دبیرخانه دائمی کنفرانس ملی
پدافند غیرعامل و توسعه پایدار

حملات جانبی بر روی کارت‌های هوشمند و بررسی راهکاری ارائه‌شده برای جلوگیری از نشت اطلاعات محرمانه کارت

هادی اسکندری سبزی[1]، مهری یحیایی[2]

1- کارشناس ارشد مخابرات، مرکز تحقیقات صنایع انفورماتیک

2 - کارشناس ارشد فناوری اطلاعات، مرکز تحقیقات صنایع انفورماتیک

Eskandari@rcii.ir

اغلب طراحان سامانه‌های رمزنگاری بر این باورند که مطالب رمز شده خود را در یک محیط بسته و امن ذخیره‌سازی و اداره کرده‌اند که قابل‌تحلیل و حمله نیست. یکی از این سامانه‌های رمزنگاری بر روی کارت‌های هوشمند پیاده‌سازی شده، که یکی از مهم‌ترین ابزارهای تصدیق کاربر و ذخیره اطلاعات محرمانه است که امروزه کاربرد وسیعی پیداکرده است. کارت‌های هوشمند دارای تراشه الکترونیکی و مغناطیسی می‌باشند که محیط مناسبی برای پیاده‌سازی الگوریتم‌های رمزنگاری و ذخیره‌سازی اطلاعات هستند. این تراشه‌های الکترونیکی در حین انجام عملیات رمزنگاری و رمزگشایی جریان الکتریکی لازم را از منبع دریافت می‌کنند که این کار باعث به وجود آمدن فرآیندهای متفاوتی در تراشه می‌گردد. این فرآیندها می‌تواند از چندین نظر موردبررسی و تجزیه‌وتحلیل اطلاعات قرار گیرد، که استفاده کردن از این اطلاعات برای رسیدن به کلید رمزنگاری را به‌اصطلاح حملات جانبی کانال گویند. یکی از قدرتمندترین و معمول‌ترین نوع حملات جانبی کانال استفاده از تجزیه‌وتحلیل توان مصرفی برای حمله است. در این نوع از حملات سعی بر پیدا کردن یک راه‌حل و رابطه مناسب بین مصرف لحظه‌ای توان و وضعیت داخلی آن در زمان اجرای الگوریتم رمزنگاری است. ازآنجایی‌که پیاده‌سازی الگوریتم‌های رمزنگاری در سامانه‌هایی مانند کارت هوشمند، منجر به نشت اطلاعات حساسی از طریق مقادیر میانی الگوریتم می‌گردد، پس اطلاعات حساس از طریق کمیت-های فیزیکی موسوم به کانال جانبی نشت می‌کند، به همراه اطلاعات در دسترس از ساختار ریاضی الگوریتم رمز پیاده‌سازی شده در سیستم، به‌منظور استخراج کلید محرمانه به‌کاررفته، استفاده می‌شود و می‌توانند اطلاعات مخفی سامانه را آشکار سازند. ما در این مقاله به بررسی حمله‌های موفقی که با استفاده از نشت اطلاعات جانبی بر روی کارت هوشمند اعمال‌شده‌اند پرداخته و درنهایت با ارائه راه‌کارهایی که می‌تواند برای جلوگیری از حملات احتمالی بر روی کارت‌های هوشمند اعمال گردد می‌پردازیم.

کلمات کلیدی: حملات جانبی کانال، کارت هوشمند، رمزنگاری، تجزیه تحلیل توان، نشت اطلاعات.

1. مقدمه

رمزنگاری از دیرباز به‌عنوان یک ضرورت برای حفاظت از اطلاعات خصوصی در مقابل دسترسی‌های غیرمجاز در تجارت، سیاست و مسائل نظامی وجود داشته است. به‌طور مثال تلاش برای ارسال یک پیام سری بین دو هم‌پیمان به‌گونه‌ای که

[1] کارشناس ارشد آزمایشگاه امنیت مرکز تحقیقات صنایع انفورماتیک

[2] مدیر آزمایشگاه امنیت مرکز تحقیقات صنایع انفورماتیک

حتی اگر توسط دشمن دریافت شود نیز قابل‌درک نباشد، در تاریخ رم قدیم نیز دیده شده، و یک تاریخچه و قدمت طولانی دارد. در سالیان اخیر رمزنگاری و تحلیل رمز از یک هنر پا را فراتر گذاشته و یک علم مستقل شده است و درواقع به‌عنوان یک وسیله عملی برای ارسال اطلاعات محرمانه روی کانال‌های غیر امن همانند اینترنت، تلفن، ماکرویو و ماهواره‌ها شناخته می‌شود. با توجه به گستردگی ارتباطات کامپیوتری و پیشرفت تکنولوژی و آسان شدن روش‌های نقل‌وانتقال اطلاعات دیجیتال و توسعه فن‌آوری‌های اطلاعات و به وجود آمدن مخابرات امن و شبکه‌های دیجیتالی مانند شبکه‌های اینترنت هرروزه بر تعداد استفاده‌کنندگان از محصولات دیجیتالی افزوده می‌شود. از طرف دیگر قابلیت کپی‌برداری راحت‌تر و بدون افت کیفیت از این محصولات باعث شده است تا همواره طراحی سامانه‌هایی که بتواند از این محصولات و حقوق صاحبان آن‌ها محافظت کند یکی از نیازهای جدی این عرضه است.

از یک دیدگاه کلی امنیت اطلاعات دارای سه هدف اصلی است که این سه هدف را می‌توان به‌صورت زیر بیان نمود:

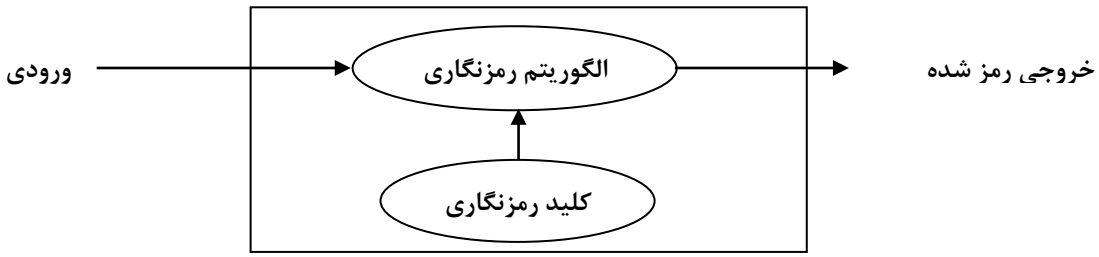
- محرمانگی: اطلاعات تنها توسط افراد مجاز قابل‌خواندن باشد.
- جامعیت: اگر اطلاعات در حین ارسال و یا پردازش دست‌کاری گردد، قابل‌تشخیص نباشد.
- در دسترس بودن: اطلاعات و منابع سیستم در دسترس افراد مجاز باشد و افراد غیرمجاز نتوانند خللی در امکان استفاده از منابع ایجاد کنند.

برای رسیدن به دو هدف اولی، اصلی‌ترین مکانیزم استفاده از روش‌های رمزنگاری است. درجه تضمین هریک از اهداف، وابستگی مستقیماً به الگوریتم استفاده‌شده برای رسیدن به آن هدف را دارد. هرچه قدر از الگوریتم‌های پیچیده و قدرتمندتری استفاده شود تضمین بیشتری برای رسیدن به اهداف وجود خواهد داشت. در سالیان دور مکانیزم‌های امنیتی و کاربردهای آن معمولاً محدود به حوزه‌های نظامی و مراکز امنیتی بوده است، اما در دهه‌های اخیر با گسترش شبکه‌های کامپیوتری و به وجود آمدن کاربردهای گوناگون الکترونیکی مانند تجارت الکترونیک، امنیت اطلاعات در سایر حوزه‌ها هم موردتوجه قرارگرفته است و به یک مسئله روزمره تبدیل شده است که ما همواره در کاربردهای روزانه با آن سروکار داریم. یکی از این کاربردهای مهم روزانه ما استفاده از کارت‌های هوشمند است[1,2,6].

2. برنامه‌ریزی کارت هوشمند

گسترش کارت‌های پلاستیکی در اوایل دهه ۵۰ میلادی آغاز شد. هزینه پایین این کارت‌ها که از جنس پلی‌وینیل کلراید بودند، باعث شد تا به‌سرعت جای کارت‌های کاغذی که تحمل تنش‌های فیزیکی و تغییرات آب‌وهوا را ندارند را بگیرند. اولین ارتقاء در این کارت‌ها با اضافه نمودن نوار مغناطیسی ذخیره داده به آن‌ها که امکان ذخیره‌سازی اطلاعات را می‌داد پدید آمد. در سال ۱۹۷۰ و با پیشرفت چشمگیر در ریزپردازنده‌ها و ترکیب آن‌ها با حافظه‌های غیرفعال این امکان به وجود آمد تا از آن‌ها در کارت‌های هوشمند استفاده گردد. کارت‌های هوشمند، امروزه در بسیاری از کاربردهایی که نیاز به نگهداری و انتقال امن اطلاعات داده‌ها، کنترل دسترسی به سیستم‌های رایانه‌ای و نیز کنترل دسترسی فیزیکی به محیط‌های خاص به‌عنوان کلید الکترونیکی وجود دارند، بکار می‌روند. کارت هوشمند که با نام‌های کارت چیپ‌دار یا کارت‌های با مدار مجتمع هم شناخته می‌شود که کارتی است که بر روی آن مدار مجتمع نصب شده است. همچنین از این نوع کارت می‌توان به‌جای کارت اعتباری و کارت پول یا در سیستم‌های امنیتی کامپیوتری، سیستم‌های تشخیص هویت و بسیاری موارد دیگر استفاده کرد. امروزه کاربردهای این تکنولوژی در سطح دنیا در اکثر زمینه‌ها قابل‌مشاهده بوده و حتی این روند، رو به رشد است. بانک‌ها، مراکز مخابراتی، سازمان‌های دولتی، مراکز بهداشتی، مراکز ارائه خدمات، مراکز آموزشی، مراکز تفریحی و غیره از این دستاوردهای کاربردی این تکنولوژی بهره می‌گیرند[3].

با توجه به کاربردهایی که اشاره‌شده پس ازاین‌رو امنیت در کارت‌های هوشمند اهمیت ویژه‌ای را ملزوم می‌کند. رمزنگاری در کارت‌های هوشمند نیازی است که به‌هیچ‌وجه قابل انکار نیست. کارت‌های هوشمند شرایطی را برای دسترسی به اطلاعات خود اعمال می‌کنند تا از محتویات داده‌های موجود در فایل‌ها محافظت بکنند. کاربران فقط در شرایطی می‌توانند به نوشتن یا خواندن اطلاعات کارت اقدام کنند که شرایط دسترسی و مجوزهای لازم را داشته باشند. کارت توسط سیستم عامل کنترل می‌شود درنتیجه سیستم عامل مسئول امنیت اطلاعات کارت است. با افزوده شدن رمزنگاری به کارت‌های هوشمند می‌بایست محاسبات پیچیده ریاضی در کارت‌ها انجام می‌شد. اما از بین روش‌های مختلفی که در رمزنگاری وجود دارد، روش AES و DES بیشترین کاربرد را نسبت به الگوریتم‌های دیگر دارا هستند. این دو روش در استاندارد رمزنگاری پیشرفته توسط دولت ایالات‌متحده پذیرفته شده و اکنون در سراسر جهان استفاده می‌گردد. الگوریتم رمزنگاری AES در سال 1999 به‌جای استاندارد رمزنگاری داده‌ها DES که در سال ۱۹۷۷ منتشر شده بود، جایگزین گردیده است این الگوریتم یک الگوریتم متقارن است، بدین معنی که از یک کلید یکسان برای رمزنگاری و رمزگشایی استفاده می‌شود[4]. ولی این الگوریتم نیز از طریق حملات جانبی کانال در برخی از موارد نیز دارای محدودیتی است. در یک سیستم رمزنگاری معمولی با استفاده از رمز کننده‌های بلوکی، رمزگشایی معمولاً با توجه و زوم کردن بر ورودی اولیه و خروجی نهایی و پنهانی به‌عنوان یک منبع اطلاعات برای حمله، آغاز می‌شود. این موارد شامل متن ورودی، کلیدهای مخفی و خروجی متن رمز شده نهایی است که در شکل (1) نشان داده شده است[7]:



شکل(1): پیاده‌سازی بلوک رمزنگاری برای ورودی و خروجی ایده‌آل[7]

برخی از فرضیاتی که در این رابطه اظهار می‌شود عبارتند از اینکه هیچ اطلاعاتی از کلید محرمانه برای مهاجم در دسترس نمی‌باشد و تابع رمزنگاری به‌عنوان یک جعبه سیاه عمل می‌کند. ازآنجایی‌که این تابع در تمامی دستگاه‌های دنیا اجرا می‌شود، پس ازاین‌رو این فرضیات ممکن است کاملاً صحیح باشد می‌توان به نحوی به این کلید دستیابی کرد. پس برای این‌که بتوان به کلید دست‌یافت باید به الگوریتم حملاتی را ارائه نمود، بر اساس اینکه حمله کننده چه کنترلی را بر عملیات رمزگذاری را دارد، حملات به دو دسته تقسیم‌بندی می‌گردد:

2.1 حملات فعال

در این نوع حملات دستگاه رمزنگاری، ورودی‌های آن و یا محیطی که دستگاه در آن در حال انجام عملیات است، دست‌کاری می‌شوند تا دستگاه رمزنگاری در شرایط غیرمعمول به اجرای عملیات رمزنگاری بپردازد. در این نوع حملات کلید مخفی از رفتار غیرعادی دستگاه تحت حمله به دست می‌آید. این موارد محدود است و به علت هزینه بالایی و درصد خطایی که می‌پذیرد زیاد مورد بررسی واقع نمی‌شود[1].

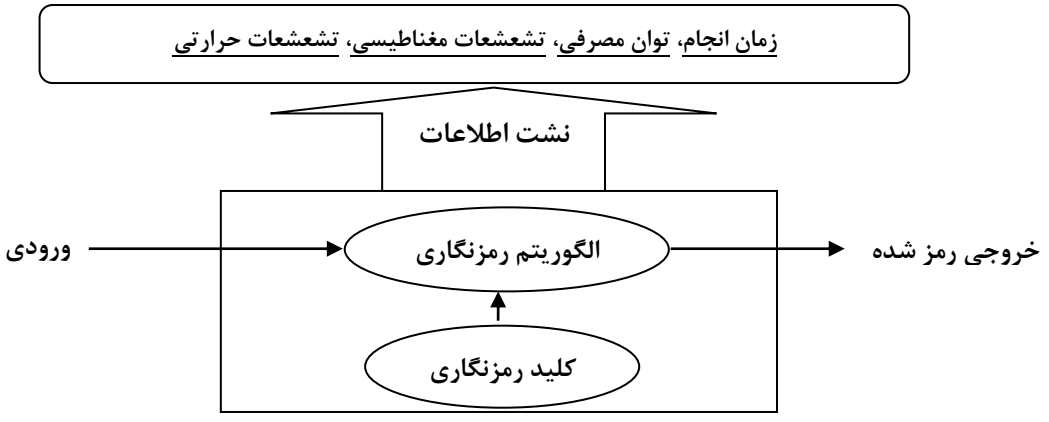
2.2 حملات غیرفعال

در این نوع حملات دستگاه رمزنگاری به کار عادی خود ادامه داده و حمله کننده سعی دارد با استفاده از کمیت‌هایی فیزیکی دستگاه تحت حمله (همچون زمان اجرا و توان مصرفی و غیره) کلید مخفی دستگاه را کشف کند. به دلیل اینکه در این نوع حملات هیچ‌گونه محدودیتی بر روی فعالیتی که دستگاه رمزنگاری انجام می‌دهد وجود ندارد، این نوع حملات قوی‌ترین نوع

از حملاتی هستند که به دستگاه‌های رمزنگاری اعمال می‌شود. در این حالت دسترسی انجام شده جهت اندازه‌گیری کمیت های فیزیکی مانند اختلاف پتانسیل و غیره باشد از نوع حملات غیرفعال و اگر مقادیر سیگنال داخلی تغییر یابند و یا در روند فعالیت دستگاه خللی ایجاد گردد از نوع غیرفعال خواهد بود. به این نوع حملات، حملات جانبی کانال گویند[1].

3. حملات جانبی بر روی کارت هوشمند

دستگاه‌های رمزنگاری دارای رابطه فیزیکی، منطقی و الکتریکی می‌باشند. دسترسی به برخی از این رابطه‌ها ساده بوده و دسترسی به برخی نیازمند ابزار و تجهیزات خاصی است. در این نوع حملات دستگاه رمزنگاری به همان شکلی که وجود دارد مورد حمله قرار می‌گیرد و هیچ خللی در شکل ظاهر و روند اجرای آن به وجود نمی‌آید، در نتیجه هیچ آثاری از حمله انجام شده بر روی دستگاه رمزنگاری باقی نخواهد ماند. اغلب حملات غیر تجاوزگرانه با استفاده از ابزار و تجهیزات ارزان‌قیمتی انجام می‌پذیرد و درنتیجه تهدیدی جدی برای امنیت دستگاه‌های رمزنگاری است. عموماً این نوع حملات را حملات جانبی کانال گویند. برای اولین بار در سال 1996 ایده استفاده از اطلاعات کانال جانبی برای تحلیل الگوریتم‌های رمز مدرن در [11] ارائه شد. کانال جانبی که در آن به بررسی پرداخته‌شده بود بررسی زمان اجرای الگوریتم بود، بااین‌وجود به سایر کانال های موجود از قبیل توان مصرفی نیز اشاره کرده بود. در [11] خاطرنشان ساخته بود که برخی از روش‌های مطرح شده برای مقابله با تحلیل زمانی ممکن است الگوی توان مصرفی مشخصی از خود بروز دهند و حمله کننده با بررسی این کانال بتواند تحلیل‌های دیگری را ارائه نماید. در سال 1998 همان افراد طرح حمله کانال جدیدی را ارائه نمودند، که ایده استفاده اصلی آن بر اساس توان مصرفی مدار بود. علاوه بر این در [8] کانال‌های جدیدی ارائه شد که احتمال رخ دادن خطا در الگوریتم‌های رمزنگاری را تحت تأثیر قرار داد. تا حال حاضر چهار کانال اصلی به‌عنوان کانال جانبی تحلیل الگوریتم‌های رمزنگاری مورد استفاده قرار گرفته است که آن‌ها را می‌توان به‌صورت زمان اجرا الگوریتم و خطای محاسباتی الگوریتم و توان مصرفی در حین اجرای الگوریتم و امواج الکترومغناطیسی اشاره کرد. البته باید ذکر کرد که عملی بودن هر یک از حملات کانال جانبی به قابل اندازه‌گیری بودن اطلاعات کانال جانبی موردنظر دارد. برای مثال تنها در صورتی توان از تحلیل توان مصرفی استفاده کرد که بتوان با دقت بالاتر و مناسبی مقدار توان مصرف شده در حین اجرای الگوریتم را به دست آورد[5]. تلاش برای به دست آوردن کلید مخفی از روی این اطلاعات را حمله از طریق کانال جانبی می‌نامند. هدف حملات جانبی کانال استفاده از نشت اطلاعاتی که یک دستگاه رمزنگاری به‌منظور دستیابی به کلید مخفی سامانه است. اگرچه برخی از الگوریتم‌های رمزنگاری در برابر این روش‌های تحلیل نظری مقاوم هستند، پیاده‌سازی‌هایی که بدون توجه به نشت اطلاعاتی کانال‌های جانبی شوند دارای ضعف‌های امنیتی خواهند بود. اگر این اطلاعات نشت اطلاعات از کانال را بتوان به کلیدهای محرمانه ارتباط داد پس این کانال‌ها مورد حمله قرار گرفته است. برخی از نمونه‌های نشت اطلاعات در شکل (2) نشان داده شده است.



شکل(2): خروجی‌های غیرمستقیم از اجرای رمزنگاری بلوکی[7]

برای مثال یک الگوریتم رمزنگاری برای اجرای یک عملیات با یک کلید متفاوت دارای زمان متفاوتی خواهد بود. این اختلاف زمان ممکن است قابل اندازه‌گیری بوده و برای حمله از طریق زمان مورد استفاده قرار گیرد، و نشت اطلاعات از تراشه‌های الکترونیکی و کامپیوتر هنگام پردازش عملیات باعث به وجود آمدن آن شده است. ازآنجایی‌که سامانه‌های رمزنگاری نوین (کارت‌های هوشمند) با استفاده از گیت‌های منطقی پیاده‌سازی می‌شوند که خود این گیت‌های منطقی از تعدادی ترانزیستور و المان‌های دیگر تشکیل شده است. جریان‌های به وجود آمده در این مدارات و ترانزیستورها باعث به وجود آمدن تشعشعات الکترومغناطیسی شده و باعث بروز اختلاف توان مصرفی و اتلاف توان مصرفی می‌گردد. توان مصرفی در یک مدار مجتمع نشان دهنده بروز اجزای سازنده مدار است. می‌توان گفت که توان مصرفی یک قسمت خاص از مدار و تغییرات به وجود آمده در توان مصرف آن براساس تغییرات اعمال شده در روشن و خاموش کردن مدار یا همان ترانزیستور است. اختلاف به وجود آمده در این مدارات را به این نوع بیان می‌کنند که در حالت روشن برابر یک و در حالت خاموش برابر صفر در نظر می‌گیرند. برای مثال یک پردازنده از مدارهای مختلفی که برای انجام دادن یک عملیات جمع و یا بارگذاری کردن مقداری خاص در ریجیستر استفاده می‌کند، که باعث تفاوت در توان مصرفی برای این دو عملیات می‌گردد. ممکن است تعداد ترانزیستورهایی که در یک عملیات جمع بین بایت‌های برای oxA7 وoxB9 سویچ می‌کند بیشتر از تعداد ترانزیستورهایی که در جمع داده‌های ox01 وox00 تغییر حالت می‌دهند. با توجه به اینکه میزان توان مصرفی یک مدار مجتمع به داده‌های پردازش شده بستگی دارد، اندازه‌گیری توان مصرفی آن اطلاعاتی درباره عملیات اتفاق افتاده را آشکار می‌کند. پس هنگامی‌که سامانه در حال پردازش داده‌های یک الگوریتم رمزنگاری است توان آن می‌تواند برای استخراج کلید مورد استفاده قرار گیرد[1]. برخی از نمونه‌های پیاده‌سازی این حملات نشان داده است که مدت زمان حمله موفق به کارت‌های هوشمند در حدود چند دقیقه بوده است و برای پیاده‌سازی آن‌ها توان محاسباتی و هزینه سخت‌افزار زیادی لازم نیست. در حمله زمانی اگر حمله کننده بتواند زمان اجرای هر دور الگوریتم را اندازه‌گیری کند، به سهولت کلید رمزنگاری را پیدا می‌کرد اما این امر معمولاً ممکن نیست، ولی این محدودیت برای تحلیل توان مصرفی وجود ندارد. در این نوع حمله‌ها حمله کننده حین انجام عملیات رمزنگاری مقدار توان مصرفی را تحت نظر دارد و نمودار توان مصرفی–زمان را به دست می‌آورد. پس کانال توان مصرفی اطلاعات دقیق‌تری از سیستم را دارد و این امر باعث قدرتمندتر شدن تحلیل توان مصرفی می‌شود[10].

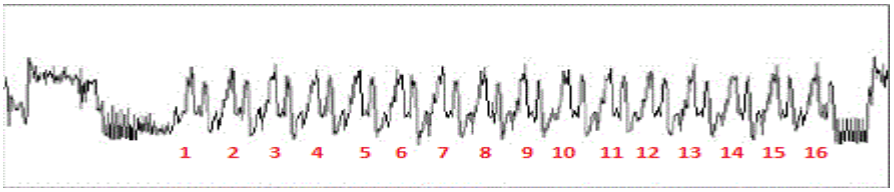
4. حمله بر اساس تجزیه‌وتحلیل توان

یکی از قدرتمندترین و معمول‌ترین نوع حملات جانبی کانال استفاده از تجزیه‌وتحلیل توان برای حمله است. این حمله از طریق نشت اطلاعات از منبع توان که در طول اجرای الگوریتم رمزنگاری رخ می‌دهد مورد استفاده قرار می‌گیرد. در حملات از طریق تجزیه‌وتحلیل توان سعی بر پیدا کردن یک راه‌حل و رابطه مناسب بین مصرف لحظه‌ای توان و وضعیت داخلی آن در زمان اجرای الگوریتم رمزنگاری است. برای اندازه‌گیری توان مصرفی یک کارت هوشمند می‌توان به‌راحتی یک مقاومت کوچک را به صورت سری با ورودی منبع تغذیه ولتاژ تراشه کارت قرار داد و ولتاژ دو سر مقاومت را اندازه‌گیری کرد که در نتیجه جریان(توان) مصرفی مدار و یا همان تراشه به دست می‌آید و می‌توان مقدار آن را بر روی سیستم ذخیره‌سازی کرد.

تجزیه‌وتحلیل توان برای حملات جانبی را می‌توان به سه بخش تقسیم‌بندی کرد:

- ✓ پیدا کردن یک رابطه منطقی بین اطلاعات کلید محرمانه و مصرف توان لحظه‌ای و همچنین نیاز به تعیین ورودی‌های مورد نیاز برای سیستم و مقادیر خروجی برای اندازه‌گیری و یادداشت کردن آن.
- ✓ استخراج حالت‌های مختلف اندازه‌گیری و یادداشت آن که شامل موارد از قبل مشخص شده برای مصرف توان می‌شود. مجموعه‌ای از اندازه‌گیری‌ها و همچنین دانستن عملیاتی که در طول اجرای الگوریتم رمزنگاری اتفاق می‌افتد.
- ✓ بررسی رابطه بین آیتم‌های اندازه‌گیری به وسیله پردازش کردن بر روی اطلاعات استخراج شده.

بنابراین با بررسی اثرات توان، استخراج کردن آنچه در طول عملیات رخ داده است برای ما ممکن خواهد بود. برای مثال شکل (5) نشان می‌دهد که مصرف توان لحظه‌ای برای یک قطعه رمزنگاری بر اساس الگوریتم (DES) انجام شده است[1,4].

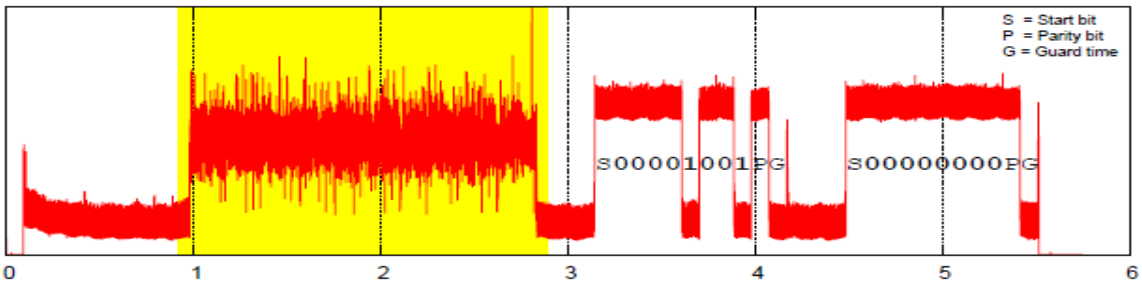


شکل(5): نشان دادن آثار مصرف توان در الگوریتم DES

16 مرحله منحصربه‌فرد از رمزنگاری با استفاده از الگوهای تکرار شده در شکل قابل مشاهده است. بااین‌حال اگرچه بیت داده منحصربه‌فرد دست‌کاری شده در طول رمز کردن را نمی‌توان مشخص کرد. باوجوداینکه نمی‌توان به‌طور مستقیم مقدار داده را مشخص کرد، اما این شکل از تجزیه‌وتحلیل هنوز هم می‌تواند مفید باشد. به وسیله شناختن این نقاط در یک رمزنگاری برای حمله کردن، می‌توان آن را برای حمله قدرتمندانه‌تر مورد استفاده قرار داد. این اختلاف و تفاوت در مصرف توان لحظه‌ای نیز می‌تواند به ارزش و مقدار هر بیت که در حال دست‌کاری و اجرای عملیات است مربوط باشد. مصرف توان سخت‌افزاری با تغییر دادن مقادیر بیت‌ها در یک مقیاس خیلی کوچک‌تر مورد تغییر قرار می‌گیرد. با توجه به ماهیت دقیق و مقیاس کوچک تغییرات توان، انتخاب و تشخیص مقدار سخت می‌شود. همچنین ممکن است تغییرات به وجود آمده در سخت‌افزار و یا روش‌های آماری نیاز برای شناسایی مفید واقع شود[7,9].

4.1 حمله از طریق تحلیل توانی ساده (SPA[1])

در این روش حمله کننده مستقیما از طریق بررسی مقدار توان خروجی توان مصرفی حمله را انجام می‌دهد و داده‌های به دست آمده از توان مصرفی الگوریتم در حین اجرای رمز، به صورت مستقیم برای پی بردن به الگوریتم رمز و بیت‌های کلید مورد استفاده قرار می‌گیرد. در این نوع روش‌ها با استفاده از شکل موج خروجی و اینکه با چه الگوریتمی سیستم در حال رمز کردن است مستقیما می‌توان پی به رابطه الگوریتم برد و مقدمات استخراج برای کلید را فراهم آورد. با توجه به اینکه با SPA می‌توان دستورالعمل‌های در حال اجرا را آشکار نمود، اگر الگوریتم رمز به نحوی پیاده‌سازی شود که مسیر اجرای دنباله دستورالعمل‌ها وابسته به داده‌های مورد پرازش مثلا بیت‌های کلید باشد در این‌صورت با روش ساده SPA اطلاعات زیادی راجب به بیت‌های کلید را می‌توان به دست آورد. در این نوع از روش‌ها که با استفاده از تجزیه و تحلیل شکل موج‌های خروجی و همچین مقادیر خروجی به دست آمده است مهاجم سعی می‌کند برای پیداکرن الگوهایی برای مطابقت دادن با یک الگوی قالب را تلاش کند و یک رابطه منطقی بین الگوریتم‌های به وجود آمده برای رمز کردن را پیدا کند[7,8]. شکل زیر استخراج و حدس کلید به این روش را نشان می‌دهد.



شکل(6): استخراج کد از طریق تجزیه و تحلیل توانی ساده[9]

1 Simple Power Analysis

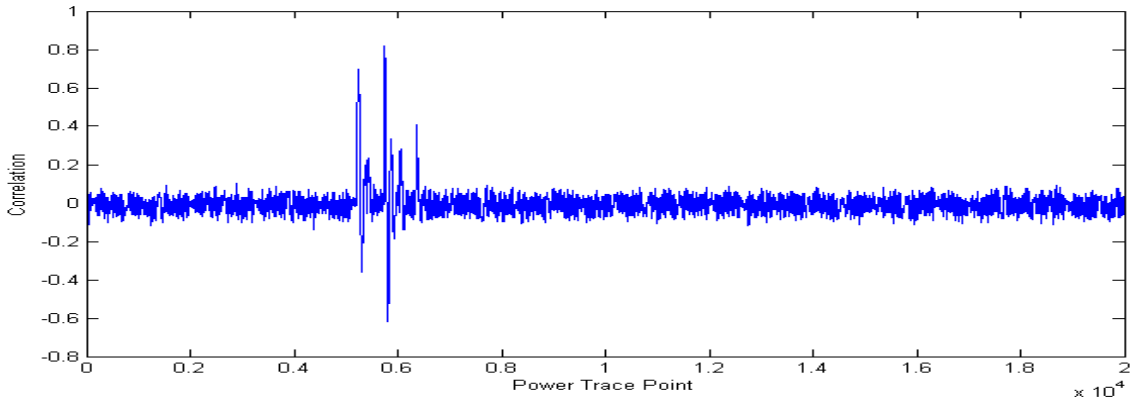
4.2 حمله از طریق تحلیل تفاضلی توان (DPA[1])

در اغلب موارد، SPA به تنهایی برای استخراج یک کلید مخفی کافی نمی‌باشد. حمله از طریق DPA بسیار قوی‌تر از حمله از طریق تجزیه و تحلیل آماری است. در روش پیشرفته‌تر تحلیل توان یعنی روش تحلیل تفاضلی توان از همبستگی بین مصرف توان سیستم و مقادیر داده‌های میانی و کلید که در هنگام اجرای الگوریتم رمز به کار می‌روند جهت حمله به سیستم استفاده می‌شوند. معمولاً این همبستگی در مقایسه با نویز موجود در اثر مصرف توان سیستم کوچک بوده و به‌راحتی قابل مشاهده نیست. برای استخراج این همبستگی‌ها در حضور نویز، بسته به کیفیت ریزپردازنده به‌کاررفته و نوع دستورالعمل های آن چندین هزار تابع نمونه مصرف توان جمع‌آوری شده و با روش‌های آماری همبستگی موجود استخراج می‌گردد. مزیت اصلی حملات DPA در مقایسه با حملات SPA این است که در این نوع حملات هیچ دانش دقیق در مورد رمزنگاری دستگاه لازم نیست. در حملات SPA آنالیز مصرف توان یک دستگاه عمدتاً در طول محور زمان قرار دارد و درنتیجه مهاجم سعی می‌کند برای پیدا کردن الگوهایی برای مطابقت دادن با یک الگوی قالب را تلاش می‌کند. در صورتی که در حمله DPA، شکل نمونه‌ها در طول محور زمان زیاد مورد اهمیت نیست و ازاین‌رو در لحظات ثابتی از زمان به داده های پردازش‌شده بستگی دارد، همچنین حملات DPA منحصراً وابسته به مصرف توان داده‌ها می‌باشد. در این روش از همبستگی بین مصرف توان سیستم و مقادیر داده‌های میانی و کلید که در هنگام اجرای الگوریتم رمز به کار می‌روند جهت حمله به سیستم استفاده می‌شوند. به این صورت که بعد از نمونه برداری از مصرف توان برای چندین هزار نمونه، نمونه‌های به دست آمده را به دو بخش (LSB,MSB) تقسیم بندی کرده و برای آنها یک میانگین را در نظر می‌گیریم. سپس تک‌تک کلیدهای ممکن را برای آن اعمال کرده و تغییرات به وجودآمده را در شکل موج‌های حاصل شده لحاظ می‌کنیم. ملاحظه خواهد شد که ما در برخی از این شکل موج‌ها دارای جهش‌هایی برای اختلاف این دو دسته خواهیم بود که آن بیانگر کلید صحیح برای ما خواهد بود.

گام‌های اساسی برای انجام یک آزمون DPA به شرح زیر است:

- ✓ انجام تعداد زیادی از عملیات رمز یا رمزگشایی بر روی یک دستگاه رمزنگاری با مجموعه‌های مختلف از داده‌ها
- ✓ پردازش و اندازه‌گیری و ثبت مصرف توان و خروجی داده‌ها یا ورودی آن در طول هر یک از عملیات اجرایی
- ✓ تقسیم‌بندی اندازه‌گیری توان به زیرمجموعه‌هایی مطابق با ویژگی پردازش‌شده
- ✓ پیدا کردن اختلاف آماری بین زیر مجموعه‌ها، وقتی که اختلاف مشاهده شد، نشت اطلاعات تشخیص داده شده است[8].

شکل (6) اجرای صحیح الگوریتم برای پیدا کردن کلید صحیح را نشان می‌دهد.



شکل(6): یک نمونه از کلید صحیح حدس زده شده

1 Differential Power Analysis

5. روش‌های مقابله با حملات جانبی کانال

- ✓ دستگاه رمزنگاری می‌تواند به‌گونه‌ای ساخته شود که تمامی عملیات‌ها مستقل از داده پردازش شده، به میزان یکسان و مساوی توان مصرف کنند. استفاده از سبک منطق خاص از مهم‌ترین این روش‌ها محسوب می‌شود.
- ✓ دستگاه رمزنگاری می‌تواند به‌گونه‌ای ساخته شود که توان مصرفی حاوی اطلاعات تصادفی بسیاری باشد.
- ✓ اگر بتوان واحد رمز را در منطقی پیاده‌سازی نمود که در آن منطق، خروجی گیت در تمام زمان‌ها مستقل از تغییرات سیگنال، توان مصرفی ثابتی را داشته باشد، در این صورت پایه و اساس حمله تحلیل توانی از بین رفته است.
- ✓ یک روش معمول برای مقاوم‌سازی در برابر حمله‌های توانی و به‌طور کلی حمله‌های کانال جانبی تصادفی کردن داده‌هایی است که از میان کانال‌های مختلف مانند توان مصرفی، ارتعاشات الکترومغناطیسی و زمان اجرای دستورالعمل‌ها نشت می‌کنند. این روش تضمین می‌کند که حمله کننده فقط اطلاعات تصادفی را به دست آورده و درنتیجه هیچ‌گونه اطلاعات سودمندی درباره داده‌های میانی که در محاسبه‌ها تولید می‌گردد نشت نمی‌کند.
- ✓ تکنیک پوشش گذاری داده یکی از روش‌های مقاوم‌سازی است که بیش از روش‌های دیگر برای مقابله در برابر حملات تحلیل توانی و الکترومغناطیسی و در برخی از موارد برای مقابله با حمله زمانی مورد استفاده قرار می‌گیرد. در این روش در ابتدا داده‌های ورودی همچون متن واضح و کلید با مقادیری که به شکل تصادفی تولید شده‌اند نقاب گذاری می‌شوند و در پایان عملیات (در پایان هر دور الگوریتم رمز) با مقادیر دیگری که متناسب با نقاب اولیه هستند پوشش برداری می‌شوند. به‌این‌ترتیب اطلاعات نشت یافته با متن واضح و یا متن رمز شده همچون قبل همبستگی نخواهند داشت.

5. نتیجه‌گیری

یکی از روش‌های دستیابی به کلید محرمانه در الگوریتم‌های رمزنگاری بر روی کارت هوشمند، حملات جانبی بر روی آن است و معتبرترین نوع آن نیز بررسی توان مصرفی در حین اجرای الگوریتم می‌باشد. حملات تحلیل توانی به دلیل وابستگی بین توان مصرفی دستگاه رمزنگاری و مقادیر میانی الگوریتم در حال اجرا حملات موفقیت آمیزی می‌باشند. در هیچ یک از روش‌های مقاوم سازی امکان حمله تحلیل توانی از بین نمی‌رود، بلکه انجام حمله دشوارتر می‌گردد. اگر بتوان علت حمله را کنترل کرد در این صورت امکان حمله از مین خواهد رفت. علت حمله تحلیل توانی آن است که سیگنال توان با تغییر داده ورودی تغییر می‌کند و در نتیجه چنانچه توان مصرفی مستقل از سیگنال ورودی باشد امکان حمله از میان خواهد رفت.

7. مراجع

1. باقرزاده، ج.، (1391) ، "تحلیل توانی کارت هوشمند"، پایان نامه کارشناسی ارشد، دانشگاه صنعتی شریف، تهران.
2. اسکندری، ه.، (1393) ، "رمزنگاری تصاویر دیجیتال "، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی، تبریز(اهر).
3. https://fa.wikipedia.org/wiki
4. International Standard, (2006) ISO/IEC 7816-3 Third edition, Published in Switzerland.
5. فرجی، آ.، (1387) ، "حمله تحلیل توانی روی الگوریتم رمز Serpent و بررسی تکنیک WDDL در ارتقاء امنیت آن"، پایان نامه کارشناسی ارشد، دانشگاه صنعتی امیرکبیر، تهران.
6. ریحانی‌تبار، م.، (1381) ، "حمله به کارت‌های هوشمند با استفاده از اطلاعات نشتی"، پایان نامه کارشناسی ارشد، دانشگاه صنعتی شریف، تهران.
7. Kevin, M., (2012) "Differential Power Analysis attacks on AES" Cryptography II VCSG-706, USA.
8. Pauk, K. (1999) "Differential Power Analysis" technical report, cryptography research inc.
9. Dennis, V,.(2012) "Reverse engineering of Java Card applets using power analysis" Faculty of Electrical Engineering, Mathematics and Computer Science, Mekelweg 4,2628 CD Delft.The Netherlands.
10. Artin ,P.,(2010) "Reverse engineering of Java Card Applets" Bachelor Thesis, Masaryk University Faculty Of Informatics.
11. Pauk, K. (1996) "timing attacks on implementations of diffie hellman rsa dss and other systems" in Advances in cryptography –crypto,. Vol 1109 ,pp104-113.