مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"

سال دوم، شماره ۲، تابستان ۱۳۹۳،ص ۷۰-۶۳

پیاده‌سازی مؤثر و کارآمد حمله تحلیل تفاضلی الکترومغناطیس بر روی یک تحقق سخت‌افزاری الگوریتم رمزنگاری AES

محمدهادی رضایتی[1*]، احمدرضا امین[2]، مسعود معصومی[3]، حامد مومنی[4]

۱- کارشناس ارشد الکترونیک، دانشگاه جامع امام حسین (ع) ۲- استادیار، دانشگاه جامع امام حسین (ع)

۳- استادیار، دانشگاه آزاد اسلامی واحد اسلامشهر، گروه الکترونیک ٤- کارشناس ارشد رمز، دانشگاه جامع امام حسین (ع)

(دریافت: ۹۲/۱۲/۲۱ ، پذیرش: ۹۳/۵/۱۵)

چکیده

حمله تحلیل الکترومغناطیس، نوع قدرتمند و منحصر بفردی از حملات کانال جانبی است که از تشعشعات ساطع‌شده از تراشه در حال رمز کردن اطلاعات برای شکستن الگوریتم رمز و به‌دست آوردن کلید آن استفاده می‌کند. پیاده‌سازی عملی این حمله بر روی تراشه‌های رمزنگاری به‌دلیل وجود پیچیدگی‌های خاص، خود موضوعی کاملا جذاب و در عین حال چالش‌برانگیز است. یکی از مهم‌ترین این چالش‌ها، اندازه‌گیری و ثبت تشعشعات الکترومغناطیس ساطع‌شده از یک تراشه به‌طور صحیح و با کمترین میزان نویز ممکن می‌باشد. در این مقاله، نحوه تحقق حمله الکترومغناطیس بر روی الگوریتم رمز AES بررسی شده است. همچنین نحوه ساخت پروب و تقویت کننده الکترومغناطیس مورد نیاز برای انجام این تحلیل که بحرانی‌ترین بخش انجام تحلیل می‌باشد، تشریح گردیده است. نتایج پیاده‌سازی حمله الکترومغناطیس علیه تحقق رمز AES بر روی میکروکنترلر ۸۰۵۱ نشان‌دهنده صحت روش تحلیل و موفق بودن حمله مزبور می‌باشد.

واژه‌های کلیدی: حمله تحلیل الکترومغناطیس، الگوریتم AES، پروب مغناطیسی

۱. مقدمه

در مدل متداول و سنتی، امنیت سیستم‌های رمزنگاری از منظر توابع ریاضی به‌کاررفته ارزیابی می‌شد. این روش، آثار فیزیکی و الکتریکی جانبی در پیاده‌سازی توابع و مدارات را در نظر نمی‌گیرد. در مدل واقعی‌تر، برای ارزیابی امنیت ابزار رمزنگاری، به حملات کانال جانبی یا حملاتی که از اطلاعات مرتبط با پیاده‌سازی فیزیکی توابع رمزنگاری استفاده می‌کنند نیز توجه می‌شود. حمله تحلیل تفاضلی الکترومغناطیس، نوع قدرتمند و منحصر بفردی از حملات کانال جانبی است که از تشعشعات ساطع‌شده از تراشه‌ای که در حال رمز کردن اطلاعات است برای شکستن الگوریتم رمز و به‌دست آوردن کلید آن استفاده می‌کند. پیاده‌سازی عملی این‌گونه حملات بر روی انواع تراشه‌های رمزنگاری به‌دلیل وجود پیچیدگی‌های هر یک از آنها موضوعی جذاب و در عین حال چالش‌برانگیز است.

بعد از مقاله پاول کوچر [۱] که در سال ۱۹۹۶ منتشر شد، مقالات زیادی موفقیت حملات کانال جانبی روی پیاده‌سازی الگوریتم‌های متقارن و نامتقارن را گزارش کردند [۶-۲].

تشعشعات الکترومغناطیس تراشه‌ها با جریان تغذیه آنها در یک دستگاه رمزنگاری همبسته هستند. استاندارد IEC ۶۱۹۶۷ حداکثر سطح مجاز تشعشعات یک تراشه را مشخص می‌کند [۷]، در حالیکه برای تراشه‌های پیاده‌ساز الگوریتم رمزنگاری، ملاحظات اضافی دیگری نیز باید در نظر گرفته شود. با توجه به اینکه انتشارات الکترومغناطیس و جریان یک تراشه به داده‌های در حال پردازش تراشه بستگی دارد، بنابراین با اندازه‌گیری آنها برای تراشه‌ای که در حال اجرای الگوریتم رمزنگاری است می‌توان اطلاعاتی در مورد کلید رمز الگوریتم رمزنگاری به‌دست آورد.

* رایانامه نویسنده مسئول: m.h.rezayati@gmail.com

از مهم‌ترین حملات کانال جانبی می‌توان به حمله تحلیل توان و تحلیل الکترومغناطیس اشاره کرد. در مقایسه با حمله تحلیل توان، حمله الکترومغناطیس دارای مزیت‌های بسیار زیادی می‌باشد، زیرا حمله تحلیل توان فقط می‌تواند توان مصرفی کلی تراشه را به‌دست آورد [۸ و ۹]. برای تحلیل تراشه‌ها و پردازنده‌های نسل جدید که در یک کلاک توانایی اجرای چند دستور را دارند، توان مصرفی به‌دست‌آمده حاصل اجرای چند دستور بوده که تحلیل را بسیار دشوار می‌کند. در برخی از مقالات، موثر بودن تحلیل الکترومغناطیس اثبات شده است که مهم‌ترین مزیت آن، گرفتن سیگنال از قسمت خاصی از تراشه است. سیگنال الکترومغناطیس دستگاه‌ها معمولا ضعیف و نویزی است [۱]. بنابراین، سیستم ابزار اندازه‌گیری سیگنال الکترومغناطیس بسیار مهم است.

بسیاری از الگوریتم‌های شناخته‌شده مانند DES، AES، RSA و ECC که به لحاظ تئوری در برابر حملات آماری و کلاسیک امن هستند، در برابر این نوع حمله، ظرف مدت کوتاهی شکسته می‌شوند.

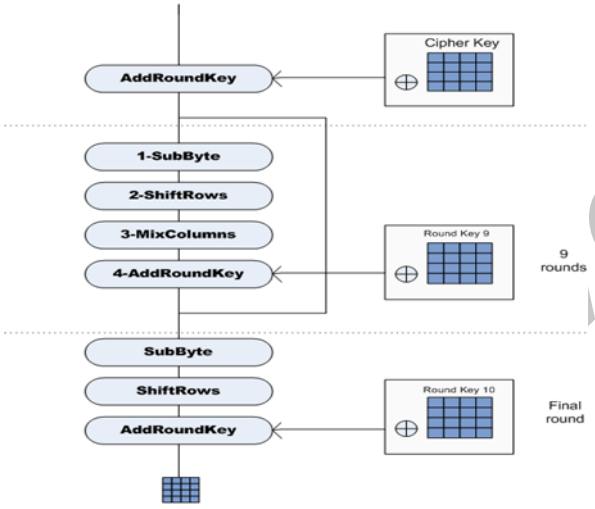
با توجه به مطالب ارائه‌شده در خصوص اهمیت پیاده‌سازی الگوریتم‌ها، امنیت میکروکنترلرها[1] در برابر حملات پیاده‌سازی نیز موضوعی بسیار مهم است. در این مقاله نحوه آسیب‌پذیری میکروکنترلر AT89C51AC2 در برابر این حملات مورد بررسی قرار گرفته و یک نمونه عملی از نحوه پیاده‌سازی حمله تحلیل الکترومغناطیس و نتایج به‌دست‌آمده از آن تشریح شده است. همچنین ابزارهای اندازه‌گیری حمله الکترومغناطیس در میدان نزدیک معرفی‌شده نیز طراحی و ساخت پروب مغناطیسی استفاده‌شده به‌منظور اجرای حمله بیان شده است.

در ادامه مقاله، ابتدا در بخش ۲، الگوریتم AES و سپس در بخش ۳، اصول تحلیل الکترومغناطیس تشریح شده است. در بخش ۴ در رابطه با ابزارهای اندازه‌گیری شامل برد و پروب ساخته‌شده بحث می‌شود. بخش ۵ به نحوه تحقق عملی حمله و بستر آزمایشگاهی مورد نیاز برای پیاده‌سازی آن اختصاص داده شده است. در بخش ۶ نتایج عملی به‌دست‌آمده را ارائه داده و در انتها به جمع‌بندی موضوع و ارائه نتایج نهایی پرداخته شده است.

۲. الگوریتم AES

الگوریتم AES یک رمز کلید متقارن است، که هم گیرنده و هم فرستنده از یک کلید مشابه برای رمزگذاری و رمزگشایی استفاده می‌کنند. طول متن اصلی ۱۲۸ بیت ثابت است، درحالیکه طول کلید می‌تواند ۱۲۸، ۱۹۲ یا ۲۵۶ بیت باشد. الگوریتم AES یک الگوریتم تکراری است. هر تکرار یک دور نامیده می‌شود و تعداد کل دورها ۱۰، ۱۲ و یا ۱۴ دور است.

ورودی الگوریتم، یک قالب ۱۲۸ بیتی اطلاعات است که به ۱۶ بایت تقسیم می‌شود. این بایت‌ها وارد آرایه‌های ۴×۴ که حالت نامیده می‌شوند، می‌شوند .هر عضو این آرایه، عنصری از میدان محدود $GF(2^8)$ است که بر چند جمله‌ای اولیه $m(x) = x^8 + x^4 + x^3 + x + 1$ بنا نهاده شده است. همه عملیات‌های مختلف الگوریتم AES از قبیل جمع با کلید دور، جانشینی بایت‌ها، شیفت سطری و مخلوط کردن ستون‌ها بر روی همین آرایه انجام می‌گیرد[۱۰].



شکل ۱. دیاگرام قالبی الگوریتم AES

هر دور الگوریتم AES شامل چهار عملیات است. فقط دور آخر یعنی دور دهم شامل سه عملیات است.

در عملیات جانشینی بایت‌ها ((SubBytes) هر بایت با معکوس ضربی خود در میدان جایگزین می‌شود یا به‌عبارت دیگر، هر بایت با بایت متناظر خود در SRDSBox جایگزین می‌شود.

$$\text{SubBytes: } S_{i,j}^{[r]} \leftarrow S_{RD}\left(S_{i,j}^{[r]}\right)$$

در عملیات شیفت دادن سطرها ((ShiftRows) سطر i از ماتریس State به‌طور حلقوی i بایت به‌سمت چپ شیفت می‌خورد

$$\text{ShiftRows: } S_{i,j}^{[r]} \leftarrow S_{i,(j+i) \bmod 4}^{[r]}$$

1. Microcontroller

در عملیات ترکیب، ستون‌ها (MixColumns()) ستون J را با ضرب‌های ثابت در $GF(2^8)$ ترکیب می‌کند.

$$\text{MixColumns: } S_{i,j}^{[r]} \leftarrow \oplus_{0\le i\le 3} S_{(i-1) \bmod 4,j}^{[r]} \odot c_i$$

$$\text{where} \sum_{0\le i\le 3} c_i X^i = 02 + 01X + 01X^2 + 03X^3$$

۳. حمله تحلیل تفاضلی الکترومغناطیس

با قرار دادن کویل‌هایی در کنار تراشه رمزنگاری و بررسی تشعشعات الکترومغناطیسی ساطع‌شده از آن می‌توان به توالی دستورالعمل‌های اجراشده توسط آن پی برد. این حمله اولین بار توسط Quisquater و Samyde [۱۱] معرفی شد و بعدا توسط دیگران گسترش داده شد. حمله تحلیل زمان، یک حمله یک بعدی است که تنها زمان را اندازه می‌گیرد. حمله آنالیز، توان یک بردار دوبعدی را باز می‌گرداند که نشان‌دهنده نمونه‌های توان در محور زمان است. چون موقعیت کویل‌های اندازه‌گیر تشعشع نیز در حمله الکترومغناطیس مهم است، لذا از این حمله به یک حمله سه بعدی تعبیر می‌شود.

حمله آنالیز مهم‌ترین حمله به پیاده‌سازی AES است. معمولا این حمله، تابع جانشینی بایت‌ها در دور اول را هدف قرار می‌دهد، زیرا این قسمت تنها بخشی از الگوریتم رمز است که مستقیما با کلید رمز در ارتباط است. ابتدا مهاجم یک بیت را که تابعی از متن آشکار و قسمتی از کلید باشد انتخاب می‌کند. معمولا این بیت یکی از بیت‌های تبدیل جانشینی بایت‌ها یا خروجی تابع جمع با کلید دور است. با اجرای مکرر روال حمله، مهاجم قسمتی از کلید را به‌دست می‌آورد که تعداد دفعات اجرای روال حمله بسیار کوچک‌تر از جستجوی جامع فضای کلید است. در ذیل، روال حمله DPA برای شکستن AES را مورد بررسی قرار می‌دهیم [۱۲].

سناریوی حمله تفاضلی توان به‌قرار زیر است:

۱) ابتدا مهاجم N متن آشکار را به‌طور تصادفی تولید می‌کند.

۲) سپس سیگنال مصرف توان هر متن که حاوی n نمونه است را به‌طور جداگانه اندازه‌گیری و ذخیره می‌کند.

۳) متن آشکار همراه با اولین بایت زیر کلید اول، به یک مدل فرضی از الگوریتم AES (مثلا یک AddRoundKey یا یک SBox) داده شده و به این خروجی فرضی، یک تابع انتخاب D اعمال می‌شود.

این تابع انتخاب مشاهدات را به دو دسته جداگانه تقسیم می‌کند: دسته‌ای که تابع انتخاب، خروجی مقدار صفر را و دسته‌ای که تابع انتخاب خروجی مقدار یک را بر می‌گرداند.

۴) پس از متوسط‌گیری از هر دو دسته، از آنها تفاضل می‌گیریم.

۵) برای هر منحنی، تفاضل بزرگترین پیک و مقدار متوسط آن محاسبه شده و مقدار نسبت بزرگترین پیک به مقدار متوسط را نگاه می‌داریم.

۶) مراحل ۳ تا ۵ را برای تمام ۱۲۸ کلید ممکن تکرار می‌کنیم که ۱۲۸ منحنی تفاضل به‌دست خواهد آمد.

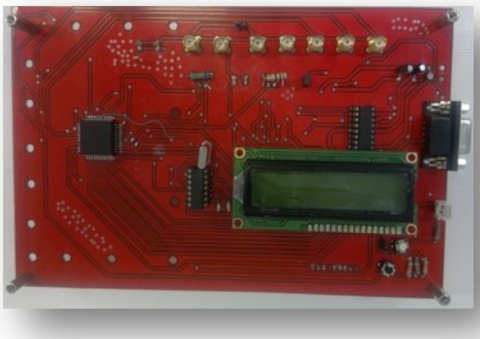
۷) سپس این منحنی‌های تفاضل را مورد بازبینی و بررسی قرار می‌دهیم. فقط برای یک حدس صحیح از زیرکلید، تابع انتخاب مقدار صحیحی را برمی‌گرداند و در منحنی‌های تفاضل ضربه‌هایی به‌طور کاملا متمایز قابل مشاهده خواهد بود. در غیر این‌صورت، مشاهدات، منحنی‌های نرم و یکنواختی بدون تغییرات عمده خواهد بود.

مراحل ۲ تا ۷ را شانزده مرتبه دیگر تکرار کرده تا ۱۲۸بیت کلید به‌طور کامل کشف شود.

به‌منظور افزایش نسبت سیگنال به نویز و نیز دقت حمله، به‌جای درنظر گرفتن یک بیت از خروجی، می‌توان یک مجموعه چند بیتی خروجی را مورد بررسی قرارداد. مرجع[۱۳] نشان داده است که به این ترتیب میزان قله‌های ثانویه و قله‌های شبح در منحنی‌های تفاضل کاهش یافته و کیفیت حمله بهبود پیدا می‌کند. مثلا در حمله به الگوریتم AES، به‌جای درنظر گرفتن یک بیت از خروجی SBox دور اول به‌عنوان تابع هدف می‌توان یک مجموعه چهار بیتی را مورد بررسی قرار داد. در این‌صورت تابع انتخاب هنگامی‌که وزن همینگ خروجی بیش از چهار باشد، مقدار یک و در غیر این‌صورت، مقدار صفر را برمی‌گرداند.

۴. پیاده‌سازی عملی تحلیل تفاضلی الکترومغناطیس علیه یک سیستم واقعی

برای اجرای حمله خود، ابتدا الگوریتم AES را بر روی یک میکروکنترلر هشت بیتی AT89C51AC2 پیاده‌سازی کرده و



شکل ۲. بورد طراحی‌شده برای اعمال حمله تحلیل الکترومغناطیس

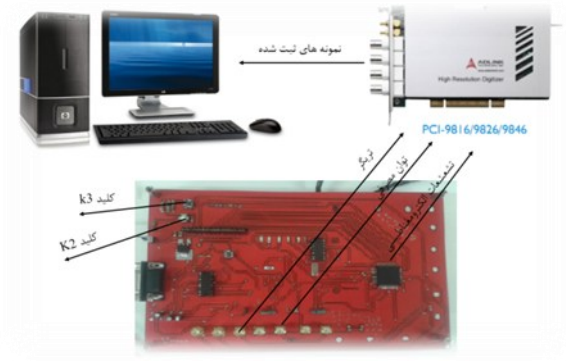
بدین‌ترتیب سخت‌افزار رمزکننده آماده رمزنگاری می‌شود. میکروکنترلر AT89C51AC2 محصول شرکت Atmel بوده و سهم بسزایی در بازار میکروکنترلرها دارد. میکروکنترلر انتخاب‌شده دارای واسط RS232 بوده و فضای کافی برای پیاده‌سازی AES را نیز دارد [۱۴]. رمزکننده ساخته‌شده از طریق درگاه RS232 به رایانه متصل می‌شود. برای اعمال حمله تحلیل الکترومغناطیس تمام تمهیدات لازم اندیشیده شده که شکل ۲، بورد ساخته‌شده را نشان می‌دهد.

یک واسط کاربری روی رایانه با استفاده از نرم‌افزار MATLAB تهیه شده که با رمزکننده ارتباط برقرار می‌کند و قالب‌های ۱۲۸ بیتی داده را برای آن ارسال می‌کند. سخت‌افزار رمزکننده با دریافت یک قالب داده، آن را رمز می‌کند و نتیجه را به رایانه باز می‌گرداند و همچنین آن را روی LCD نیز نمایش می‌دهد.

برای ذخیره نمونه‌ها، جهت تحلیل آنها از کارت نمونه‌بردار شرکت ADLINK استفاده شده که در شکل ۳ نمایش داده شده است.

شکل ۳: بورد نمونه‌بردار سیگنال ساخت شرکت ADLINK

شکل ۴ کلیات و چگونگی ارتباط بین رایانه، سخت‌افزار رمزنگار و کارت نمونه‌بردار را نشان می‌دهد.



شکل ۴. ارتباط بین رایانه، سخت‌افزار رمزنگار و کارت نمونه‌بردار

همان‌طور که گفته شد برای نمونه‌برداری از اثر توان، از یک کارت نمونه‌بردار که روی مادربورد رایانه قرار می‌گیرد، استفاده شده است.

این کارت دارای نرخ نمونه‌برداری ۴۰MSample/S است. برای شروع یک نمونه‌برداری از سیگنال الکترومغناطیس، ابتدا رایانه کارت نمونه‌بردار را آماده می‌کند و کارت منتظر دریافت سیگنال چکانه برای شروع نمونه برداری می‌ماند. این چکانه به‌صورت خارجی و از طریق رمزنگار تولید خواهد شد. علت این امر آن است که در لحظه شروع یک عملیات خاص، کارت شروع به نمونه‌برداری کند و داده‌ای از دست نرود.

حال رایانه داده مورد نظر برای رمزنگاری را به رمزنگار می‌فرستد. سپس به رمزنگار فرمان شروع می‌دهد. رمزنگار با دریافت این دستور، عملیات خود را آغاز می‌کند و در ابتدای عملیات، سیگنال چکانه را نیز تولید می‌کند. با این کار، کارت شروع به نمونه‌برداری کرده و یک نمونه از اثر تشعشعات الکترومغناطیس شامل ۲۰۰۰ نقطه برداشته می‌شود. وقتی رمزنگار عملیات خود را تمام کرد، اتمام کار خود را به رایانه اعلام می‌کند. در این لحظه رایانه با ارسال دنباله دستورات مناسب به کارت، نمونه تشعشع الکترومغناطیس برداشته‌شده را روی هارد دیسک رایانه ذخیره می‌کند و سپس کارت را برای نمونه‌برداری بعدی آماده می‌کند.

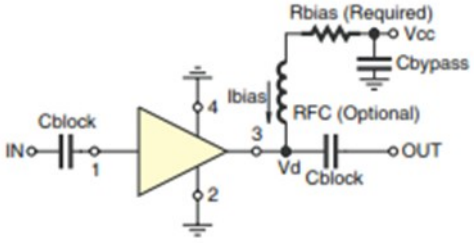
در حملات تحلیل الکترومغناطیس برای داشتن یک نتیجه خوب باید اثر نویزهای تصادفی و نویزهای الکترونیک را حذف کرد. برای حذف نویز، عملیات رمزنگاری برای یک داده مشخص (Plaintext) را ده بار تکرار کرده و نمونه‌های تشعشع الکترومغناطیس ذخیره می‌شود. سپس با انتقال داده‌ها به رایانه، از این نمونه‌ها میانگین‌گیری می‌شود. در واقع با میانگیری از ده سیگنال تشعشعات الکترومغناطیس به ازای هر متن اصلی، اثر نویزهای ناخواسته را تا

حد امکان از بین برده تا تحلیل دقیق‌تری انجام شود. در نهایت داده‌ها برای میانگین‌گیری، رسم نمودارهای تشعشعات الکترومغناطیس و انجام دیگر تحلیل‌ها از نرم‌افزار MATLAB کمک گرفته شده است.

۱.۴. طراحی و ساخت پروب مغناطیسی برای اجرای حمله الکترومغناطیس

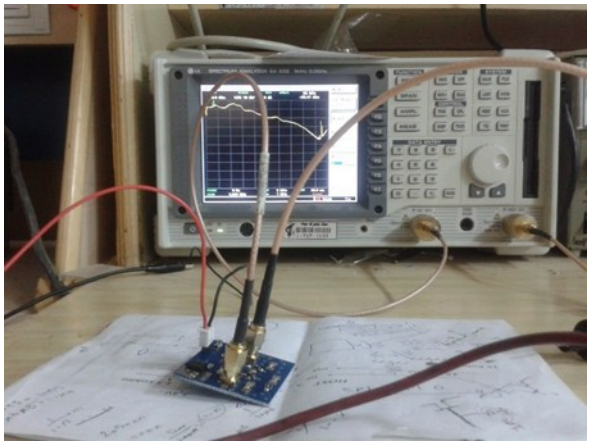
یکی از ابزارهای مهم در اجرای حمله الکترومغناطیس، پروب مغناطیسی می‌باشد. پروب مغناطیسی ساخته‌شده دارای دو قسمت است : تقویت کننده و آنتن.

برای ساخت تقویت کننده، از دو طبقه تقویت کننده فرکانس بالا که شامل تراشه MAR8 است، استفاده شده است. در شکل ۵ نمایش مداری این تراشه را ملاحظه می‌کنید.



شکل ۵. نمایش مداری تراشه MAR8

تقویت کننده ساخته‌شده سیگنال گرفته‌شده را تا فرکانس ۵۰۰MHz و به میزان ۵۰dbm تقویت می‌کند. شکل ۶ تقویت ساخته‌شده را نشان می‌دهد.



شکل ۶. نمایی از تقویت کننده پروب و دستگاه تحلیلگر طیف

آنتن استفاده‌شده، از نوع آنتن متعادل حلقوی است که در این آنتن، شکاف هوایی وسط حلقه قرار دارد و هادی داخلی در گردنه حلقه زمین می‌شود. در این حلقه به‌دلیل تقارن، از اثرات ناشی از عدم تعادل جریان‌های کابل جلوگیری می‌شود. در شکل ۷ پیکربندی این نوع آنتن نشان داده شده است [۱۵و۱۶].

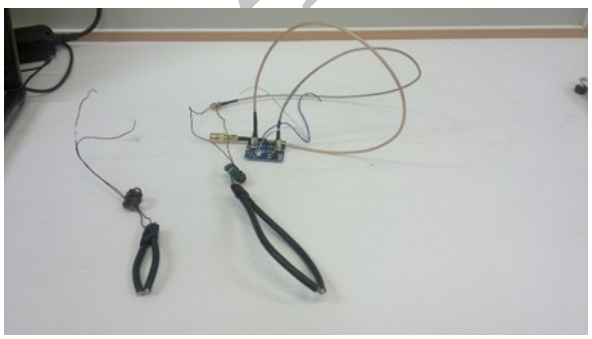
شکل ۷. پیکربندی آنتن متقارن حلقوی

مشخصات آنتن ساخته‌شده در جدول ۱ آمده است.

جدول ۱. مشخصات آنتن ساخته‌شده

قطر حلقه	۷cm
قطر کابل کواکسیال	۴٫۵mm
شکاف شیلد	۲mm
نوع بالون	بالون با هسته فریتی و ۷ دور سیم

در شکل ۸ نمای کلی پروب مغناطیسی ساخته‌شده نشان داده شده است.

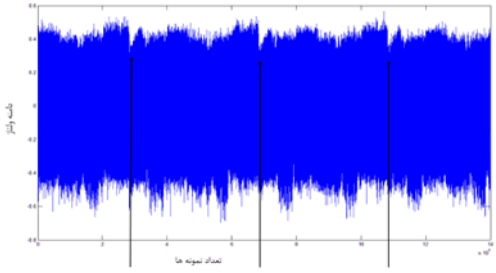


شکل ۸. نمایی از دو قسمت تقویت کننده و آنتن پروب مغناطیسی ساخته‌شده

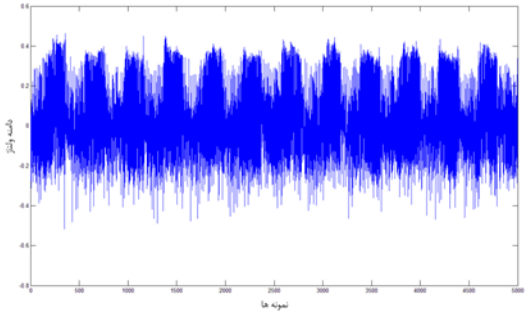
۵. نتایج عملی و تحلیل

در این بخش، نتایج حاصل از اعمال حمله روی پیاده‌سازی ارائه می‌شود. برای اجرای حمله، ۱۰۰ متن اصلی برای رمزنگاری به سخت‌افزار رمز کننده ارسال می‌شود. برای تابع انتخاب تشعشات الکترومغناطیس و جداسازی مشاهدات از یکدیگر، از وزن همینگ استفاده شده است و داده‌ها به دو دسته با وزن همینگ کمتر و بیشتر یا مساوی از چهار تقسیم شده‌اند. همچنین داده‌های خروجی S-Box دور اول به عنوان داده میانی انتخاب شده‌اند.

پس از نمونه‌برداری، سیگنال تشعشات الکترومغناطیس میکروکنترلر در هنگام پردازش چهار دور الگوریتم رمزنگاری AES مانند شکل ۹ می‌باشد. همان‌طور که مشخص است، نمودار دارای بخش‌های تکراری است که بیانگر دورهای الگوریتم است.



شکل۹. نمودار تشعشات الکترومغناطیس پردازش چهار دور الگوریتم AES

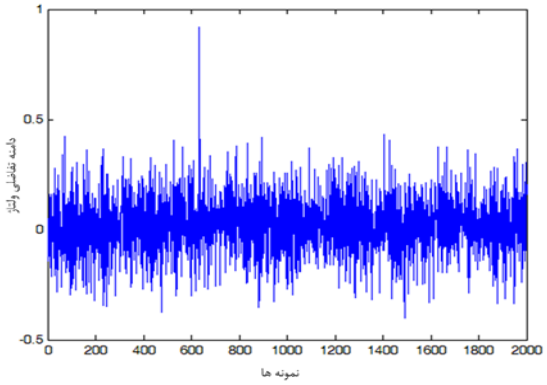


شکل ۱۰. سیگنال الکترومغناطیسی حاصل از عملیات جانشینی بایت

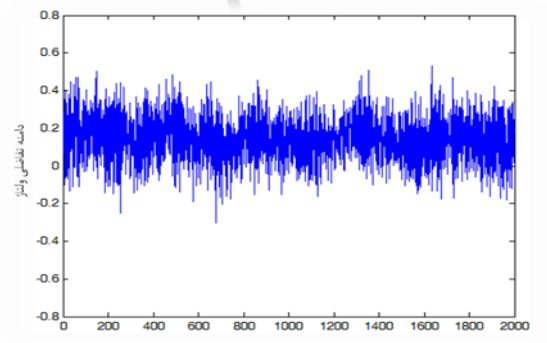
در شکل ۱۰ سیگنال الکترومغناطیس حاصل از عملیات جانشینی بایت در دور اول الگوریتم نشان داده شده است.

در شکل‌های ۱۱ تا ۱۳ به ترتیب نمودارهای تفاضلی حاصل برای یک حدس صحیح و دو حدس غیر صحیح برای بایت اول کلید آمده است. همان‌گونه که در شکل‌ها مشخص است، در حالتی که فرض کلید 0x2b است، بیشترین جهش در نمودار حدود $۰/۹ \times ۱۰^{-۳}$ است و در فرض‌های دیگر، بیشترین اندازه جهش نمودار به ترتیب $۰/۵ \times ۱۰^{-۳}$ و $۰/۵۱ \times ۱۰^{-۳}$ است. این به‌دلیل درست بودن حدس اول و اشتباه بودن دو فرض بعد است. نموداری که دارای بزرگ‌ترین قله متمرکز باشد نشانگر بیشترین همبستگی با بایت متناظر از کلید واقعی است و این حدس را به‌عنوان حدس صحیح کلید در نظر می‌گیرند. این نمودارها دلالت بر این دارد که حدس ما از کلید با آنچه که واقعا در سخت‌افزار اتفاق افتاده همبستگی زیادی دارد.

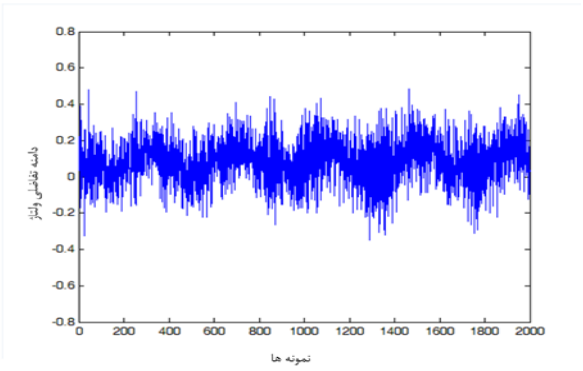
به‌منظور مقایسه‌ای بین تمام حدس‌های یک بایت از کلید نمودار دیگری رسم می‌کنیم. اگر بخواهیم حداکثر دامنه تشعشات الکترومغناطیس را به‌ازای تمام حدس‌ها (۲۵۶ حالت) از بایت اول کلید در دور اول، به‌طور همزمان نمایش دهیم شکل ۱۴ را خواهیم داشت. در واقع با توجه به شکل، به ازای عدد ۴۳ که نمایش دسیمال عدد 2B می‌باشد، بیشترین مقدار تشعشات الکترومغناطیس ملاحظه می‌شود که نشان‌دهنده حدس صحیح از بایت متناظر در کلید دور اول است. همانطور که در شکل ملاحظه می‌شود، قله توان کلید صحیح و دیگر کلیدها دارای اختلاف قابل قبولی است.



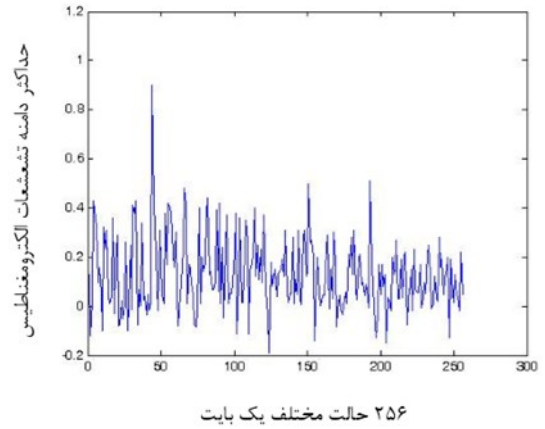
شکل۱۱. نمودار تفاضل مشاهدات تشعشات الکترومغناطیس با یک حدس صحیح از زیرکلید دور اول الگوریتم



شکل۱۲. نمودار تفاضل مشاهدات تشعشات الکترومغناطیس با یک حدس اشتباه از زیرکلید دور اول الگوریتم



شکل ۱۳. نمودار تفاضل مشاهدات تشعشعات الکترومغناطیس با یک



شکل ۱۴. نمودار حداکثر دامنه تشعشعات الکترومغناطیس به ازای همه حدس‌ها از بایت کلید

۶. نتیجه

حملات کانال جانبی از جمله مهم‌ترین تهدیدات برای امنیت سیستم‌های رمزنگاری معاصر هستند. اهمیت این حملات به‌گونه‌ای بوده است که به‌محض مطرح شدن، مورد توجه ویژه صاحب‌نظران این رشته، کارخانه‌های سازنده و مؤسسات مختلف استفاده کننده از این سیستم‌ها قرار گرفته‌اند. الگوریتم‌هایی نظیر الگوریتم رمزنگاری استاندارد یا AES از نظر ریاضی به‌اندازه کافی در مقابل حملات مقاوم هستند، اما این مقاله نشان داد هنگامی‌که بر روی ماژول‌های سخت‌افزاری مانند میکروکنترولر پیاده‌سازی می‌شوند در مقابل تحلیل الکترومغناطیس کاملا آسیب‌پذیرند.

در این مقاله به بررسی امنیت میکروکنترلر AT89C51AC2 که یکی از تراشه های پرکاربرد در بازار است در برابر حمله تحلیل الکترومغناطیس تفاضلی پرداخته شد و ضمن معرفی تجهیزات سخت‌افزاری و نرم‌افزاری لازم و روش کنترل آنها، نحوه اعمال حمله تشریح شد. با استفاده از تجهیزات معرفی‌شده، از آنجاکه مرحله نمونه‌برداری با استفاده از کارت نمونه‌بردار با دقت صورت گرفت، همزمانی بین داده‌ها حفظ شد و اثرهای تشعشعات الکترومغناطیس متناظر با هر ورودی به‌درستی ذخیره شدند. مرحله تحلیل داده‌ها بدون دردسر و با سرعت اجرا شد و بعد از حدود ده ثانیه شانزده بایت کلید رمزنگاری کشف گردید.

یکی از قسمت‌های بحرانی این حملات، ابزار اندازه‌گیری تشعشعات است که طراحی و ساخت پروب مغناطیسی استفاده‌شده در این کار به‌طور مفصل بررسی شد. محتمل است در آینده حملاتی که ترکیبی از چند منبع اطلاعات کانال جانبی مانند ترکیب حمله تحلیل الکترومغناطیس و القاء خطا هستند همراه با روش‌های قدرتمندتر آماری و مشاهده همزمان چند عملیات بتوانند به‌طور جدی‌تر سخت‌افزارهای رمزنگاری را مورد تهدید قرار دهند. از این‌رو برای مقابله با این تهدید امنیتی بایستی بسیار آماده و هشیار بود.

۷. مراجع

[1] P. C. Kocher: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and other Systems, Advances in Cryptology CRYPTO 1996, (N. Koblitz, ed.), Lecture Notes in Computer Science, vol. 1109, pp. 104-113, Springer-Verlag, 1996.

[2] Information Technology Research and Standardization-Center (INSTAC) Japanese Standardization Association (JSA). Tamper-resistance Standardization Research Committee. The Activity Report 2003-2006. http://www.jsa.or.jp/stdz/instac/committe/index.htm.

[3] Paul C. Kocher, J. Jaffe, B. Jun, "Differential Power Analysis" CRYPTO'99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, LNCS1666, pages 388-397, Springer, 1999.

[4] F. X. Standaert, L. vanOldeneel, D. Samyde, and J. J. Quisquater, "Power Analysis of FPGAs, How Practical is the Attack?" Proc. the International Conference on Field Programmable Logic and Application, pp. 701-711, 2003.

[5] F.-X. Standaert,S.B. Ors, B. Preneel, "Power Analysis of an FPGA Implementation of Rijndael is Pipelining a DPA Countermeasure?" in the proceding of CHES 2004, Lecture Notes in Computer Science, vol 3156, pp 30-44, Boston, USA, August 2004.

[6] F.-X. Standaert,S.B. Ors, J.-J.Quisquater, "Power Analysis Attack against FPGA Implementation of the DES", in the proceding of FPL 2004, Lecture Notes in Computer Science, vol 3203, pp 84-94, Antwerp, Belgium, September 2004.

[7] International Electrotechnical Commission. IEC 61967: Integrated Circuits - Measurement of Electromagnetic Emissions, 150 kHz to 1 GHz. http://www.iec.ch, 2003.

[8] Karine Gandolfi, Christophe Mourtel and Francis Olivier, "Elecromagnetic Analysis: Concrete Results", Lecture Notes In Computer Science, vol. 2162, Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems, 2001,pp. 51 - 261.

[9] H.Yousefi and M.Gardeshi,"introduction a successful SPA to AES implementation on PIC microcontroller", international journal of signal and data processing,2012,vol1,pp 49-58 (in Persian)

[10] ADVANCED ENCRYPTION STANDARD (AES), Federal Information Processing Standards Publication 197, November 26, 2001.

[11] J.-J. Quisquater and D. Samyde. Electromagnetic analysis (EMA) Measures and countermeasures for smart cards", In Proceedings of e-Smart 2001, Lectures Notes in Computer Science (LNCS), vol. 2140, pages 200–210, Springer, 2001.

[12] Massoud Masoumi, "Differential Power Analysis, A Serious Threat to FPGA Security", Int. J. Internet Tech. and Secured Transactions, Vol. 4, No.1, 2012.

[13] Massoud Masoumi and Soheyl Mohammadi, "A New and Efficient Approach to protect AES against Differential Power Analysis", IEEE WorldCIS 2011, London, UK, Feb. 2011.

[14] http://www.alldatasheet.com/datasheet-pdf/pdf/175350/ATMEL/AT89C51AC2.html.

[15] X. Yingqing, Luo, J. Ye H. "A standard shielded loop antenna with load resistor" Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, 2009 3rd IEEE International Symposium , 27-29 Oct. 2009, pp 405 – 407.

[16] S.M.Nargesi, " design and create loop antenna with display system to measurement magnetic field", MSc thesis, Amirkabir University of technology, 2011(in Persian)