پیاده‌سازی و آشکارسازی تروجان های سخت‌افزاری با استفاده از تحلیل کانال جانبی تشعشعات الکترومغناطیسی

سبحان پستادست [1,*]، عبدالرسول میرقدری

۱- کارشناسی ارشد برق مخابرات امن و رمزنگاری، دانشگاه جامع امام حسین (ع)

۲- دانشیار دانشکده فناوری اطلاعات و ارتباطات، دانشگاه جامع امام حسین (ع)

چکیده

یکی از نقاط ضعف امنیتی تراشه‌ها، نفوذ مهاجم به دستگاه در فرآیند طراحی تراشه یا فرآیند ساخت آن است و این باعث نگرانی‌های جدی برای دستگاه‌های نظامی، اقتصادی و حتی خانگی شده است. همان‌گونه که در طراحی و کاربرد نرم‌افزارهای تحت شبکه‌های کامپیوتری امکان نفوذ بدافزارها از قبیل تروجان‌های نرم‌افزاری وجود دارد، از دید سخت‌افزاری نیز می‌توان هسته‌های سخت‌افزاری را در حین فرآیند ساخت در درون تراشه‌ها قرار داد که به‌صورت یک تروجان در حین کارکرد تراشه، نقش بازی کند. تروجان سخت‌افزاری یک مدار اضافی مخرب است که به همراه مدار اصلی و باهدف خاصی پیاده‌سازی می‌شود و می‌تواند عملکرد سخت‌افزار اصلی را تحت تأثیر قرار دهد. در این مقاله در خصوص مفاهیم تروجان‌ها، خصوصیات آن‌ها، نحوه دسته‌بندی و برخی روش‌های آشکارسازی و پیاده‌سازی تروجان‌ها بحث شد. سپس با استفاده از نرم‌افزار ISE Design یک شمارنده ۱۶ بیتی طراحی شد. ازآنجایی‌که الگوریتم رمزنگاری استفاده‌شده در این مقاله، الگوریتم AES می‌باشد این الگوریتم با شمارنده ۱۶ بیتی همگام‌سازی شده است؛ یعنی به‌محض اینکه الگوریتم شروع به کار کند شمارنده هم شروع به شمارش می‌کند. درنهایت سطح تراشه ناحیه‌بندی شد و تشعشعات الکترومغناطیس در این ناحیه‌ها نمونه‌گیری شد و داده‌ها با استفاده از روش آزمون آماری T تحلیل شد. در این مقاله با مقایسه مقدار آزمون آماری T ناحیه‌ها، تروجان سخت‌افزاری آشکارسازی و محل فیزیکی آن در تراشه کشف شد. در این مقاله برای اولین بار در داخل کشور به‌صورت عملی، تروجان سخت‌افزاری آشکارسازی و محل قرارگیری فیزیکی تروجان سخت‌افزاری کشف شد و در نهایت با دو روش تحلیل همبستگی و تفاضلی توان مقایسه شد و در نتیجه مشخص شد که تحلیل تشعشعات الکترومغناطیس از دقت بالایی برخوردار است.

کلمات کلیدی: تروجان سخت‌افزاری، آشکارسازی تروجان، روش آماریT-test، تحلیل کانال جانبی، تشعشعات الکترومغناطیس

* **Corresponding author:** مهندس برق الکترونیک و کارشناس ارشد مخابرات گرایش امنیت و رمزنگاری
Email: S.pastadast@gmail.com

۱. مقدمه

با توجه به گسترش روزافزون صنایع نیمه‌هادی و فرآیندهای طراحی و تولید تراشه‌ها، مدارهای مجتمع در معرض خطر آسیب‌پذیری از جهت عملکردهای عمدی و تغییرات مخرب در مدار هستند. تروجان‌های سخت‌افزاری[1] باعث تغییرات مخرب در یک مدار مجتمع می‌شوند که با هوشیاری دشمن می‌تواند باعث استخراج اطلاعات حساس نظامی و دولتی شود همچنین می‌تواند باعث از کار افتادن یک تراشه شود. وجود بدافزارها باعث شده تا دولت‌ها و صنعت یک کشور توجه ویژه‌ای به امنیت سخت‌افزار از نظر تروجان‌ها نمایند. با پیشرفت صنعت نیمه‌هادی‌ها، مدارهای دستکاری شده مانند تروجان‌های سخت‌افزاری می‌توانند با پیاده‌سازی مخفیانه در تراشه یک مدار مجتمع امنیت سخت‌افزار را مورد تهدید قرار دهند. حمله با استفاده از تروجان بر روی یک تراشه دارای عواقب جدی بوده به‌نحوی‌که می‌تواند بر روی عملکرد خیلی از دستگاه‌های الکترونیکی حساس تأثیر منفی بگذارد. ممکن است برای مدت طولانی متوجه این سخت‌افزار مخرب نشوند و شاید مهم‌تر از آن، اثرات مخرب و شکستن امنیت ناشی از این حمله تقریباً غیرقابل بازسازی است زیرا در تراشه‌ها امکان به‌روزرسانی نرم‌افزاری وجود ندارد و تروجان به‌صورت سخت‌افزاری پیاده‌سازی شده است. طی سال‌های اخیر تحقیقات زیادی در خصوص تروجان‌های سخت‌افزاری انجام شده و اقدامات متقابل برای این حمله منتشر شده است. در اولین بررسی روی مدارهای مخرب، وانگ[2] و همکارانش به طبقه‌بندی انواع تروجان‌ها پرداختند [۱]. تهرانی پور و همکارانش به طبقه‌بندی انواع حملات تروجان‌های سخت‌افزاری پرداخته‌اند. این طبقه‌بندی شامل سه موضوع طراحی و طبقه‌بندی تروجان، روش‌های کشف و شناسایی تروجان، طراحی برای اطمینان از سخت‌افزار است [۲] و [۳]. در ادامه ساختار مقاله بدین شرح است که در بخش ۲ کارهای مرتبط با تروجان‌های سخت‌افزاری بیان می‌شود. در ادامه در بخش ۳ روش‌های کشف تروجان سخت‌افزاری معرفی گردید. در بخش ۴ انواع کانال جانبی معرفی گردید و در ادامه در بخش ۵ به پیاده‌سازی تروجان سخت‌افزاری پرداخته شد که یک شمارنده ۱۶بیتی می‌باشد که هم‌زمان با الگوریتم رمزنگاری AES شروع به کار می‌کند.در ادامه در بخش ۶ به بررسی آشکارسازی تروجان با استفاده از تشعشعات الکترومغناطیس می‌پردازد که در این بخش روش کشف تروجان بیان‌شده است. در بخش های بعدی با جزئیات بیشتری به تروجان سخت‌افزاری پرداخته شده است. در بخش اخر نتایج حاصل از نمونه‌گیری از تشعشعات نشان داده‌شده است و درنهایت منجر به کشف تروجان سخت‌افزاری شده است و در انتها دقت و سرعت آن با روش‌های هبستگی و تفاضلی توان مقایسه و نتیجه‌گیری شده است.

[1] Hardware Trojan

۲. کارهای مرتبط با تروجان‌های سخت‌افزاری

در سال‌های اخیر سخت‌افزار امن و قابل اعتماد از موضوعات راهبردی و بسیار مهم تحقیقاتی به شمار می‌آید. در سال ۲۰۰۷ آگراوال و همکاران در همایش امنیت و محرمانگی انجمن IEEE در خصوص کشف تروجان با استفاده از اثرانگشت در مدار مجتمع مقاله‌ای ارائه دادند [۴]. در زمینه دسته‌بندی تروجان‌های سخت‌افزاری، وانگ و همکارانش در سال ۲۰۰۸ یک تقسیم‌بندی کلی با نگاه جامع بر اساس مشخصات فیزیکی، نوع تحریک مدار و عملکرد مدار تروجان ارائه کردند [۳]. بعد از آن در طی سال‌های ۲۰۰۸ تا ۲۰۱۰ با نگاه کلی به نوع عملکرد مدار اصلی تروجان و اثر آن‌ها در مدار، تقسیم‌بندی‌های مختلفی ارائه شد. در سال ۲۰۱۰ چاکرابورتی و همکاران انواع تهدیدات تروجان‌های سخت‌افزاری و راه‌حل‌های مقابله با آن‌ها را ارائه دادند و درنهایت این تقسیم‌بندی را با نگاهی جدیدتر و کامل‌تر وسعت بخشیده و یک طرح دقیق از مجموعه تروجان‌های سخت‌افزاری ارائه کردند [۵]. در سال ۲۰۱۶ مقاله [۶] آشکارسازی تروجان سخت‌افزاری با استفاده از تحلیل توان پرداخته است که درنهایت منجر به فاش شدن کلید شده است. یک روش عملی برای آشکارسازی تروجان سخت‌افزاری با استفاده از تشعشعات الکترومغناطیس در مقاله [۷] ارائه‌شده است و همچنین رویکردهایی برای افزایش حساسیت تشخیص تروجان سخت‌افزاری با استفاده از کانال جانبی در [۸] بررسی‌شده است.در [۸] یک روش کلی برای مدل کردن نویز برای کشف تروجان ارائه کرده است. در [۹] از یک تقسیم‌بندی برای سطح زمانی به‌منظور از عهده برآمدن مشکل فرآیند نویز ارائه‌شده است این روش امضای دیجیتال یک تراشه را در دو زمان مختلف برای حذف کردن کامل تأثیر فرآیند نویز ترکیب می‌کند. نویسنده مقاله بر این باور است که فن وی بیشترین آشکارسازی تروجان در اندازه‌های مختلف را فراهم می‌سازد و تأکید دارد که این روش، نیازی به تراشه طلایی ندارد.

تمام مقالاتی که اشاره شد دارای اشکالاتی می‌باشد که در مقاله [۱۰] به‌طور خلاصه بیان‌شده است. در این مقاله در مقایسه با روش‌هایی که تا به حال مورد بررسی قرارگرفته است عملی می‌باشد و بدون در نظر گرفتن فرآیند نویز به کشف تروجان سخت‌افزاری می‌پردازد. همچنین در این مقاله با روش‌های آماری به کشف تروجان می‌پردازد که قادر است با درصد بالایی، تروجان سخت‌افزاری را آشکارسازی کند.

۳. روش‌های کشف تروجان‌های سخت‌افزاری

با توجه به حساسیت وجود تروجان‌های سخت‌افزاری در قطعات الکترونیکی، تنوع روش‌های پیاده‌سازی باعث پیچیدگی هر چه بیشتر نحوه آشکارسازی آن‌ها در مدارات و تراشه‌های الکترونیکی می‌شود. یکی از مسائل مهم و اساسی حوزه امنیت سخت‌افزار، افزایش میزان اعتماد به سخت‌افزار و آشکارسازی تروجان‌های احتمالی موجود در تراشه‌ها و سخت‌افزارهای امنیتی می‌باشد. طراحی و تولید مدارات مجتمع امن و قابل اعتماد، ضرورت اساسی برای حوزه‌های حساس سلامت، دفاع و ارتباطات ملی است. هدف اصلی آشکارسازی و کشف تروجان سخت‌افزاری تعبیه شده درون یک تراشه یا مدار مجتمع توسط تجزیه‌وتحلیل کانال جانبی می‌باشد. تا به امروز روش‌های بسیاری برای مقابله با تروجان‌ها ارائه‌شده که به دودسته کلی مخرب و غیر مخرب تقسیم شده‌اند.

در کل روش‌های تشخیص تروجان با توجه به ساختار آن‌ها به چهار دسته به شرح ذیل تقسیم شده‌اند [۱۱].

۱- بازرسی فیزیکی

۲- بررسی عملکرد مدار

۳- نیمکت آزمون تعبیه شده در تراشه

۴- تجزیه‌وتحلیل کانال جانبی

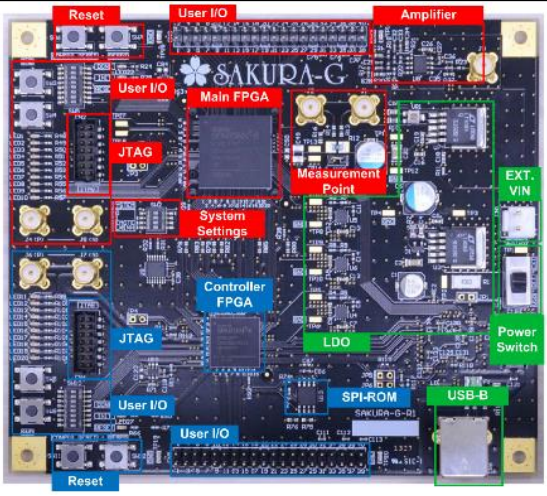
۴. تحلیل کانال جانبی

هر مدار الکتریکی از خود سیگنالی تولید می‌کند که با تجزیه‌وتحلیل این سیگنال می‌توان عملکرد و اطلاعات مدار را پردازش و بررسی نمود. روش‌های تحلیل کانال جانبی بر این واقعیت استوارند که تعبیه المان‌های مخرب در مدارهای مجتمع روی برخی خصوصیات ازجمله تأخیر مسیر، تشعشعات الکترومغناطیسی به‌واسطه کلید زنی اثر می‌گذارد. مزیت مهم استفاده از کانال جانبی برای کشف تروجان، عدم نیاز به فعال‌سازی کامل تروجان می‌باشد. همچنین این روش برای کشف تروجان‌هایی که تنها برای نشت اطلاعات سامانه به کار رفته‌اند نیز مناسب است. یکی از تحلیل‌های کانال جانبی تحلیل تشعشعات الکترومغناطیس است که با استفاده از آن و روش‌های آماری می‌توان وجود تروجان سخت‌افزاری را تشخیص داد.

۵. پیاده‌سازی تروجان سخت‌افزاری

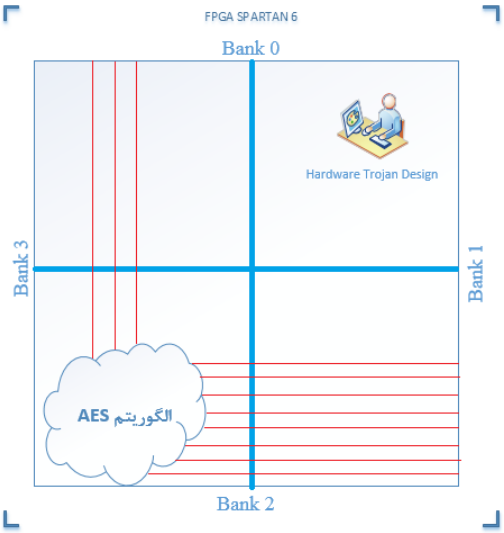
برد SAKURA-G برای تحقیق و پژوهش روی امنیت سخت‌افزار مانند حملات کانال جانبی[1]، حملات تزریق خطا[2]، توابع فیزیکی غیرقابل کپی کردن[3] و پیکربندی پویا[4] طراحی گردیده است. این برد شامل دو FPGA سری SPARTAN-6 از شرکت Xilinx می‌باشد که یکی برای کنترل و دیگری برای مدار امنیتی اصلی طراحی گردیده است. این برد با نویز فوق‌العاده پایین طراحی‌شده است در این مقاله از این برد استاندارد برای تحلیل تشعشعات الکترومغناطیس استفاده شده است که در شکل ۱ نمای کلی از این برد قابل مشاهده است.

[1] Side-Channel Attacks (SCA)
[2] Fault Injection Attacks (FIA)
[3] Physical Unclonable Functions (PUF)
[4] Dynamic Reconfiguration



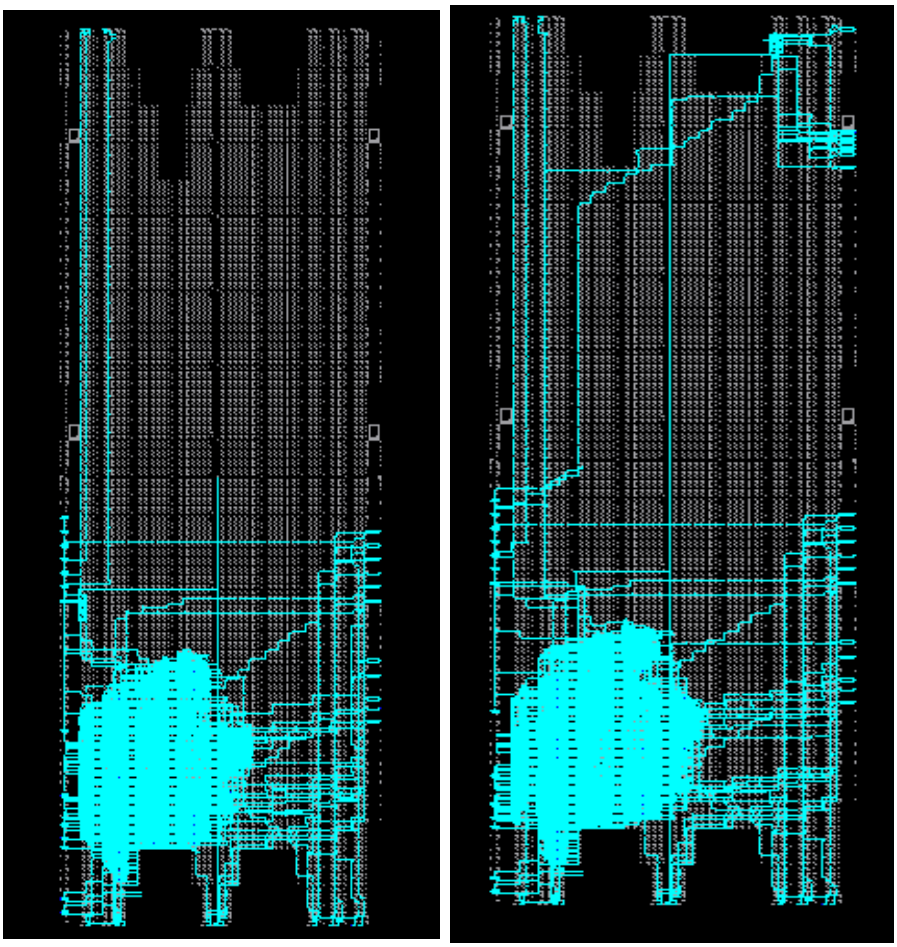
شکل ۱- نمای کلی از بردSAKURA-G [۱۲]

برای اطلاعات بیشتر در خصوص برد ساکورا به مرجع [۱۲] مراجعه شود. برای پیاده‌سازی آزمایشگاهی ابتدا با استفاده از نرم‌افزار Xilinx ISE 14.4 ابتدا یک شمارنده ۱۶ بیتی به‌عنوان یک تروجان سخت‌افزاری طراحی کردیم که به صورت فعال می‌باشد. سپس این شمارنده را با الگوریتم AES همگام‌سازی کرده تا هم‌زمان با الگوریتم AES شروع به کار کند. سپس با استفاده از FPGA Editor Tools نرم‌افزار Xilinx ISE اجزای تروجان سخت‌افزاری شمارنده ۱۶ بیتی را به مکان‌های استفاده نشده در تراشه Spartan 6 انتقال دادیم. ابتدا الگوریتم AES را به قسمت پایین و چپ یعنی بانک ۳ برده و تروجان سخت‌افزاری را به قسمت بلااستفاده در بانک ۱ برای تحلیل نتایج حاصل از تشعشعات الکترومغناطیس برده شد که در شکل۲ پیاده‌سازی تروجان سخت‌افزاری را به‌صورت کلی نشان خواهد داد. در این مقاله از الگوریتم رمزنگاری AES برای رمزگذاری برد ساکورا استفاده شده است تا با تحلیل تشعشعات موجود در تراشه، پی به وجود تروجان نهفته در آن برده شود.



شکل ۲- نمایی کلی از پیاده‌سازی تروجان سخت‌افزاری

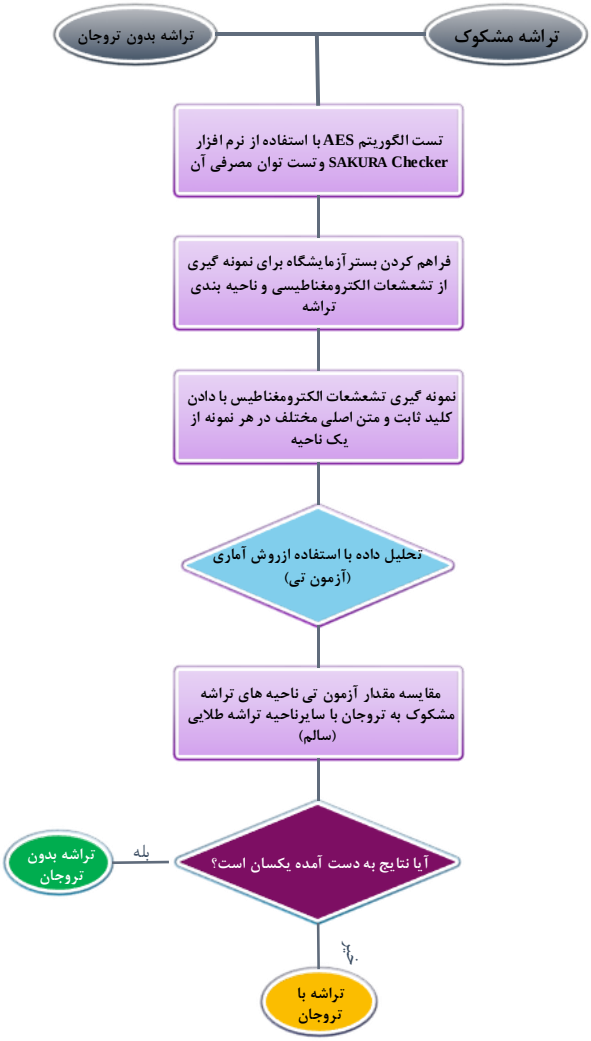
سپس با استفاده از نرم‌افزار FPGA Editor تروجان سخت‌افزاری را با توجه به شکل ۲ در قسمت راست و بالای تراشه قرار دادیم. برای آشکارسازی تروجان سخت‌افزاری نیاز به تراشه طلایی داریم تا با استفاده از کانال جانبی و تحلیل تشعشعات الکترومغناطیس، تراشه مشکوک به تروجان را نسبت به تراشه طلایی بررسی کنیم که در بخش‌های بعدی روش آشکارسازی تروجان را تشریح خواهیم کرد. در این مقاله دو تراشه، حاوی تروجان و بدون تروجان را موردبررسی و مقایسه قرار دادیم.



شکل۳- الف) تراشه با تروجان ب) تراشه بدون تروجان

۶. بررسی روش آشکارسازی تروجان سخت‌افزاری تشعشعات الکترومغناطیسی

در این بخش مراحل کار در تشخیص تروجان سخت‌افزاری و روش نظری کشف تروجان ارائه می‌شود.



شکل۴- بلوک دیاگرام مراحل کار آشکارسازی تروجان سخت‌افزاری

۶-۱. روش تئوری کشف تروجان

در شکل ۴ مراحل آشکارسازی تروجان بیان‌شده است همان‌طور که در بلوک دیاگرام مشاهده می‌شود در این مقاله برای آنالیز داده های الکترومغناطیس از روش آماری آزمون تی(T-test) استفاده شده است.

روش آماری T-test از نوع Welch's two-tailed که برای مقایسه دو مجموعه داده از لحاظ تفکیک‌پذیری و تفکیک‌ناپذیری به کار می‌رود که طبق رابطه زیر محاسبه می‌شود و درنهایت در محیط متلب برای به دست آوردن T-test ،شبیه‌سازی و استفاده شده است.

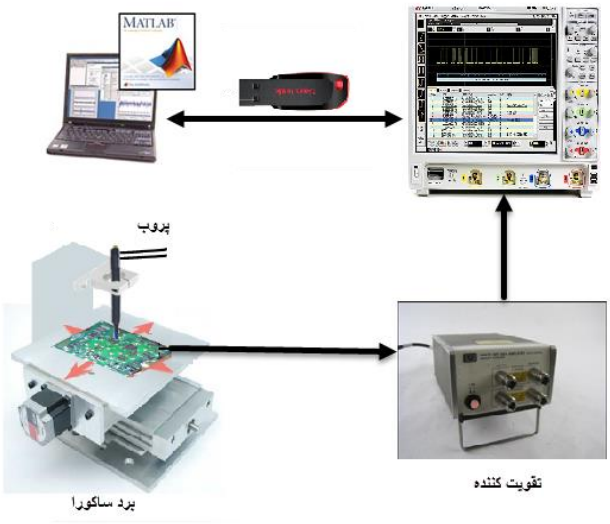
$$t = \frac{\mu_0 - \mu_1}{\sqrt{\frac{\sigma_0^2}{N_0} + \frac{\sigma_1^2}{N_1}}}$$

مقدار μ_0 و μ_1 میانگین نمونه‌ها و σ_0^2 و σ_1^2 واریانس مجموعه‌ها و N_0 و N_1 عدد کاردینالیتی مجموعه داده‌ها می‌باشد. همان‌طور که در بخش ۲ بیان شد دو تراشه در اختیار داریم. پس دو مجموعه داده خواهیم داشت. ما هر تراشه را طبق شکل ۲ در صفحه ۶ به چهار قسمت تقسیم کرده درنتیجه چهار ناحیه خواهیم داشت. در در دو تراشه، مقدار آزمون تی ناحیه‌های متناظر دو تراشه به دست آورده می‌شود که در شکل ۵ مشخص شده است.

شکل ۵- ناحیه‌های موردبررسی برای به دست آوردن مقدار T-test

۲-۶. تنظیمات آزمایش

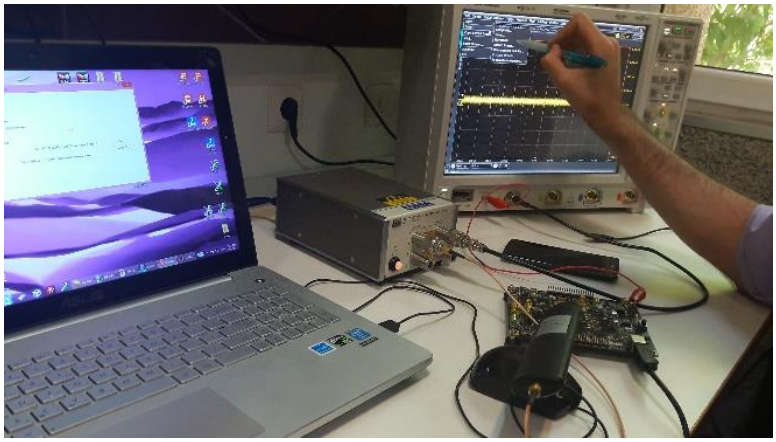
برای نمونه‌گیری داده‌های مصرف توان و تشعشعات الکترومغناطیس از دو اسیلوسکوپ دیجیتال Agilent مدل MSO9064 و اسیلوسکوپ Rohde & Schwarz مدل Handheld ۸FSH استفاده شده است که اسیلوسکوپ Agilent با نرخ نمونه‌برداری ۱۰ گیگاهرتز و با فرکانس کاری ۶۰۰ مگاهرتز است که دارای ۴ کانال برای نمونه‌گیری می‌باشد. اسیلوسکوپ Rohde & Schwarz برای مشاهده طیف الکترومغناطیس بکار رفته که بیشترین توان ورودی آن ۱۰۰ میلی ولت و ۲۰ دسی‌بل می‌باشد. برای نمونه‌گیری از تشعشعات الکترومغناطیس از پروب مخصوص Rohde & Scwarz از نوع Near-Field استفاده شده است که یک پروب ۵۰ مگا اهم می‌باشد. نکته‌ی حائز اهمیت این است که بایستی اسیلوسکوپ هم، برای نمونه‌گیری روی ۵۰ مگا اهم تنظیم شود تا از طریق پروب Rohde & Scwarz HZ-14 برای تحلیل تشعشعات الکترومغناطیسی، نمونه‌ها درست ذخیره شوند. این پروب با استفاده از یک تقویت‌کننده HP8447F Amplifier سیگنال تشعشعات الکترومغناطیس آن را تقویت کرده سپس آن را روی اسیلوسکوپ نمایش می‌دهد. سپس برای تحلیل نتایج با استفاده از روش‌های آماری به کامپیوتر انتقال داده می‌شود. شکل زیر بستر آزمایش برای نمونه‌گیری را نشان می‌دهد.



شکل ۶- نمای کلی از بستر آزمایش

شکل‌های ۷ و ۸ به ترتیب بستر آزمایش با اسیلوسکوپ‌های Agilent و Rohde & Scwarz را نشان می‌دهند.

شکل ۷- بستر آزمایش با استفاده از اسیلوسکوپ دستی Rohde & Schwarz

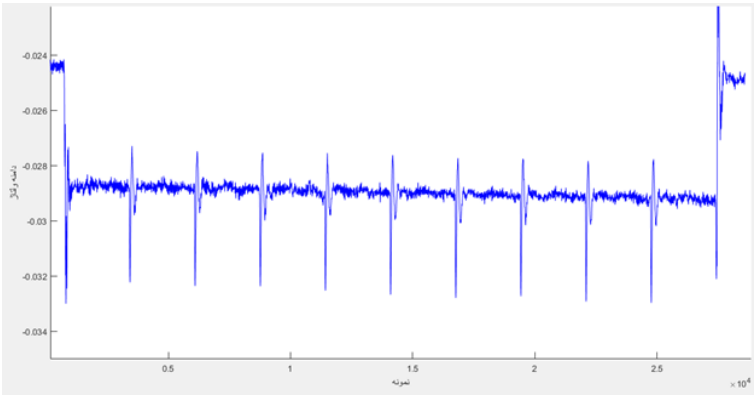


شکل۸- بستر آزمایش با استفاده از اسیلوسکوپ Agilent

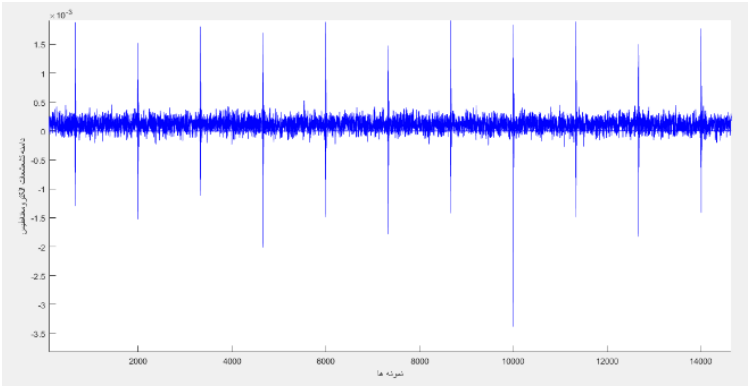
در شکل ۲ مشاهده می‌شود که تروجان در ناحیه بالا سمت راست تراشه جاسازی شده است و بایستی آن ناحیه را باحالتی که تروجان وجود ندارد مقایسه کرد. نکته حائز اهمیت این است که برای انجام T-test نیاز به مقدار نمونه کافی از تشعشعات می‌باشد [۱۳] و همچنین دمای محیط برای نمونه‌گیری از هر دو تراشه بایستی یکسان باشد. در این مقاله در هر ناحیه اعم از تراشه باوجود تروجان و تراشه بدون تروجان در هر ناحیه ۱۰۰ نمونه درمجموع ۸۰۰ نمونه تشعشعات الکترومغناطیسی در محیط با نویز خیلی کم و شرایط دمایی یکسان را توسط اسیلوسکوپ با پسوند CSV. ذخیره کرده سپس برای انجام شبیه‌سازی و T-test به کامپیوتر انتقال داده شد.

۳-۶. سیگنال‌های توان مصرفی و تشعشعات الکترومغناطیس در حین اجرای الگوریتم AES

همان‌طور که گفته شد الگوریتم رمزنگاری پیاده‌سازی شده بر روی تراشه Spartan 6 الگوریتم AES می‌باشد که از ۱۰ دور تشکیل شده است که برای اطلاعات بیشتر از مراحل رمزنگاری به منبع [۱۴] ارجاع داده می‌شود. شکل ۹ توان مصرفی تراشه در حین اجرای الگوریتم و شکل ۱۰ تشعشعات الکترومغناطیس آن را نشان می‌دهد که در محیط نرم‌افزار متلب شبیه‌سازی شده است.



شکل۹- توان مصرفی در حین اجرای الگوریتم AES

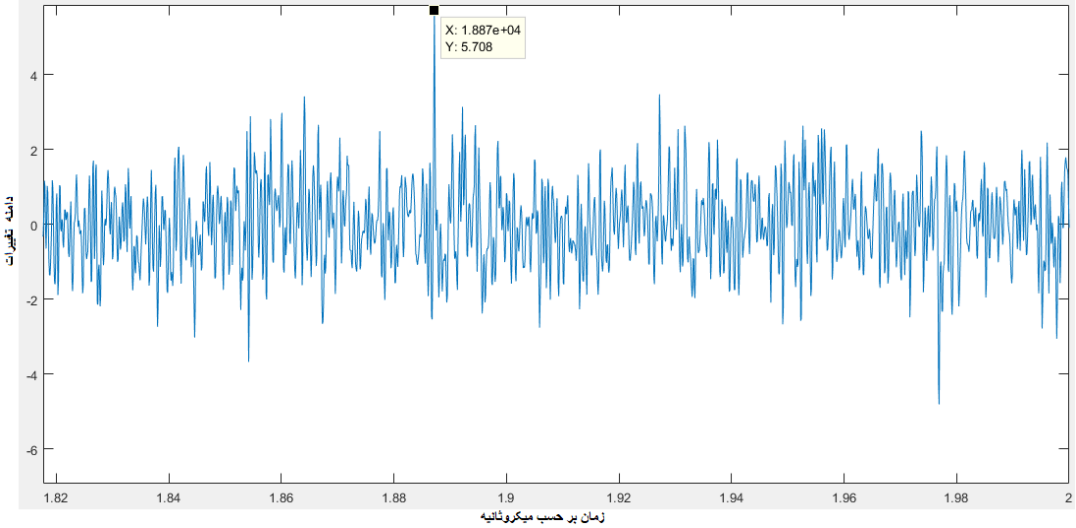


شکل۱۰- تشعشعات الکترومغناطیس حین اجرای الگوریتم AES

همان‌طور که مشاهده می‌شود شکل ۹ و ۱۰ دارای ۱۰ دور است که نشان‌دهنده درست اجراشدن الگوریتم AES توسط تراشه است.

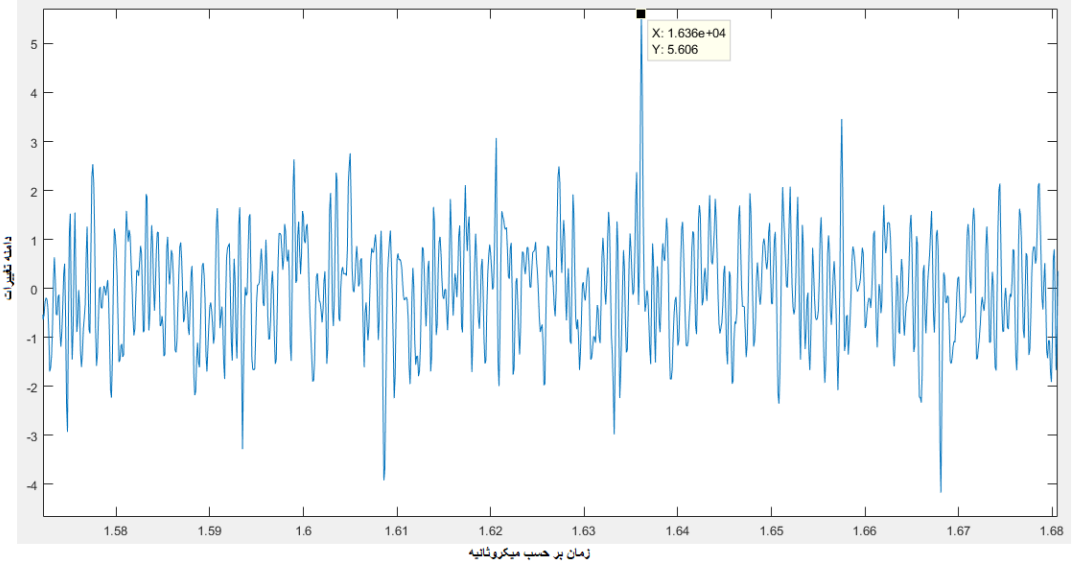
۷. نتایج عملی از کشف تروجان سخت‌افزاری

در ابتدا T-test ناحیه یک هردو تراشه که حاوی الگوریتم AES می‌باشد را به دست آوردیم و در نرم‌افزار متلب شبیه‌سازی کردیم. بیشترین مقدار پیک در شبیه‌سازی برابر مقدار T-test می‌باشد. شکل ۱۱ نشان‌دهنده T-test دو مجموعه ، در حالت تراشه بدون تروجان و تراشه باحالت تروجان در ناحیه یک می‌باشد که مقدار آزمون تی آن تقریباً برابر ۵/۷ شده است.



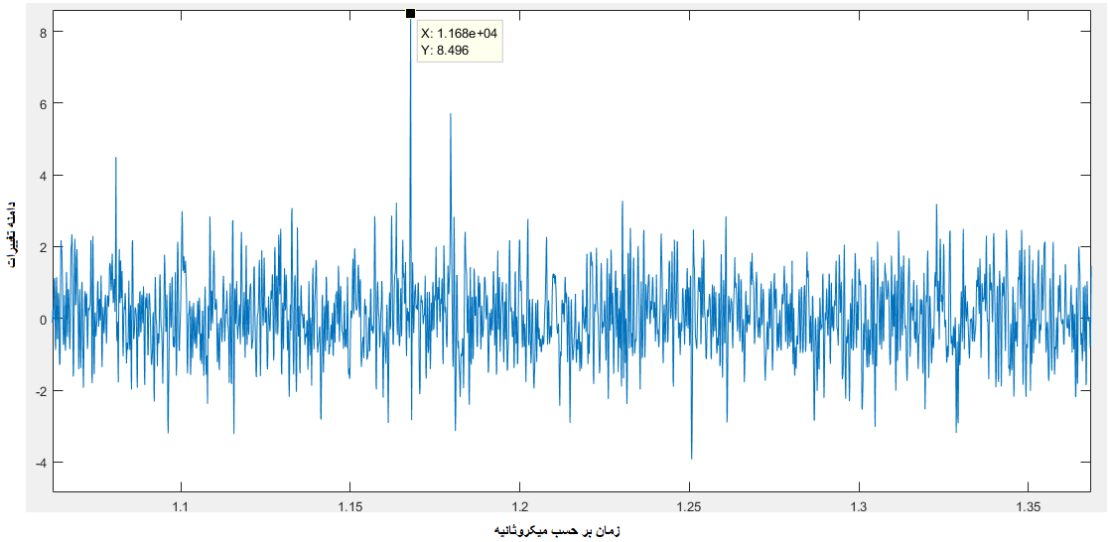
شکل ۱۱- مقدار آزمون تی در ناحیه یک هر دو تراشه

سپس با بررسی ناحیه دوم هر دو مجموعه، مقدار آمار T-test آن را به دست آوردیم که مقدار آن برابر ۵/۷ شد. در شکل ۱۲ شبیه‌سازی ناحیه دوم و چهارم در دو حالت تراشه را نشان می‌دهد.



شکل ۱۲- مقدار آزمون تی در ناحیه دوم و چهارم هر دو تراشه

سپس به ناحیه مهم تراشه یعنی ناحیه سوم پرداخته شد که تراشه حاوی یک تروجان است و هم‌زمان با الگوریتم AES شروع به کار می‌کند. همچنین در این ناحیه مقدار T-test از طریق شبیه‌سازی در محیط متلب محاسبه‌شده است که در شکل ۱۲ مقدار T-test آن با مقدار ۸/۵ مشاهده شد.



شکل ۱۳- مقدار آزمون تی در ناحیه سوم هر دو تراشه

با مقایسه شکل‌های ۱۱، ۱۲ و ۱۳ مشاهده شد که در ناحیه‌هایی که اجزای تروجان وجود ندارد یعنی در شکل‌های ۱۱ و ۱۲ مقدار T-test با هم برابر و مقدار آن ۵/۷ می‌باشند ولی در ناحیه سوم که حاوی تروجان است مقدار T-test آن برابر ۸/۵ می‌باشد که نسبت به سایر نقاط متفاوت بوده و افزایش دارد.

۸. نتیجه‌گیری

در این مقاله با بررسی و تحلیل تشعشعات الکترومغناطیس تراشه مشکوک توسط آزمون T نتیجه گرفتیم در نواحی شامل تروجان، مقدار T-test در مقایسه با سایر نقاط بیشتر است و این مشاهده حکایت از وجود یک تروجان در آن ناحیه می‌باشد. درنتیجه برای جلوگیری از ورود تروجان‌های سخت‌افزاری تعبیه‌شده در تراشه، ابتدا تراشه را قبل از به‌کارگیری در صنعت، با نمونه‌گیری تشعشعات الکترومغناطیس تراشه و انجام آزمون آماری تی T بررسی نموده که اگر تمام ناحیه‌ها دارای مقدار آزمون تی یکسان باشند لذا این تراشه فاقد تروجان سخت‌افزاری است و اگر مقدار آزمون T ناحیه‌ای با سایر نقاط متفاوت بود حاکی از وجود تروجان سخت‌افزاری در آن ناحیه می‌باشد. همچنین در این مقاله سرعت و دقت آن با دو روش همبستگی توان و تفاضلی توان [۷] مقایسه شد که در آن با استفاده از همبستگی نمونه‌ها به امنیت تراشه می‌پردازد و نشان داده شد که در روش تشعشعات الکترومغناطیس زمان زیادی برای آشکارسازی تروجان سخت‌افزاری صرف خواهد شد(به دلیل نمونه‌گیری از دو تراشه و شرایط دمایی یکسان و محیط کم نویز) ولی دقت بالایی ارائه خواهد داد درصورتی‌که در دو روش قبل، زمان صرف شده

برای آشکارسازی کم ولی دقت بالایی نخواهد داشت و نمی‌توان با درصد بالایی بیان کرد که تراشه حاوی تروجان سخت‌افزاری و یا تراشه دارای امنیت سخت‌افزاری است و عاری از هرگونه موارد مشکوک در تراشه است.

	تحلیل تشعشعات الکترومغناطیس	تحلیل همبستگی توان	تحلیل تفاضلی توان
تعداد نمونه‌ها	۱۰۰	۱۰۰	۱۰۰
زمان	دو ساعت	۵۳ ثانیه	۵ ثانیه
دقت	بالا	متوسط	کم
میزان کشف	عالی	خوب	ضعیف
نتیجه	✓	✓	×

شکل ۱۴- مقایسه تحلیل تشعشعات الکترومغناطیس و همبستگی و تفاضلی توان در ۱۰۰ نمونه

	تحلیل تشعشعات الکترومغناطیس	تحلیل همبستگی توان	تحلیل تفاضلی توان
تعداد نمونه‌ها	۲۰۰	۲۰۰	۲۰۰
زمان	چهار ساعت	۶۳ ثانیه	۱۰ ثانیه
دقت	خیلی بالا	متوسط	متوسط
میزان کشف	عالی	خیلی خوب	خوب
نتیجه	✓	✓	×

شکل ۱۵- مقایسه تحلیل تشعشعات الکترومغناطیس و همبستگی و تفاضلی توان در ۲۰۰ نمونه

۹. منابع

1. X. Wang, M. Tehranipoor & J. Plusquellic, "DetectingMalicious Inclusions in Secure Hardware: Challenges and Solutions", IEEE International Workshop on Hardware-Oriented Security and Trust", 2008, pp. 15-19.

2. M. Tehranipoor and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy", IEEE design and test of computers, 2010.

4. R. M. Rad, X. Wang, M. Tehranipoor, J. Plusquellic, "Taxonomy of Trojans and Methods of Detection for IC Trust", ICCAD, 2008.

5. D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi & B.Sunar, "Trojan Detection Using Ic Fingerprinting", IEEE Symposium on Security and Privacy, 2007.

6. M. Banga and M. S. Hsiao, "A Region Based Approach for the Identification of Hardware Trojans", Bradley Department of Electrical and Computer Engineering, Virginia Tech., 1st IEEE International Workshop on Hardware-Oriented Security and Trust (HOST'08), 2008.

۷. سبحان‌پستادست، عبدالرسول‌میرقدری، "یک‌نمونه پیاده‌سازی و آشکارسازی تروژان سخت‌افزاری با تحلیل توان"چهارمین کنفرانس بین‌المللی مهندسی برق و کامپیوتر، دانشگاه تهران، ۱۳۹۵.

8. A. Lakshminarasimhan, "Electromagnetic side- channel analysis for hardware and software watermarking," Master's thesis, University of Massachusetts Amherst, 2011.

9. D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using IC fingerprinting," in IEEE Symposium on Security and Privacy - IEEE S&P 2007. IEEE Computer Society,2007, pp. 296–310.

10. S. Narasimhan, X. Wang, D. Du, R. S. Chakraborty, and S. Bhunia, "TeSR: A robust Temporal Self-Referencing approach for Hardware Trojan detection," in Hardware-Oriented Security and Trust – HOST 2011. IEEE Computer Society, 2011, pp. 71–74.