیتال استفاده نمود. در مقایسه با رمزنگاری متقارن این روش از محاسبات پیچیده و زمان‌گیری استفاده می‌نماید و لذا برای رمزنگاری حجم زیادی از داده بکار نمی‌رود. اغلب از این نوع رمزنگاری، برای ارسال مقادیر کمی از داده‌ها کلیدهای رمزنگاری متقارن استفاده می‌شود.

[1] International Data Encryption Algorithm

[2] Ronald Rivest of RSA

متداول‌ترین الگوریتم برای رمزنگاری، کلید عمومی الگوریتم RSA[1] است (Tiri, 2004: 246).

۲-انواع حملات نرم افزاری

۲-۱- تغییر اطلاعات

در این نوع حمله فعال، اطلاعات در حین انتقال به مقصد موردحمله قرار می‌گیرد و جامعیت داده‌ها از دست می‌رود. حمله‌کننده با دریافت اطلاعات، آن‌ها را تغییر می‌دهد و یا آن‌ها را با اطلاعات دیگر جایگزین می‌کند. مقصد نیز این مسئله را تشخیص نداده و داده‌ها را استفاده می‌نماید. برای جلوگیری از این نوع حمله از توابع چکیده ساز[2] استفاده می‌شود (Bilski,2010:1049).

۲-۲- جعل هویت

در این نوع حمله فعال، حمله‌کننده خود را به‌عنوان یک کاربر مجاز به سامانه‌های محلی معرفی می‌کند و بدین ترتیب از سرویس‌های مختلف شبکه محلی استفاده می‌کند. برای جلوگیری از این نوع حملات و فراهم کردن احراز هویت کاربران و نرم‌افزارها از امضاء دیجیتال استفاده می‌شود. در این روش، حمله‌کنندگان از ارائه سرویس‌های یک موسسه جلوگیری می‌نمایند. راه‌اندازی این نوع حملات راحت است و اغلب از روش‌های جعل هویت و نیز ارسال مقادیر زیادی از سامانه‌های پروتکل اینترنت[3] انجام می‌گیرد. این حملات به‌اختصار DOS[4] نامیده می‌شود؛ و جزء حملات فعال هستند. با استفاده از دیواره آتش می‌توان این حملات را کاهش داد(Bilski, 2010: 1049).

۲-۳- استراق سمع

در این حمله نوع حمله غیرفعال[5]، اطلاعات تغییر نمی‌یابند ولی محرمانگی آن‌ها از دست می‌رود. اگر بخواهید اطلاعات را به متن عادی و رمز نشده به سامانه‌های راه دور ارسال کنید آنگاه ممکن است این اطلاعات توسط افراد غیرمجاز دریافت شوند. دستبرد اطلاعات ممکن است در مکان‌های مختلفی همانند شبکه‌های محلی، سوئیچ‌های انتقال داده‌ها و یا شبکه اینترنت انجام شود.

[1] Rivest Shamir Adelman
[2] Hash function
[3] Internet Protocol
[4] denial-Of-Service
[5] Passive

هم‌اکنون نرم‌افزارهای مختلفی برای دریافت اطلاعات مختلف از روی شبکه محلی وجود دارد و ویروس‌ها و حمله‌کنندگان نیز می‌توانند اطلاعات انتقال‌یافته بر روی یک شبکه عمومی را دریافت کنند. برای جلوگیری از این مشکل امنیتی از فن‌های رمزنگاری متقارن و نامتقارن داده‌ها استفاده می‌شود (Bilski, 2010: 1049).

۳- معرفی انواع حملات سخت‌افزاری

مهمترین چالش در ابزارهای مورد استفاده در کاربردهای رمزنگاری و حساس، چگونگی حفظ امنیت آن‌ها است. در دو دهه گذشته نوعی از حملات، تحت عنوان حملات سخت‌افزاری معرفی شده که قادر است امنیت این ابزارها را به مخاطره اندازد. این نوع از حملات مستقیما با قطعه پیاده سازی شده در ارتباط است، این نوع از حملات در سه دسته غیر مخرب، نیمه مخرب و مخرب دسته بنده می شوند که در ادامه توضیح کامل آن داده شده است.

۳-۱- حملات غیرمخرب

بیشتر حملات غیرمخرب به‌صورت تغییرات در ولتاژ تغذیه و یا سیگنال کلاک تعریف می‌شوند. این تغییرات می‌توانند برای غیرفعال‌کردن حافظه و یا مجبور کردن پردازنده برای اجرای عمل اشتباه، مورد استفاده قرار گیرند. به همین دلیل برخی از پردازنده‌های امنیتی دارای مدار تشخیص تغییرات ولتاژند ولی باز هم اگر تغییرات خیلی سریع باشند ممکن است تشخیص داده نشوند. تغییرات سریع در ولتاژ تغذیه و فرکانس کلاک می‌توانند برای تأثیرگذاری در کدگشاها[1] در یک پردازنده و اجرای دستورات مشخصی نیز به کار بروند. حمله‌ی ممکن دیگر تحلیل جریان[2] هست. توسط یک مبدل آنالوگ به دیجیتال می‌توانیم نوسانات در جریان مصرفی وسیله‌ی موردنظر را اندازه بگیریم. درایورهایی که بر روی باسهای داده و آدرس قرار دارند اغلب شامل حدود ۱۲ معکوس‌کننده‌ی موازی به ازای هر بیت هستند، که هر کدام از این درایورها باید بارهای با ظرفیت خازنی بالا را درایو کنند. به همین دلیل در حالات گذرای مربوط به تغییر وضعیت باسها، دقیقاً بعد از لبه‌ی کلاک جریانی در حدود ۰,۵ تا ۱ میلی‌آمپر مصرف می‌شود. بنابراین یک مبدل آنالوگ به دیجیتالِ ۱۲بیتی برای تخمین تعداد تغییراتی که در هرلحظه در بیت‌های باسها اتفاق می‌افتد، کافی هست. حمله‌ی غیر-

[1] Decoders
[2] Current Analysis

مخرب بعدی در مورد وسایل امنیتی حمله‌ی باقی‌ماندگی داده‌ها[1] است. این پدیده، ویژگی‌ای از حافظه‌های فرار در نگهداری اطلاعات برای مدت زمانی حتی بعد از قطع تغذیه هست. توسط فریز کردن داده‌ها این زمان نگه‌داری را می‌توان به حدی افزایش داد که یک حمله‌گر بتواند داده‌ها را از حافظه استخراج کند. البته این ویژگی تنها برای حافظه‌ی فرار نیست و حافظه‌های غیر فرار نیز دچار ایراد مشابهی هستند.

راه دیگر برای انجام حمله از نوع غیرمخرب کار کردن بر روی سیگنال‌های رابط کاربری و یا کار بر روی خود پروتکل‌ها و الگوریتم‌های استفاده شده در دستگاه هست. مسلماً یک سامانه که حتی از لحاظ سخت‌افزاری دارای امنیت بالایی باشد، اگر پروتکل‌های آن به‌طور غلط پیاده‌سازی شده باشند امکان حمله به آن وجود خواهد داشت. برخی از میکروکنترلرها و کارت‌های هوشمند دارای یک رابط آزمایش کارخانه‌ای می‌باشند که به تولیدکنندگان اجازه‌ی دسترسی به حافظه‌ی درون تراشه و انجام آزمایش‌ها لازمه روی تراشه را می‌دهد. اگر یک حمله‌گر بتواند راهی برای نفوذ به این رابط بیابد، او می‌تواند به‌راحتی اطلاعات ذخیره‌شده‌ی درون تراشه را به دست آورد. مثلاً حمله‌گر می‌تواند به تراشه سیگنال‌ها و سطوح منطقی متفاوتی را اعمال کند تا سرانجام تراشه به‌طور اتفاقی وارد حالت آزمایشی خود شود. این کار در مورد میکروکنترلرها اغلب جواب می‌دهد ولی در مورد کارت‌های هوشمند معمولاً امکانی وجود دارد تا در صورت تغییرات غیرمجاز در کارت بلافاصله کارت را می‌سوزد.

۳-۱-۱ حملات اخلال

حملات اخلال[2] تغییرات سریع در سیگنال‌های داده‌شده به یک دستگاه می‌باشند و برای این طراحی‌شده‌اند تا بر عملکرد عادی آن وسیله اثر بگذارند. معمولاً اخلال در سیگنال‌های کلاک و منبع تغذیه قرار داده می‌شوند، اما یک اخلال می‌تواند میدان الکتریکی خارجی و یا یک پالس الکترومغناطیسی نیز باشد. مثلاً با قرار دادن دو سوزن فلزی در فاصله‌ی چند صد میکرومتری از سطح تراشه‌ی یک کارت هوشمند، و سپس با اعمال ولتاژ بالا در یک زمان کوتاه (کمتر از یک میکروثانیه)، می‌توان یک میدان الکتریکی درون تراشه به وجود آورد که دارای قدرت کافی برای تغییر موقتی ولتاژهای آستانه ترانزیستورهای نزدیک آن باشد(موسوی و همکاران، ۱۴۰۱: ۳۹).

[1] Data Remanence

[2] Glitch Attacks

هـر ترانزیسـتور و مسـیرهای ارتبـاطی آن بـا عناصـر اطـرافش مثـل یـک عنصـر مقـاومتی– خازنی(RC) با یک تأخیر زمانی مشخصی رفتار می‌کند. حـداکثر فرکـانس قابـل اسـتفاده بـرای یـک پردازنده نیز توسط حداکثر تأخیر بین عناصرش محاسبه می‌شود. از طرفی هر فیلیپ فلـاپی[1] در داخـل تراشه دارای یک پنجره‌ی زمانی است که در این پنجره‌ی زمانی ولتـاژ ورودی‌اش را مـی‌گیـرد و بعـد بسته به این ولتاژ، مقدار خروجی‌اش را تغییر می‌دهد. این‌ها مواردی هسـتند کـه غالبـاً در حملـه‌هـای اخلال مورد استفاده قرار می‌گیرند. مثلاً به کمک یک اخلال در کلـاک و یـا یـک اخلـال در ولتـاژ، و بـا توجه به تاخیرات بین عناصر، می‌توان باعث نمونه‌برداری اشتباه فلیـپ‌فلاپهـا شـد. در حملـات اخلـال به‌طورکلی با تغییر دادن عوامل مختلف، پردازشگر مجبور به اجرای دستورات اشتباه دیگری می‌شود.

الف) اخلال در کلاک: ایجاد خطا به کمک اخلال در کلاک[2] معمولاً آسان‌ترین و عملی‌ترین نـوع اخلال هست. در کاربردهای واقعی، اخلال‌ها معمولاً برای جابه‌جایی بین دستورات پـرش‌هـای شـرطی با خود دستورات شرطی به کار می‌روند. این‌ها با ممانعت از اجرا شدن کـدهای امنیتـی، مثلـاً کـدهای بررسی احراز هویت، سعی در ایجاد رخنه‌های امنیتی دارند. همچنین اخلال مـی‌توانـد بـرای گسـترش دادن و بیشتر کردن زمان اجرای حلقه‌ها نیز استفاده شود.

برای انجام یک حمله از نوع اخلال در کلاک، فرکانس کلاک پردازنده باید بـرای بیشـتر از نصـف دوره–تا نهایتاً یک دوره‌ی کامل– به‌طور موقت افـزایش یابـد تـا برخـی از فلیـپ‌فلاپهـا ورودیشـان را زودتر از موعد و قبل از اینکه حالت جدیدی رخ دهد، نمونه‌برداری کنند.

چون حملات اخلال در کلاک معمولاً در جریان دستورات پردازنده پیاده‌سازی می‌شوند، آنهـا در مورد وسایلی که از حفاظت‌های امنیتی با پیاده‌سازی سخت‌افزاری بهره می‌برنـد، خیلـی مـؤثر نیسـتند. بنابراین استفاده از این اخلال‌ها برای حمله به میکروکنترلرها و یا برخی کارت‌های هوشـمند، عملـی‌تـر هست. البته استفاده از اخلال در کلاک در برخی از میکروکنترلرها نیز خیلی دشوار هسـت. بـرای مثـال میکروکنترلرهـای خـانواده‌ی MSP430 از تگـزاس اینسـترومنت از یـک مولـد کلـاک RC درونـی استفاده می‌کنند. در این حالت سنکرون شدن با کلـاک داخلـی و تخمـین زمـان دقیـق حملـه سـخت هست. برخی از کارت‌های هوشمند نیز در روند اجرایی دستورات توسط پردازنده تـاخیرات تصـادفی را اعمال می‌کنند، که این کار حمله‌ی اخلال را خیلی سخت‌تر می‌کند. در اینجا استفاده از تحلیـل تـوان

[1] Flip-Flop
[2] Clock Glitch

می‌تواند مؤثر باشد اما نیاز به تجهیزات گران‌قیمت و پیچیده برای استخراج سیگنال مرجع در هرلحظه دارد.

ب) اخلال در تغذیه: نوسانات ولتاژ تغذیه می‌تواند سطح آستانه‌ی ترانزیستورها را تغییر دهد. درنتیجه برخی از فلیپ‌فلاپها ممکن است در زمان متفاوتی ورودیشان را نمونه‌برداری کنند و یا وضعیت قطع‌کننده‌های امنیتی غلط خوانده خواهد شد. این به‌طور معمول با افزایش ولتاژ تغذیه یا افت آن در دوره‌ی زمانی خیلی کوتاهی (حدود ۱ تا ۱۰ کلاک) به دست می‌آید.

اخلال‌ها در تغذیه می‌توانند به میکروکنترلرها با هر نوع رابط برنامه‌نویسی اعمال شوند چراکه آنها می‌توانند هم بر عملکرد پردازنده و هم مدار امنیت فیزیکی تأثیر بگذارند. البته در کل اخلال در تغذیه نسبت به حمله‌ی اخلال در کلاک جهت بهره‌برداری سخت‌تر است چراکه علاوه بر عوامل زمانی، دامنه و زمان‌های بالاروندگی و پایین‌روندگی سیگنال‌ها نیز جزء متغیرهای مسئله محسوب می‌شوند.

۳-۱-۲- حملات زمانی

از بین حملات کانال جانبی[۱]، از لحاظ اجرا، حملات زمانی ارزان‌ترین نوع می‌باشند چراکه برای پیاده‌سازی این حملات نیازی به ابزار اندازه‌گیری پیچیده و گران‌قیمت نیست. اساس حملات زمانی تفاوت در زمان اجرای برخی عملیات امنیتی(مثل رمزنگاری‌ها) در یک تراشه هست. این زمان اجرای الگوریتم وابسته به طول داده‌های ورودی و طول کلید هست. اندازه‌گیری و تحلیل دقیق این زمان‌ها می‌تواند باعث به دست آوردن کلید خصوصی یک سامانه شود. این ایده اولین بار توسط کاچر[۲] (Kocher, 1999: 1) مطرح و منتشر شد. بعد از آن نیز برای شکستن الگوریتم‌های RSA، DES و حتی AES به‌طور مکرر استفاده شد که غالباً هم مؤثر بوده است.

برای اجرای این حمله نیاز به مجموعه‌ای از پیغام‌ها (داده‌های ورودی) به همراه زمان دقیق پردازش آنها هست. خیلی از الگوریتم‌های رمزنگاری دیده‌شده‌اند که مقابل این حملات آسیب‌پذیرند. علت اصلی این امر در پیاده‌سازی نرم‌افزاری الگوریتم‌ها هست. معمولاً کارهایی که برای بهینه‌سازی کدها انجام می‌شوند مثل کاهش حلقه‌ها و شرط‌ها، استفاده از حافظه‌ی کش[۳]، استفاده از دستورات پردازشی که دارای زمان اجرای ثابتی نیستند مثل ضرب و تقسیم، باعث ایجاد این آسیب‌پذیری‌ها می‌شوند.

۱ Side Channel Attacks

۲ Kocher

۳ Cache Memory

۳-۱-۳- حمله‌ی تحلیل توان

بعد از معرفی حملات کانال جانبی توسط کاچر در ۱۹۹۹، حملات تحلیل توان در جامعه‌ی رمزنگاری بسیار مورد توجه قرار گرفتند. اگرچه کارهای اولیه در این زمینه متهی به حملات روی کارت‌های هوشمند می‌شد ولی در سال‌های اخیر نشان داده‌شده است که بیشتر پیاده‌سازی‌های سخت‌افزاری توسط این حملات آسیب‌پذیر می‌باشند. به‌ویژه FPGA ها که گزینه‌ی مناسبی برای پیاده‌سازی الگوریتم‌های رمزنگاری می‌باشند، امنیتشان در مقابل این حملات تضمین شده نیست. اولین حمله‌ی تحلیل توان موفقیت‌آمیز بر روی FPGA ها توسط ارس[۱] و همکارانش در ۲۰۰۳ انجام شد. آنها این حمله را بر روی یک پردازنده‌ی رمزنگاری منحنی بیضوی[۲] انجام دادند و توانستند کلید سری را با تحلیل خطوط تغذیه به دست آورند. بعد از آن نیز مقالات گوناگونی قابلیت اعمال حمله‌ی تحلیل توان به FPGA ها را بررسی و تصدیق نمودند(موسوی و همکاران، ۱٤۰۱: ۳۹).

توان مصرفی یک وسیله‌ی محاسباتی وابسته به فعالیت کنونی آن دارد. به خاطر ماهیت ترانزیستورهای CMOS، مصرف توان یک تراشه مبتنی بر CMOS به‌جای وابسته بودن به خود وضعیت ترانزیستورها، به تغییر وضعیت‌های آنها وابسته است. با استفاده از یک مقاومت ۱۰ تا ۲۰ اهمی در خط تغذیه می‌توان نوسانات جریان ناشی از تغییر وضعیت‌ها را اندازه‌گیری کرد. برای به دست آوردن نتایج بهتر، اندازه‌گیری‌ها باید با وضوح حداقل ۱۲ بیت و فرکانس نمونه‌برداری ۵۰ مگاهرتز انجام شوند. این مقادیر به ما اجازه‌ی تشخیص تفاوت بین دستورالعمل‌های مختلف پردازنده و تخمین تعداد بیت‌های باس که در هرلحظه تغییر می‌کنند را می‌دهد. با میانگیری بر روی مقادیر جریانات و توان‌های مصرفی به تعداد زیاد، حتی سیگنال‌های کوچکی که از طریق باس انتقال نمی‌یابند نیز قابل‌تشخیص‌اند.

مقالات متعددی در مورد روش‌های مختلف تحلیل توان وجود دارند که می‌توانند برای شکستن تعداد زیادی از الگوریتم‌ها به کار بروند. فرآیند کلی تحلیل توان از لحاظ پیاده‌سازی نسبتاً آسان است و فقط نیاز به ابزار اندازه‌گیری معمولی که در حد چند هزار پوند هستند، دارد. به‌طورکلی ۲ نوع روش عمده‌ی تحلیل توان وجود دارد: تحلیل توان ساده[۳](SPA) و تحلیل توان تفاضلی[٤](DPA).

[۱] Ors
[۲] Elliptic Curve
[۳] Single Power Analysis
[٤] Differential Power Analysis

SPA به معنی مشاهده و بررسی مستقیم توان مصرفی سامانه‌ی مورد حمله در حین عملیات رمزنگاری است و بدین‌وسیله اطلاعاتی در مورد کلید سری به دست می‌آید. درصورتی‌که حمله‌گر الگوریتم رمزنگاری و یا نحوه‌ی پیاده‌سازی آن را بداند، می‌تواند به‌سادگی با بررسی دنباله‌ی دستورات پردازشگر، مخصوصاً دستورات شرطی و پرش‌ها، برخی از بیت‌های کلید را به دست آورد. در صورت بررسی نتایج عملکردهای منطقی و محاسباتی مثل وضعیت پرچم‌های منفی یا صفر و یا علامت، می‌توان اطلاعات بیشتری از کلید به دست آورد.

DPA یک روش قدرتمندتر هست، چون در آن حمله‌گر نیاز به دانستن خیلی از جزئیات در مورد الگوریتم رمزنگاری پیاده‌شده ندارد. او در عوض از تحلیل آماری برای استخراج اطلاعات حین رمزنگاری استفاده می‌کند. روش‌های آماری تفاوت‌های کوچک در مصرف توان را به‌سادگی متمایز می‌سازند.

مؤلفه‌های توان مصرفی اغلب شامل نویز نیز می‌باشند. نویز خارجی می‌تواند با طراحی صحیح مسیرهای اخذ سیگنال و استفاده‌ی دقیق از ابزار اندازه‌گیری کاهش یابد. غالباً برای افزایش سطح سیگنال به نویز می‌توان تعداد نمونه‌های میانگیری شده را افزایش داد. یک پروب فعال[1] نیز می‌تواند به کاهش ظرفیت خازنی ورودی و لذا افزایش پهنای باند سیگنال موردنیاز کمک کند. همچنین گاهی از یک کابل هم‌محور خیلی کوتاه که مستقیماً به ورودی اسیلوسکوپ وصل می‌شود برای کاهش ظرفیت خازنی ورودی‌های پروب استفاده می‌شود. البته این کار می‌تواند اندازه‌گیری‌ها را دچار اشتباه کند چراکه اکثر اسیلوسکوپهای جدید از پروبهای با تضعیف‌کننده‌ی داخلی و کالیبره شده استفاده می‌کنند که تغییر در ساختار آن می‌تواند ایجاد خطا نماید.

ابتکار دیگر در این زمینه استفاده از مبدل با هسته‌ی فریت[2] به‌جای مقاومت هست. مسلماً این کار باعث تغییراتی در سیگنال‌ها می‌شود چرا که باعث می‌شود مؤلفه‌های DC را از دست بروند. البته مزایایی نیز دارد، مثلاً در اینجا محدودیتی در جریان DC وجود ندارد، در حالی که با وجود مقاومت ۱۰ اهمی در صورت عبور جریان گذرای ۱۰۰ میلی‌آمپری، ۱ولت افت ولتاژ ایجاد می‌شود که ممکن است باعث اختلال در عملکرد عادی وسیله شود. کاهش مقدار مقاومت این مشکل را حل می‌کند اما نوسانات در توان مصرفی اندازه‌گیری شده نیز کاهش می‌یابند. مزیت بعدی مبدل این است که با وجود آن دیگر نیازی به پروب‌های گران‌قیمت فعال نیست.

[1] Active Probe

[2] Ferrite

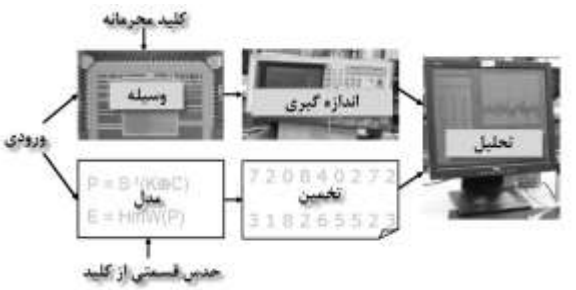
همان‌طور که گفته شد حملات تحلیل توان یک تهدید مهم برای سامانه‌های امنیتی سخت-افزاری به حساب می‌آیند. با این حال این حملات نسبت به تحلیل‌های کلاسیکی(مثل تحلیل خطی و تفاضلی) از عمومیت کمتری برخوردارند و اهدافشان محدود به یک سری مدار خاص بوده است. به همین دلیل اولین قدم در تحلیل توان مشخص کردن و شناسایی وسیله‌ی مورد حمله و نحوه‌ی پیاده-سازی الگوریتم‌های آن هست.

در حملات تحلیل توان، حمله‌گر از یک مدل فرضی برای پیش‌بینی توان مصرفی وسیله‌ی مورد حمله استفاده می‌کند. سپس این پیش‌بینی‌ها با اندازه‌گیری‌های واقعی توان مصرفی مقایسه می-شوند.کیفیت و جزئیات مدل فرض شده تأثیر مهمی در موفقیت حمله دارد. برای مثال در مدارات CMOS این منطقی است که فرض کنیم مؤلفه‌ی اصلی توان مصرفی به علت تغییر وضعیت‌های منطقی است و لذا برای یک گیت منطقی می‌توان نوشت:

$$P_D = C_L . V_{DD}^2 . P_{0\to1} . f \quad (۱-۲)$$

که در آن C_L خازن معادل هر گیت، V_{DD} ولتاژ تغذیه، $P_{0\to1}$ احتمال تغییر وضعیت از صفر به یک و f فرکانس کلاک هست. این رابطه می‌گوید که توان مصرفی یک مدار CMOS وابسته به تغییر وضعیت‌ها هست. البته مدل‌های مصرف توان دقیق‌تر و پیچیده‌تری نیز می‌توانند در نظر گرفته شوند که در اینصورت بازدهی حمله نیز افزایش می‌یابد.

در مرحله‌ی بعدی حمله‌گر به کمک مدلی که انتخاب کرده است و با پیش‌بینی تعداد تغییرات بیت‌ها در رجیسترهای پردازنده، توان مصرفی آن را تخمین می‌زند. هر چه مدل انتخابی کامل‌تر باشد و جزئیات بیشتری را پوشش دهد این تخمین صحیح‌تر خواهد بود. این تخمین توان برای تعداد N پیغام مختلف محاسبه می‌شود.



شکل ۱. رویه‌ی کلی یک حمله‌ی تحلیل توان

بعد از تخمین، حمله‌گر اجازه می دهد تا دستگاه تعداد N پیغام مشابه مرحله‌ی پیش‌بینی را با یک کلید خصوصی که حدس زده، رمز کند. و در همین حال وی توان‌های مصرفی را اندازه‌گیری و ثبت می‌نماید. در نهایت نیز حمله‌گر پیش‌بینی‌های خود را با توان‌های اندازه گرفته شده مقایسه می-کند. یک راه برای این مقایسه، محاسبه‌ی ضریب همبستگی بین بردار توان‌های مصرفی واقعی و پیش‌بینی‌شده هست. اگر حمله موفقیت آمیز باشد، یعنی کلید حدس زده درست باشد، ضریب همبستگی حداکثر خواهد شد(موسوی و همکاران، ۱۴۰۱: ۳۹).

در کاربردهای سخت افزاری مبتنی بر حفظ و انتقال ایمن اطلاعات، استفاده از سیستم‌های رمزنگاری بسیار زیاد شده است(سازدار و همکاران، ۱۳۹۲: ۲۹). نتیجه پیشرفت‌های امنیتی و نیاز مبرم به آن را می‌توان به شدت در دستگاه‌های امروزی از جمله موبایل، کارت هوشمند، رایانه‌های قابل حمل و سیستم‌های کنترل صنعتی و غیره مشاهده نمود. با توجه به نیاز بازار به سرعت بالا، امنیت قابل قبول و توان مصرفی کم، محققین روی رمزنگاری‌های سخت‌افزاری تمرکز کرده‌اند. بعد از معرفی تحلیل توان به عنوان ابزاری برای بدست آوردن کلید رمزنگاری توسط کوچر در سال ۱۹۹۹، حمله‌کنندگان به سیستم‌های رمزنگاری نیز روی حملات کانال‌های جانبی بسیار کار کرده‌اند، به طوری که در سال‌های اخیر مهم‌ترین تهدید علیه سیستم‌های رمزنگاری سخت‌افزاری، حملات مبتنی بر تحلیل توان شده است(Brier, 2004: 16). تکنیک‌های SCA، DPA، CPA و تحلیل‌های مختلف توان از دست آوردهای اصلی سال‌های اخیر است(Popp, 2007: 535). سادگی و سرعت بالای این روش‌ها علت اصلی استفاده وسیع از این تکنیک‌ها بجای تحلیل‌های ریاضیاتی و تئوری است. با پیشرفت تکنولوژی، استفاده از ادوات رمزنگاری سخت‌افزاری جدید، همراه با تنوع حملات سخت‌افزاری در حال افزایش است(cui, 2013). در تحلیل‌های حملات کانال جانبی اساس کار مبتنی بر میزان امواج الکترومغناطیسی، امواج آکوستیک، دما و حرارت و یا توان مصرفی است که از سیستم خارج می‌شود. این پارامترها به نحوی وابسته به داده‌های در حال پردازش در داخل تراشه‌ها هستند(WANG, 2013: 833).

اندازه‌گیری دقیق این خروجی‌ها، پیدا کردن کلید صحیح را ممکن می‌سازد، یکی از مفیدترین مسیرهای نفوذ، اندازه‌گیری توان مصرفی در سخت‌افزار رمزنگاری می‌باشد(Fournier, 2003). در اندازه‌گیری توان باید تمرکز روی توان مصرفی پویا باشد، زیرا توان مصرفی استاتیک اطلاعات چندانی در اختیار حمله‌کننده قرار نمی‌دهد. توان پویا وابستگی مستقیم به تغییر حالات ترانزیستورها

دارد، که این امر نقطه قوت حملات کانال جانبی است. تغییر حالات ترانزیستورها اساس عملکرد فاصله همینگ نیز می‌باشد(Lee, 2014: 49) که می‌تواند منجر به یافتن کلید یا زیر کلید صحیح شود. الگوریتم AES که پس از شکسته شدن DES ارائه شد، یکی از الگوریتم‌های بسیار پرسرعت و ایمن می‌باشد که هم‌اکنون نیز بسیار مورد استفاده قرار می‌گیرد. در این الگوریتم برای امنیت بیشتر، طول کلیدها حتی به ۲۵٦ بیت نیز می‌رسد که در این صورت تعداد حالات ممکن برای کلید برابر با عدد ۲۲۵٦ می‌باشد که این تعداد حالات امکان پیدا کردن کلید با سعی و خطا در زمان قابل‌قبول را منتفی می‌کند. با این وجود الگوریتم AES هنوز هم در مقابل حملات توان آسیب‌پذیر است (WANG, 2013: 833) همه روش‌های موجود به نحوی به دنبال به هم زدن رابطه میان داده‌های در حال پردازش در داخل سخت‌افزار با توان مصرفی قابل‌مشاهده و اندازه‌گیری می‌باشند. هرکدام از این روش‌ها به نوعی هزینه سرباری شامل هزینه ساخت، فضا یا توان مصرفی و کاهش فرکانس کاری سیستم را به دنبال دارند.

حملاتی همچون SCA، DPA و CPA برای شکست الگوریتم AES در مقالات مختلف بررسی شده است، که از میان آن‌ها روش DPA و CPA بیشتر از بقیه روش‌ها مورد استفاده قرار گرفته و بررسی شده‌اند که دلیل آن، قدرت بالای این دو روش در شکست الگوریتم‌ها می‌باشد، تاکنون روش‌های بسیار زیادی برای مقابله با این حمله گرها توسط متخصصین ارائه شده است، که اکثراً از مقام سازی‌هایی مبتنی بر سخت‌افزار هستند. از جمله روش‌های ارائه شده تاکنون SABL، WDDL، Dual-Rail Logic می‌باشد که نیاز به سلول کتابخانه جدید دارد، روش‌های مبتنی بر ولتاژ و فرکانس پویا با استفاده از مدارات جانبی امکان‌پذیر است، روش RSL مبتنی بر استفاده از گیت‌های تصادفی بوده ، روش موازی کردن حافظه و به اشتراک گذاشتن آن به‌صورت نرم‌افزاری ، رمز کردن و موازی نمودن حافظه، تصادفی کردن توان مصرفی با اضافه کردن مصرف‌کننده‌های مختلف، منطق مکمل و منطق غیر هم‌زمان و روش های glitch، hazard، Ring Oscillators، روش‌های مبتنی بر تأخیرهای تصادفی در زمان‌های اجرا، روش ۱-of-n مبتنی بر کد کردن داده و روش‌های بسیار دیگر می‌باشد. متأسفانه اکثر این تکنیک‌ها برای محافظت FPGA ها در عمل ناکارآمد هستند. برای مثال طرح SABL یا Ring Oscillators در FPGA غیر قابل پیاده سازی است، یا طرح Dual-Rail Logic در صورت ساخته شدن، دو برابر حجم خود الگوریتم اصلی فضا اشغال کرده و توان مصرف می‌کند.

اکثر روش‌های فوق بجز طرحهای مبتنی بر مقاوم سازی نرم افزاری و ایجاد تاخیر، به نحوی نیاز به تغییر در ساختار سخت افزاری در لایه CMOS دارند. این کار علاوه بر هزینه بالا گاهی اوقات امکان پذیر نمی‌باشد، زیرا ایجاد تغییر در سطح CMOS صرفا در اختیار شرکت تولید کننده می باشد. همان طور که قبلا نیز گفته شد، امکان پیاده سازی اکثر این روش ها در FPGA وجود ندارد. برای مثال در FPGA توانایی استفاده از مدارات ترکیبی فیدبک دار وجود ندارد تا پیاده سازی رینگ اسیلاتور مبتنی بر گیت NOT با فیدبک مقدور گردد. برای پیاده سازی روش RSL حتما نیاز به تحریک ترانزیستورها می‌باشد که این عمل در تعارض مستقیم با خواص ذاتی FPGA مبنی بر دیجیتال بودن آن است.

اگرچه بر هم ریختن رابطه میان توان مصرفی و داده ها با استفاده از تزریق نویز در مقالات متعددی مورد بررسی قرار گرفته است. ولی استفاده از تغییرات توان مصرفی PLL در ناحیه گذرا به عنوان نویز توان توام با اعمال تاخیرهای تصادفی با استفاده از خروجی PLL در ناحیه گذرا کمتر بررسی شده است.

همانطور که گفته شد، اساس کلی حملات توان اندازه گیری توان مصرفی و پردازش آن برای کشف ارتباط این توان با مقادیر داخل تراشه در حال پردازش می باشد. اصولا برای اندازه گیری توان در حملات توان روشهای مختلفی بکار می رود. که از بین روشهای موجود دو روش CAD و FPGA Board انتخاب شده است.

پژوهش‌های انجام شده در ارتباط با موضوع رمز نگاری سخت افزاری و مقاومت آن در داخل FPGA و تحلیل توان در سیستم های رمز نگاری را می‌توان در سه بخش مورد بررسی دانشمندان قرار دارد:

۱- طرح هایی که فقط به دنبال پیاده سازی الگوریتم و افزایش کارایی آن بوده اند. این دسته از مطالعات نسبت به ضعف های سیستم از لحاظ حمله کمتر توجه کرده اند.

۲- طرحهایی که به دنبال کار آقای پال کاچر بوده و فقط در پی تحلیل توان در بلوک های رمز نگاری بوده اند و در این دست کارها، نوآوری چندانی نبوده و هدف فقط پیاده سازی عملی تحلیل است.

۳- طرح هایی که به دنبال مقاوم سازی سیستم در برابر حملات کانال جانبی بوده اند. طبیعتاً با توجه به عنوان پایان نامه، گروه سوم در سطح وسیعتری قرار داشته و عمیق تر به آن پرداخته خواهد

شد.

محققین در دو دهه گذشته با بررسی توان مصـرفی تراشـه هـای در حـال رمزنگـاری توانسـتند کلیدهای خصوصی قرارگرفته در تراشه‌های رمز نگاری را خیلی سریعتر از روشـهای تئـوری بدسـت بیاورند. در روش تحلیل توان میزان توان مصـرفی در زمـان پـردازش رمزنگـاری بـه دفعـات متعـدد ذخیره شده و از این اصل که در مدارات CMOSوابستگی میزان تـوان مصـرفی را مـی تـوان طبـق رابطه (۱) به داده‌های میانی در حال پردازش مدل کرد، استفاده می شود.

$$P\_D=C\_L\ (V\_PP\ )\hat{}2\ P\_(0\rightarrow1)\ f \qquad (۱)$$

اگر در رابطه فوق PD توان مصرفی پویا گرفته شده باشد و CL ظرفیت خـازنی گیـت هـا یـا ترانزیستورها و f فرکانس کاری تراشه و VPP ولتاژ تغذیـه باشـد، مـی تـوان P(۰→۱) را احتمـال تغییرات خروجی گیت از ۰ به ۱ در نظر گرفت. یکی از ملزومات اصلی حملاتDPA اندازه گیـری دقیق توان پویا در تراشه‌ها، هنگام پردازش داده‌ها می باشد. در روش DPA برخلاف سـایر روش هـا نیاز چندانی به دانستن جزییات زیاد از نحوه پیاده سازی الگوریتم در تراشه نیست، که این امـر از نقـاط قوت این روش نسبت به سایر روشهای تئوری است.

در سال ۲۰۰٤ اولین حمله کاملا موفق بر اساس پردازش تشعشعات الکترومغناطیسـی توسـط ارس ارائه شد. با گذشت بیش از یک دهه از آن تاریخ و پیشرفتهای بسیار زیاد در ساخت و استفاده از FPGA ها، استفاده از این قطعه قابل برنامه ریزی بسیار زیاد شده است. مهمترین دلیل استفاده از FPGA ها ارزان بودن قیمت، قابلیت انعطاف و تغییرپذیری آن در سطح سخت افزار می باشد، همچنـین نحـوه اسـتفاده از FPGA نیز به خاطر پیشرفت زبانهای توصیف سخت افزار HDL بسیار آسان تر شده است، به مـوارد فوق اگر سادگی شبیه سازی و سنتز در FPGA اضافه گردد، مشاهده خواهد شـد کـه یکـی از بهتـرین انتخاب‌ها برای ساخت تجهیزات جدید، FPGA ها هستند. امروزه FPGA به عنوان یکـی از بهتـرین انتخاب‌ها برای پیاده سازی الگوریتم رمزنگاری با سرعت بالا می‌باشد. علـی الخصـوص قبـل از سـاخت تراشه ASIC ، استفاده از FPGA یک کار کاملا بهینه می‌باشد.

مقاوم سازی‌های معمول که روی FPGA انجام شده است اصولا مبتنی بر اضـافه کـردن نـویز، تصادفی کردن داده ها، masking، hiding، ایجاد تاخیر زمانی، تصادفی کـردن کلـاک، پیـاده سـازی پویا و تفاضلی و HDRL، قـرار دادن Ring Oscillator ترتیبـی در تراشـه و ... مـی‌باشـد. هـدف اکثر این روش‌ها پیچیده کردن توان مصرفی می‌باشد، که این پیچیدگی عامل مقاومت می‌باشد.

٤-زیر ساخت های اساسی کشور

حفاظت از زیرساخت‌های حیاتی (CIP) به مجموعه فعالیت‌هایی گفته می‌شود که برای حفاظت زیرساخت‌ها (Infrastructure) که در هر کشوری بنیان اساسی جامعه آن کشور محسوب می‌شوند و آسیب به آن‌ها می‌تواند پیامدهای جبران‌ناپذیری را در کشورها ایجاد نماید و آسیب در یک بخش می‌تواند بخش‌های دیگر را نیز تحت تأثیر جدی قرار دهد. برای مثال یک ویروس رایانه‌ای توزیع گاز طبیعی در یک منطقه ر ا مختل کند. این موضوع می‌تواند پیامدهایی را در تولید برق داشته باشد که به نوبه خود می‌تواند منجر به قطع خطوط شبکه‌ای و ارتباطات رایانه‌ای دیگر شود. این امر می‌تواند به ترافیک در راه‌ها، ترافیک هوایی یا حتی ترافیک قطارها منجر شود و حتی ممکن است خدمات اورژانسی را نیز تحت تأثیر قرار دهد. همین موضوع می‌تواند در اثر یک اتفاق طبیعی نیز به وجود آید و منجر به فلج شدن یک منطقه و حتی یک کشور شود.

زیرساخت به ساختار اولیه فیزیکی و سازمان یافته‌ای گفته می‌شود که برای اجرای مأموریت و اهداف یک سازمان یا یک جامعه مورد نیاز است و در حالت کلی به عناصر ساختاری مرتبط و بهم پیوسته‌ای گفته می‌شود که چهارچوبی را برای توسعه کل ساختارهای دیگر فراهم می‌کند و می‌تواند به عنوان یکی از عناصر توسعه یافتگی یک کشور مطرح گردد. زیرساخت به تسهیل تولید کالاها و خدمات (شامل خدمات اجتماعی) و توزیع آن‌ها کمک می‌کند. به‌طور مثال جاده‌ها به حمل و نقل کالاها و مواد اولیه به کارخانه‌ها کمک می‌کنند.

زیرساخت‌ها می‌تواند به دو صورت کلی باشند؛ زیرساخت‌های نرم و زیرساخت‌های سخت. زیرساخت‌های سخت می‌تواند شامل زیرساخت‌های حمل و نقل، زیرساخت‌های مدیریت آب، زیرساخت‌های ارتباطی، زیرساخت مدیریت زباله‌های جامد، زیرساخت شبکه مانیتورینگ و اندازه‌گیری زمین است. زیرساخت‌های نرم می‌تواند شامل زیرساخت‌های حکمرانی، زیرساخت اقتصادی، زیرساخت اجتماعی زیرساخت فرهنگی و زیرساخت‌های ورزشی و تفریحی باشد. واژه زیرساخت معمولاً از سوی دولت‌ها برای توصیف دارایی‌هایی استفاده می‌شود که مدیریت و عملیات ساختارهای اساسی جامعه مثل اقتصاد را ممکن می‌سازد و برای اجرای آن ضروری می‌باشند. در یک تقسیم‌بندی کلی این واژه با موارد زیر در ارتباط است:

- تولید، حمل و نقل و توزیع برق
- تولید، حمل و نقل و توزیع گاز

- نفت و تولید و توزیع محصولات نفتی
- ارتباطات و خطوط ارتباطی
- منابع تأمین آب شامل آب آشامیدنی و نیز فاضلاب و آب‌های سطحی
- کشاورزی و ساختارهای کشاورزی و نیز محصولات کشاورزی و خطوط توزیع آن
- ابزارها، وسایل و اسباب گرمایشی شامل سوخت نفت و گاز طبیعی و...
- بهداشت و سلامت عمومی شامل بیمارستان‌ها و وسائط حمل و نقل مربوط مثل آمبولانس‌ها
- سیستم‌های حمل و نقل شامل شبکه‌های ریلی، هواپیمایی، بنادر و حمل و نقل داخلی
- سیستم‌های خدمات مالی مثل بانک‌ها
- سیستم‌های امنیتی شامل نیروهای پلیس و ساختارهای نظامی

هدف از برنامه‌ریزی در این حوزه توسعه یک برنامه برای حفاظت زیرساخت‌های حیاتی و جلوگیری از انجام حملات و ممانعت از ارائه خدمات این بخش هاست. این امر با ایجاد و تقویت هماهنگی و همکاری بین بخش‌های خصوصی و دولتیدر و نیز با ارائه دهندگان خدمات در این حوزه‌ها و ارتباط اطلاعاتی این بخش‌ها و نیز صاحبان زیرساخت‌های حیاتی امکان‌پذیر خواهد بود. این برنامه‌ریزی باید شامل بخش‌های زیر باشد:

الف. شناسایی زیرساخت‌های حیاتی در کشور

ب. شناسایی صاحبان و مالکان اصلی و فرعی زیرساخت‌های حیاتی

ج. طراحی و ایجاد راهبردهای دفاع از زیرساخت‌های حیاتی

د. شناسایی اجزای مختلف و نقش آن‌ها در زیرساخت‌های حیاتی

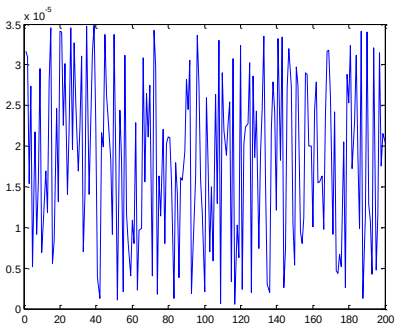
هـ. توسعه سیاست‌های حفاظت و رویه‌های حفاظتی و افزایش تدریجی حفاظت از زیرساخت‌ها

و. مانورهای دوره‌ای برای بررسی اثربخشی و کارایی روش‌های حفاظت

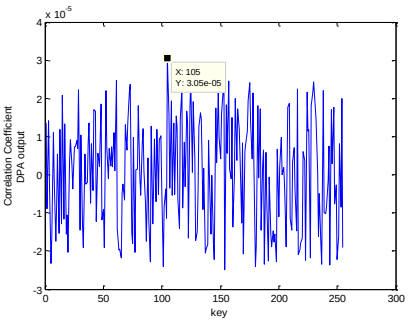
به‌طور مثال در حوزه زیرساخت‌های اطلاعاتی و ارتباطی یکی از آسیب‌های جدی حملات توزیع شده ممانعت از ارائه خدمات (DDoS) می‌باشد که رشد بسیاری در سال‌های اخیر داشته‌است و زیان‌های مالی زیادی را به دولت‌ها تحمیل کرده‌است. همچنین این گونه حملات به شدت نارضایتی مردم را نیز بالا برده است. یکی از بهترین کارهایی که برای جلوگیری از این حملات می توان انجام داد بالا بردن سیستمهای امنیتی در دنیای الکترونیک است. و این امر با بهبود سامانه های رمز نگاری میسر می شود.

۵- نتایج شبیه سازی

برای شبیه سازی توان مصرفی دینامیکی و حملات DPA از ابزار cadence در تکنولوژی 65nm استفاده شده است. ابتدا طرح بدون مقاوم سازی مورد آنالیز قرار گرفت. شکل 2a میزان توان مصرفی یک سامانه غیر ایمن را نشان می دهد تعداد نمونه‌ها ۲۰۰ عدد برا هر نمودار توان است. با اجرای چندین باره الگوریتم به تعداد ۲۰۰۰۰ عدد نمونه توان ذخیره می کنیم با اجرای حمله DPA بر روی این ۲۰۰۰۰ نمونه آسیب پذیری سیستم طبق شکل 2b مشخص می شود. زیر کلید رمزنگاری در این آزمایش عدد ۱۰۵ است.



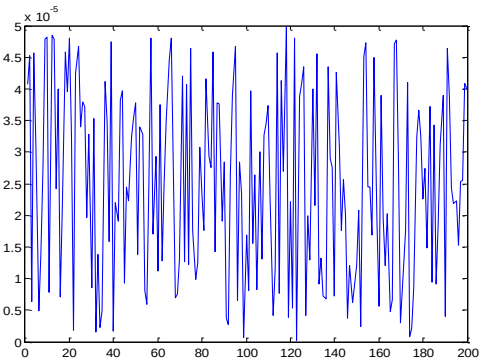
(a):نمودار توان مصرفی در یک دوره رمزنگاری



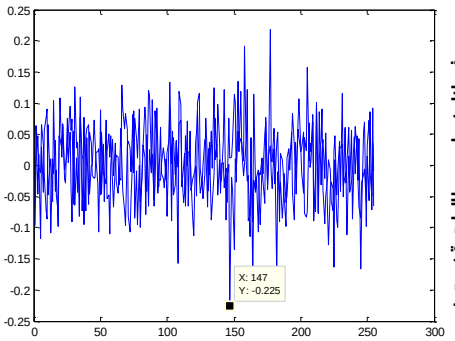
(b) :نمودار خروجی DPA برای ۸ بیت اول کلید با ۲۰۰۰۰ نمونه

شکل ۲. توان مصرفی و خروجی DPA برای سیستم بدون مقاوم سازی

حال سامانه را توسط دو عامل PLL و گیت ارتقاء یافته به صورت توام مقاوم می کنیم. شکل شماره 3a میزان توان مصرفی در این حالت و شکل شماره 3b نمودار خروجی حمله DPA را نشان می دهد. همان طور که در این شکل دیده می شود سامانه در مقابل حمله توان با تعداد 60000 عدد نمودار هنوز مقاوم است.

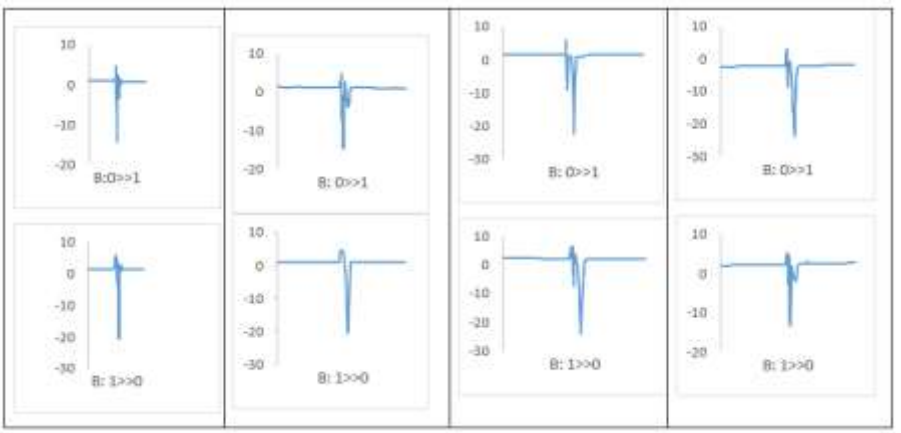


(b):نمودار خروجی DPA برای ۸ بیت اول کلید با ۶۰۰۰۰ نمونه



(a):نمودار توان مصرفی در یک دوروه رمزنگاری

شکل ۳. توان مصرفی و خروجی DPA برای سیستم با مقاوم سازی



۵-۱- مقایسه با کارهای قبلی

یکی از معیارهایی که برای بررسی توانمندی روشهای مقاوم‌سازی وجود دارد میزان سربار سخت‌افزاری و تحمیل توان اضافی در روش مقاوم‌سازی پیشنهادی می‌باشد. برای بررسی این موضوع سربار سخت‌افزاری و توان مصرفی روش پیاده‌سازی شده در جدول (۱) ارائه گردیده است.

جدول ۱. مقایسه و هزینه سربار شده به سیستم با روش‌های قبلی

Technology	method	design	Area/ Overhead	Power sample need	Power / Overhead
۹۰nm	PSPLL+RPFL	protected	۰٫۳۱ mm² / ۳۲٪	۶۰۰۰۰ / ۹۵٪	۲۰ mW / ۲۰٪
		Un protected	۰٫۲۴ mm²	۳۲۰۰۰	۱۷ mW
۹۰nm	RPFL	protected	۰٫۲۵ mm² / ۱٪	۴۰۰۰۰ / ۲۵٪	۱۸ mW / ۱٪
		Un protected	۰٫۲۴ mm²	۳۲۰۰۰	۱۷ mW
۹۰nm	Pulse Steal PLL	protected	۰٫۲۹ mm² / ۲۵٪	۳۵۰۰۰ / ۱۰٪	۱۹٫۷ mW / ۱۵٪
		Un protected	۰٫۲۴ mm²	۳۲۰۰۰	۱۷ mW
۹۰nm	CP-PLL	protected	۰٫۲۴ mm² / ۳٫۵٪	-	۱۵٫۰ mW / ۳٫۵٪
		Un protected	۰٫۲۴ mm²	-	۱۴٫۵ mW
۱۸۰nm	WDDL	protected	۰٫۲٫۴ mm² / ۲۱۰٪	-	۲۰۰ mW / ۲۷۰٪
		Un protected	۰٫۷۹ mm²	-	۵۴ mW
۹۰nm	Digital Ring Oscillator	protected	۰٫۱۰ mm² / ۶٪	-	۷٫۱۰ mW / ۱۸٫۵٪
		Un protected	۰٫۰۹ mm²	-	۵٫۹۹ mW
۱۳۰nm	Switched Capacitor	protected	۰٫۴۴ mm² / ۲۷٪	-	۴۴٫۳ mW / ۳۳٪
		Un protected	۰٫۳۵ mm²	-	۳۳٫۳ mW

نتیجه گیری

در این مقاله در جنگ‌های مدرن مبتنی بر جنگ الکترونیک، روش جدیدی مبتنی بر پنهان نگاری و ماسک گذاری برای مقابله با حملات DPA در الگوریتم AES ارائه شد. اساس این روش تزریق نویز توان به سیستم با استفاده گیت ارتقاء یافته است، مقایسه نتایج در حالت شبیه‌سازی نشان داد که سیستم در مقابل حملات DPA با تعداد معقولی از نمودار توان، مقاومت خوبی دارد به طوری که نسبت به طرحهای قبلی تعداد نمودارهای توان تقریبا دو برابر شده و تنها هزینه سربار سیستم به اندازه افزایش حجم فضای اشغالی به اندازه ۳۳ درصد و توان مصرفی ۲۰ درصد است.

منابع

اصغرزاده، افسانه و میرزائی، محمد(۱۳۹۹). تحلیل و شبیه سازی گیرنده DIFM و روش اندازه‌گیری لحظه‌ای فرکانس در سیستم‌های پشتیبان جنگ الکترونیک. روش‌های هوشمند در صنعت برق، ۱۱(٤۱)، ۸٤-۷۳.

زبردست، شراره(۱٤۰۱). بررسی نقص حقوق جنگ در مخاصمات مسلحانه بشر دوستانه بین اکراین و روسیه، قانون یار، ٦(۲۳)، ۱۱۳-۱۰۱.

سازدار، امیرمهدی؛ نجاتی‌جهرمی، منصور؛ راعی، جلال و احمدلو، افشین(۱۳۹۲). ارائه الگوی الگوریتم رمزنگاری و احراز اصالت در سامانه‌های دورسنجی نظامی، علوم و فنون نظامی، ۹(۲٤)، ٤٤-۲۹.

سلامی، یاشار؛ خواجه وند، وحید و زینالی، اسماعیل(۱٤۰۲). بهره وری تبادل کلید همزمان- استخراج رمزنگاری از کلید عمومی در تخلیه ایمن مبتنی بر فدراسیون مه-ابر برای سیستم های رصد ایستگاه های هواشناسی خودکار. نیوار، ٤۷(۱۲۰)، ۱٦٤-۱۵۱.

فرحبخت، احمدرضا و دهقانی، مهدی(۱۳۹۸). همگرایی جنگ الکترونیک و جنگ سایبری و الزامات اجرای آن در سازمان‌های نظامی، امنیت ملی، ۹(۳۱)، ۲۱۸-۱۹۹.

موسوی، سید حمیدرضا؛ صفائیان، مهدی و احمدی قلعه، امیرحسن(۱٤۰۱). روش جدید در امنیت سیستم‌های رمزنگاری توسط گیت‌های نامتوازن، سیستم‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند، ۳(۸)، ۵۰-۳۹.

وفایی‌جهان، مجید؛ ستایشی، سعید و اکبرزاده توتونچی، محمدرضا(۱۳۸٦). رمزنگاری اطلاعات بر اساس عوامل محیطی با استفاده از اتوماتای سلولی، چهارمین کنفرانس انجمن رمز ایران.

D. Suzuki, M. Saeki, and T. Ichikawa(2004), "Random switching logic: a countermeasure against DPA based on transition probability," IACR ePrint, rep, vol. 346.

E. Brier, C. Clavier, and F. Olivier(2004), "Correlation Power Analysis with a Leakage Model," pp. 16–29.

I. Hammad, K. El-Sankary, and E. El-Masry(2010), "High-speed AES encryptor with efficient merging techniques," IEEE Embed. Syst. Lett., vol. 2, no. 3, pp. 67–71.

I. Verbauwhede and K. Tiri(2008), "A Dynamic and Differential CMOS Logic with Signal-Independent Power Consumption to Withstand Differential Power Analysis.

J. J. A. Fournier, S. Moore, H. Li, R. Mullins, and G. Taylor(2003), "Security Evaluation of Asynchronous Circuits," Cryptogr. Hardw. Embed. Syst. - CHES.

J. W. Lee, S. C. Chung, H. C. Chang, and C. Y. Lee(2014), "Efficient power-analysis-resistant dual-field elliptic curve cryptographic processor using heterogeneous dual-processing-element architecture," IEEE Trans. Very Large Scale Integr. Syst., vol. 22, no. 1, pp. 49–61.

K. Tiri and I. Verbauwhede(2004), "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," Proc. - Des. Autom. Test Eur. Conf. Exhib., vol. 1, pp. 246–251.

K. Tiri, D. Hwang, A. Hodjat, and B.-C. Lai(2005), "Prototype IC with WDDL and differential routing–DPA resistance assessment," Cryptogr. Hardw. Embed. Syst. – CHES 2005, vol. 3659/2005, pp. 354–365.

M. Masoumi, P. Habibi, A. Dehghan, M. Jadidi, and L. Yousefi(2016), "Efficient implementation of power analysis attack resistant advanced encryption standard algorithm on side-channel attack standard evaluation board," Int. J. Internet Technol. Secur. Trans., vol. 6, no. 3, p. 203.

P. Bilski and W. Winiecki(2010), "Multi-core implementation of the symmetric cryptography algorithms in the measurement system," Meas. J. Int. Meas. Confed., vol. 43, no. 8, pp. 1049–1060.

P. C. Kocher et al.(1999), "Differential Power Analysis," Journal of Cryptographic Engineering. pp. 1–10.

R. Bevan, E. Knudsen, and B. Bp(2002), "Ways to Enhance Differential Power Analysis," Icisc 2002, vol. 1, pp. 327–342.

S. Mangard(2002), "A Simple Power-Analysis (SPA) Attack on Implementations of the AES Key Expansion," Society, vol. 2587, pp. 343–358.

T. Popp and S. Mangard(2005), "Masked Dual-Rail Pre-charge Logic: DPA-Resistance Without Routing Constraints," pp. 172–186.

T. Popp, E. Oswald, and S. Mangard(2007), "Power Analysis Attacks and Countermeasures," Des. Test Comput. IEEE, vol. 24, no. 6, pp. 535–543.

U. Rührmair et al.(2014), “Efficient Power and Timing Side Channels for Physical Unclonable Functions.” pp. 476–492.

X. Cui, R. Li, W. Wei, J. Gu, and X. Cui(2013), “AHardware implementation of des with combined countermeasure against DPA,” in Proceedings of International Conference on ASIC.

Z. Y. and Z. X. WANG Pengjun(2013), “Design of Two-phase SABL Flip-flop for Resistant DPA Attacks,” Chinese J. Electron., vol. 22, no. 4, pp. 833–837.