فصلنامه علمی- پژوهشی
فناوری اطلاعات و ارتباطات ایران

سال نهم، شماره‌های ۳۱ و ۳۲، بهار و تابستان ۱۳۹۶
صص: ۳۲- ۱۳

دسته‌بندی و پیاده‌سازی تروجان‌های سخت‌افزاری و ارائه راهی نوین برای کشف آن‌ها

* صادق حاجی محسنی ** محمدعلی دوستاری *** محمدباقرغزنوی قوشچی
*گروه کامپیوتر، دانشگاه شاهد، ایران
**گروه کامپیوتر، دانشگاه شاهد، ایران
*** گروه برق الکترونیک، دانشگاه شاهد، ایران

تاریخ دریافت: ۱۳۹۵/۰۳/۲۴ تاریخ پذیرش: ۱۳۹۶/۱۱/۰۷

چکیده

در سال‌های اخیر نوعی حمله سخت‌افزاری به نام تروجان سخت‌افزاری مطرح شده است که فرد متخاصم با تغییرات بدخواهانه بر روی تراشه، آن را برای رسیدن به مقصود خود آماده می‌کند. هدف از این حملات از کار انداختن تراشه، تغییر مشخصات و بدست آوردن اطلاعات حساس می‌باشد.

در این مقاله ابتدا دسته‌بندی مناسبی از انواع تروجان‌های سخت‌افزاری و روش‌های کشف و مقابله با آن‌ها انجام شده است. در ادامه چهار نمونه عملی تروجان بر روی الگوریتم رمزنگاری DES پیاده‌سازی شده و نتایج آن مورد بررسی قرار گرفته است. سپس سخت‌افزاری بر پایه مشخصه تاخیر مدار پیشنهاد شده است که ورودی آن فرکانس حلقه‌های نوسانگر تعبیه شده در مدار تحت تست و خروجی آن یک رشته بیت متناظر با چالش اعمال شده می‌باشد. سخت‌افزار پیشنهادی به گونه‌ای طراحی شده است که در صورت تغییر در مدار اصلی، با تغییر در فرکانس حلقه‌های نوسانگر و در نتیجه رشته بیت مورد انتظار، وجود سخت-افزار تروجان را مشخص می‌کند. از طرفی با بررسی عوامل موثر بر فرکانس حلقه نوسانگر از جمله دما، ولتاژ و تغییرات پروسس، حلقه‌های نوسانگری برای تعبیه درون مدار توصیه شده است که باعث کاهش تغییرات فرکانس در برابر این عوامل شده و تغییرات فرکانس ناشی از این عوامل به منزله تغییر فرکانس ناشی از حمله به سخت‌افزار تلقی نمی‌شود و در نتیجه با حذف عوامل تاثیرگذار منفی محیطی در مدار طراحی‌شده، سخت‌افزار پیشنهادی با دقت بالایی برای کاربرد کشف تروجان پیشنهاد شده‌است.

واژه‌های کلیدی: امنیت، تغییرات خرابکارانه، تروجان سخت افزاری، کشف تروجان، حلقه نوسانگر

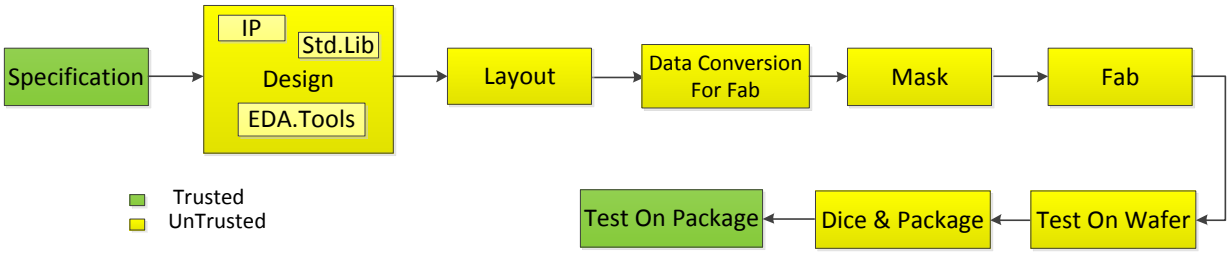
۱. مقدمه

مهمترین چالش وسایل حساس و در کل کاربردهای رمزنگاری، چگونگی حفظ امنیت آن‌ها است. در سال‌های گذشته انواع حملات سخت‌افزاری و نرم‌افزاری، از جمله حملات آنالیز توان مصرفی، فیزیکی، مرد میانی، تکرار و ... مطرح بوده و تحقیقات فراوانی نیز روی آن‌ها انجام شده است. اما اخیرا یک حمله سخت‌افزای جدید معرفی شده که

نویسندهٔ عهده‌دار مکاتبات: محمدابراهیم سمیع samie@shirazu.ac.ir

با توجه به اینکه عمر آن کمتر یک دهه است، بسیار مورد توجه قرار دارد. برای ساخت یک تراشه از مرحله ایده فکری و طرح اولیه تا ساخت و تولید انبوه آن بخش‌های مختلفی درگیر بوده و مراحل گوناگونی باید سپری شوند که هریک از این مراحل به دیگری مرتبط می‌باشد. ارتباط این بخش‌ها مکان انجام حمله در مراحل مختلف طراحی، ساخت و توسعه، حمله بر روی سخت‌افزار رمزنگاری را مستعدتر می‌کند[۲۱].

به دلیل وسعت طراحی و ساخت صنعت نیمه هادی، تراشه‌ها برای فعالیت‌های بدخواهانه و مهاجمانه آسیب پذیر شده‌اند. این مخاطرات، نگرانی‌ها در موضوع تهدیدات ممکن برای سیستم‌های نظامی، سازمان‌های مالی و امنیت حمل و نقل را افزایش داده است. مداری که در هریک از مراحل تولید تا ساخت توسط طراحان مدار یا کارخانه سازنده در طرح اصلی گنجانده می‌شود و باعث تغییرات خرابکارانه بر روی تراشه شود، تروجان سخت‌افزاری نام دارد. فرد متخاصم می‌تواند تروجانی را طراحی کند که در زمان‌های آتی سیستم را مختل کرده یا باعث نشت اطلاعات محرمانه شود. در شکل ۱ مراحل تولید تا ساخت یک مدار مجتمع و همچنین امن یا غیر امن بودن هر مرحله نمایش داده شده است. مرحله‌هایی که با رنگ سبز مشخص شده‌اند، امکان قرارگیری تروجان در این مراحل وجود ندارد و مراحلی که با رنگ زرد نشان داده شده‌اند مستعد حضور تروجان سخت‌افزاری می‌باشند.

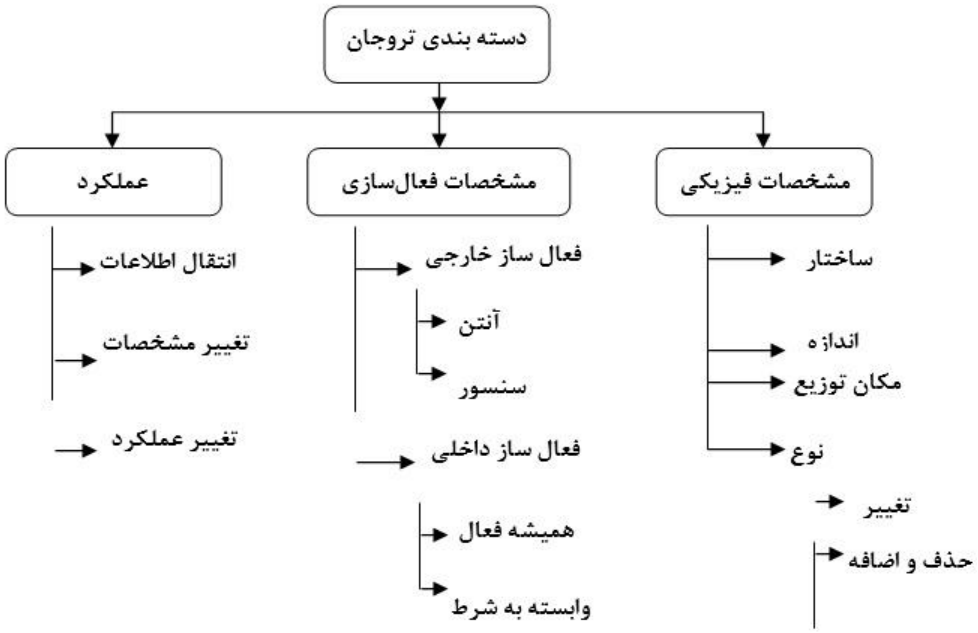


شکل۱: آسیب‌پذیری مراحل ساخت مدارمجتمع

در این مقاله به معرفی کامل این تهدید جدید، راه‌های مقابله با آن و به برخی از فعالیت‌های انجام شده در این زمینه پرداخته و همچنین سخت‌افزاری برای کشف این حمله سخت‌افزاری پیشنهاد شده است که شامل قسمت‌های زیر می‌باشد. در بخش دوم تروجان‌های سخت‌افزاری با توجه به پارامترهای گوناگون تقسیم‌بندی شده‌اند. در بخش سوم به روش‌های گوناگون کشف و شناسایی این حمله سخت‌افزاری و همچنین تولید یک تراشه امن پرداخته شده است. در بخش چهارم پیاده‌سازی‌های انجام شده از تروجان سخت‌افزاری بیان شده است. در بخش پنجم به مفهوم حلقه نوسانگر، عوامل موثر بر آن و چگونگی عملکرد آن در کشف تروجان سخت‌افزاری در بخش ششم پارامتر تغییرات پروسس مورد بررسی قرار گرفته است. سخت افزار پیشنهادی برای تست مدار و کشف تروجان و همچنین بررسی میزان دقت این سخت‌افزار پیشنهادی، در بخش پایانی آورده شده است.

۲. دسته‌بندی تروجان

تروجان‌های سخت‌افزاری در سه دسته اصلی بر طبق مشخصات فیزیکی، مشخصات فعال‌سازی و عملکرد آن‌ها طبقه‌بندی می‌شوند.[۲۲]. این دسته‌بندی در شکل ۲ نشان داده شده است. همچنین تروجان‌ها می‌توانند ترکیبی از این سه دسته نیز باشند. به‌طور مثال می‌توانند چندین مشخصه فعال‌سازی داشته باشند[۲۰].



شکل ۲: دسته‌بندی تروجان

۲-۱- پارامتر اول دسته‌بندی تروجان: مشخصات فیزیکی

مشخصات فیزیکی یکی از پارامترهایی است که بر اساس آن تروجان‌ها به چهار زیر دسته تقسیم می‌شوند[۲۲]. زیر دسته نوع، خود به دو بخش تغییر و حذف و اضافه تقسیم می‌شود. کلاس حذف و اضافه شامل تروجان‌هایی می‌شود که به صورت فیزیکی به اضافه یا حذف ترانزیستورها و گیت‌ها اشاره دارد. در حالیکه کلاس تغییر به تروجان‌هایی اشاره دارد که به تغییر سیم‌ها و منطق‌های موجود تحق بخشیدند. دسته اندازه، تعداد اجزای داخل تراشه که اضافه و حذف شده‌اند را محاسبه می‌کند. دسته مکان توزیع، محل قرارگرفتن تروجان در طرح‌بندی فیزیکی تراشه را توصیف می‌کند. دسته ساختار به موردی اشاره دارد که فرد متخاصم به منظور تعبیه تروجان، مجبور به ساخت دوباره طرح تراشه شده که باعث تغییر شکل فیزیکی تراشه می‌شود. باید مدنظر داشت که تغییر بدخواهانه در طرح فیزیکی که پارامترهای تاخیر و توان را تغییر دهد، می‌تواند کشف تروجان را آسان کند.

۲-۲- پارامتردوم دسته بندی تروجان: مشخصات فعال‌سازی

دسته مشخصات فعال‌سازی به معیارهایی اشاره دارد که باعث راه اندازی تروجان می‌شود. مشخصات فعال‌سازی شامل دو زیر دسته می‌باشد: ۱. فعال‌ساز خارجی که بوسیله آنتن یا سنسور که با دنیای بیرون در ارتباط هستند، راه‌اندازی می‌شود. ۲. فعال‌سازی داخلی که خود این دسته شامل دو زیر قسمت همیشه فعال و وابسته به شرط می‌باشد[۲۲].

وضعیت همیشه فعال به این معناست که تروجان همیشه در حال فعالیت بوده و می‌تواند در هر لحظه فعالیت تراشه را مختل کند. وضعیت وابسته به شرط شامل تروجان‌هایی می‌شود که تا زمانی‌که شرط خاصی تامین نشود، غیرفعال هستند. شروط فعال‌سازی می‌توانند بر پایه خروجی یک سنسور

باشند. به‌طوری که تابعی از دما، ولتاژ یا هر شرط دیگر محیط باشند. همچنین این شرایط می‌توانند بر پایه وضعیت منطق داخلی مانند یک الگوی ورودی خاص یا مقدار یک شمارنده داخلی باشند[۲۰].

۳-۲- پارامتر سوم دسته‌بندی تروجان: مشخصه عملکرد

نوع رفتار مختل کننده تروجان را بیان می‌کند. این بخش شامل سه زیر دسته می‌شود:

۱. تغییر عملکرد: به تروجان‌هایی اشاره دارد که عملکرد تراشه را به‌وسیله اضافه کردن منطق جدید یا کنارگذاشتن منطق‌های موجود تغییر می‌دهد. ۲. تغییر مشخصات به تروجان‌هایی اشاره دارد که هدف آن‌ها تغییر ویژگی‌های پارامتری تراشه مانند تاخیر می‌باشد. ۳. انتقال اطلاعات شامل تروجان‌هایی می‌شوند که اطلاعاتی مانند کلید را برای فرد متخاصم ارسال می‌کند[۲۰].

۳- دسته‌بندی کشف و مقابله با تروجان

پس از شناسایی انواع تروجان سخت‌افزاری، هدف اصلی چگونگی شناسایی و مقابله با آن‌ها می‌باشد. نویسندگان این مقاله روش‌هایی را که مورد بررسی قرار گرفته‌است مورد مطالعه قرار داده و دسته‌بندی از آن ارائه داده‌اند. در زیر هر دسته برای واضح‌تر شدن ابعاد مسئله، منابع مرتبط و سال‌های فعالیت در آن زمینه نیز آورده شده است. بر طبق دسته‌بندی انجام شده، روش‌های کشف و مقابله با تروجان سخت‌افزاری مطابق شکل ۳ به چهار دسته اصلی تقسیم می‌شوند.

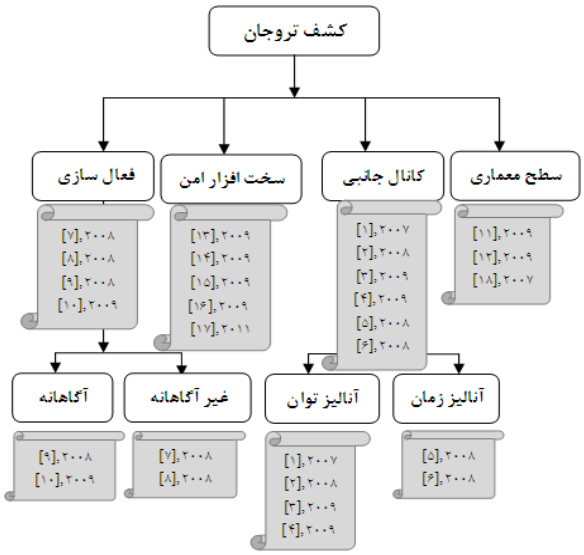
۳-۱- کشف تروجان بر پایه آنالیز سیگنال‌های کانال جانبی

سیگنال‌های کانال جانبی مانند زمان و توان برای کشف تروجان استفاده می‌شوند. سیگنال‌های کانال جانبی بر پایه توان یک دید مناسب از ساختار داخلی فعالیت‌های داخلی تراشه و در نتیجه توانایی کشف تروجان بدون راه‌اندازی آن‌ها را فراهم می‌کنند.

۳-۱-۱- کشف تروجان بر پایه آنالیز توان

آگراوال اولین شخصی بود که از اطلاعات کانال جانبی برای کشف تروجان با کمک از مصرف توان مدار استفاده کرد[۱]. برای بدست آوردن الگوی توانی مدار بدون تروجان، الگوهای تصادفی به مدار داده شده و توان آن اندازه‌گیری می‌شود. بعد از اعمال ورودی، تعداد محدودی از تراشه‌ها مهندسی معکوس می‌شوند تا ازعدم وجود تروجان در آن‌ها اطمینان حاصل شود. وقتی الگوی مرجع بدست آمد، الگوی تصادفی مشابه به تراشه‌های تحت تصدیق هویت داده می‌شود. اگر الگوی توانی این تراشه‌ها با الگوی مرجع متفاوت باشد، این تراشه مشکوک تلقی شده و احتمال وجود تروجان در آن زیاد می‌باشد.

Rad روش آنالیز تغییرات سیگنال توان بر پایه منطقه را به منظور کاهش سهم تغییرات پردازش و جریان‌های نشتی پیشنهاد کرد[۳]. منطقه یک بخش طرح است که بخش عمده توان خود را از پورت‌های توان دریافت می‌کند.



شکل ۳: دسته‌بندی روش‌های کشف تروجان

۳-۱-۲- کشف تروجان بر پایه آنالیز زمان

Li و Lach برای کشف تروجان روش PUF را بر پایه تاخیر پیشنهاد کردند[۵]. این روش از تکنیک‌های اندازه‌گیری تاخیر کلاک برای اندازه‌گیری تاخیر مسیر ثبات-ثبات انتخاب شده، استفاده می‌کند. مدار اصلی شامل ثبات و مدار ترکیبی است که توسط کلاک ۱ راه‌اندازی شده‌اند. ثبات سایه، ورودی مشابه ثبات مقصد می‌گیرد، اما توسط کلاک ۲ راه‌اندازی می‌شود و در نتیجه حاصل هر دو در طول هر کلاک مقایسه می‌شود.

۲-۳- کشف تروجان توسط پارامترهای فعال‌سازی

روش‌های فعال‌سازی می‌تواند فرآیند کشف تروجان را تسریع بخشیده و در بعضی موارد با آنالیز توان هنگام اجرا ترکیب شوند. اگر بخشی از تروجان فعال شود، مدار تروجان توان دینامیکی بیشتری مصرف می‌کند که به بررسی تفاضل توان مدار بدون تروجان و با تروجان کمک می‌کند.

۱-۲-۳- فعال‌سازی غیر آگاهانه

این روش بر پایه فعال‌سازی تصادفی یا تروجان‌ها می‌باشد. برای مثال Jha و همکارانش روشی احتمالی را برای کشف تروجان‌ها ارائه کردند[۷]. آن‌ها نشان دادند اعمال برخی مشخصات احتمالی برای الگوهای اعمال شده به ورودی، به کشف تروجان کمک می‌کند. در نتیجه الگوهای ورودی بر پایه مشخصات احتمالی را برای تراشه تحت تصدیق هویت اعمال کرده و خروجی آن را با مدار اصلی مقایسه کردند. اگر اختلاف در خروجی‌ها مشاهده شود، مدار شامل تروجان سخت‌افزاری می‌باشد. برای کشف تروجان در تراشه‌های ساخته شده، الگوها می‌توانند فقط بر پایه بعضی احتمالات و به منظور بررسی یکسان بودن طراحی ساخته شده و تراشه اصلی، اعمال شوند.

Wolff ترکیبات مدارات نادر در طراحی را آنالیز کرد[۸]. این سیم‌های به ندرت فعال، برای فعال‌سازی تروجان استفاده می‌شوند. او یک مجموعه بردار را برای فعال‌سازی اینگونه سیم‌ها تولید کرده و پیشنهاد ترکیب آن‌ها با بردارهای تست ATPG را برای فعال‌سازی تروجان مطرح کرد.

۲-۲-۳- فعال‌سازی آگاهانه

Banga و Hsiao تکنیک تولید تست دو مرحله‌ای را ایجاد کردند.[۹] هدف آن‌ها بزرگنمایی اختلافات بین تراشه تحت تصدیق هویت و شکل موج‌های توان طراحی اصلی بود. در مرحله اول (جزءبندی مدار) یک الگوی آگاه از منطقه کمک می‌کرد تا مناطق مستعد قرار گرفتن تروجان مشخص شود. در مرحله بعد (بزرگنمایی فعالیت) الگوهای جدید تست در مناطق شناسایی شده برای بزرگنمایی اختلاف بین مدار اصلی و مدار همراه تروجان اعمال می‌شوند. در این مرحله بردارهای بیشتری برای مناطقی که احتمال وجود تروجان در آن‌ها بیشتر است، با استفاده از الگوی تولید تست مشابه در مرحله اول ساخته می‌شوند.

۳-۳- کشف تروجان در سطح معماری

تکنیک‌هایی مانند قرار گرفتن قسمت‌های امن در موارد خاص با نور، دما، مداخله یا سنسور می‌توانند حفاظت را در سطح فیزیکی فراهم کنند. برای سر و کار داشتن با حملات کانال جانبی در سطح میکرو معماری، Verbauwhede و Schaumont پیشنهادکردند دستورات if thenelse برای مصرف مقدار زمان و توان در طول اجرا بالانس شوند[۱۸].

۴-۳- سخت‌افزار امن برای مقابله با تروجان

فعالیت‌های طراحی حال حاضر، آنالیز سیگنال کانال جانبی یا تولید الگو برای کشف تروجان را پشتیبانی نمی-کنند. در این بخش به چند روش پیشنهاد شده برای بهبود کشف تروجان از طریق ایزوله‌کردن سخت‌افزار به کمک تغییر یا اصلاح نقشه اصلی طرح پرداخته شده است. این روش ها طراحی برای سخت افزار امن نام دارند. آن‌ها به جلوگیری از تعبیه تروجان و تسهیل بیشتر کشف تروجان کمک کرده و احراز هویت موثر تراشه را فراهم می‌کنند.

Banga و Hsiao یک طرح ولتاژ معکوس را برای بزرگنمایی فعالیت تروجان پیشنهاد کردند[۱۴]. از آنجاییکه تروجان تحت شرایط خاصی فعال می‌شود، ورودی های تراشه باید قابلیت تغییرات داشته‌باشند که شرایط نادر برای فعال سازی تروجان ایجاد شوند. برای مثال در یک گیت AND ۴ ورودی، یک شرط نادر زمانی است که همه ورودی ها یک باشند. (احتمال۱ به ۱۶). هدف تغییر عملکرد تروجان برای حذف شرایط نادر است. معکوس کردن VDDو GND عملکرد آن را تغییر داده و حاشیه نویز را که هنگام خروجی VDD - VTH و VTH جا به جا می شود را کاهش می‌دهند. در نتیجه تغییر AND به NAND و ۱ در خروجی تروجان NAND مقدار نادری نیست. (احتمال ۱۵ به ۱۶). همچنین در این روش باید سختی تغییر بین ولتاژ VDD و GND را برای هر گیت مدار در نظر گرفت.

۴- پیاده‌سازی تروجان

در این بخش چهار نمونه از تروجان‌های پیاده‌سازی شده توسط نویسندگان مقاله با عملکردهای گوناگون روی الگوریتم **DES** توضیح داده می‌شود. باید توجه شود روش‌های پیاده‌سازی شده روی هر الگوریتم رمزنگاری دیگری مانند **AES** و غیره نیز قابل پیاده سازی است. برای پیاده سازی آن باید چند نکته را مد نظر داشت. مراحل زیر به ترتیب برای پیاده‌سازی تروجان سخت‌افزاری پیشنهاد می‌شود[۲۸].

۱. مطالعه طرح ۲. انتخاب نوع ۳.انتخاب مکان ۴. بهینه‌سازی کد ۵. احتمال کشف

در ابتدا طرح و نکات سیستم مورد حمله باید به دقت مورد مطالعه قرار گیرد. این مرحله بسیار کلیدی و حساس است، چون باید ضعف‌های امنیتی سیستم و چگونگی راه نفوذ به سیستم پیدا شود. معمولا تروجان در واسطی که از توابع رمز استفاده می‌کند قرار می‌گیرد، ولی تعبیه آن در خود توابع رمز و تغییر عملکرد آن‌ها نیز ممکن و محتمل است. پس از آن باید یکی از انواع تروجان که در بخش ۲ شرح داده شد، انتخاب شود. در مرحله بعد نوبت به پیاده سازی تروجان است. از آنجایی که مدار تروجان نباید بزرگ و مورد توجه باشد، در صورت امکان پیش پردازش‌هایی می‌تواند اثر بخش باشد. یکی از این پیش پردازش‌ها برای پیاده‌سازی تروجان در سطح کد، بهینه سازی کد بوده که بستر را برای قراردادن تروجان در کد فراهم می‌کند. هدف از این کار پایین آوردن سربار ناشی از تروجان و کاهش تاثیر حضور آن بر روی پارامترهای مدار می‌باشد. مرحله آخر و بسیار مهم طراحی تروجان، ارزیابی احتمال کشف آن است. برای اختفای تروجان و موثر بودن حمله، باید تا حد امکان احتمال کشف آن کاهش یابد. یک روش مناسب، فعال‌سازی تروجان با شرایط خاص است که احتمال کشف تصادفی آن بسیار کاهش یابد.

نویسندگان این مقاله چهار تروجان در سطح کد سخت‌افزاری طراحی کرده‌اند. مرحله‌ای که برای تعبیه تروجان انتخاب شده‌است، اولین مرحله آسیب‌پذیر مشخص‌شده در شکل ۱ می‌باشد که در مرحله طراحی، تروجان‌های مورد نظر در مدار قرار می‌گیرند. همچنین روش فعال‌سازی در نظرگرفته شده برای فعال‌سازی تروجان‌ها، استفاده از شرایط ورودی خاص همراه با محدودیت زمان است. این بدین معنی است که ورودی‌های خاص همراه با بازه زمانی خاص برای فعال‌سازی تروجان در نظر گرفته شده‌است که احتمال فعال‌سازی تصادفی آن را به سمت صفر میل می‌دهد. به طور مثال به کارگیری دو کلید خاص به فاصله زمانی مشخص نمونه عملی این ایده است. جدول ۱ خلاصه‌ای از تروجان‌های پیاده‌سازی شده می‌باشد. فعال ساز پیشنهادی برای تروجان ۱، دو ورودی از صفحه کلید با ۱۰۰ کلید است که احتمال حدس درست هر کلید ۰/۰۱است. فعال ساز پیشنهادی برای تروجان ۲ دو ورودی با فاصله زمانی ۱۰- ۱۱ثانیه است که اگر در این بازه کلید دیگری فشرده شود، فعال سازی متوقف می‌شود. همان‌طور که گفته شد کد سخت‌افزاری که پیاده‌سازی شده است الگوریتم رمزنگاری DES می‌باشد که بر روی آن چهار تروجان گوناگون طراحی شده است. در هر شکل دوایری که ترسیم شده‌اند محل‌های حساسی می‌باشند که برای درک عملکرد تروجان باید به آن‌ها توجه شود. در هریک از چهار آزمایش داده‌های ورودی و خروجی موجود در طراحی به شرح زیر قرار دارند:

DES_TB/Clock: سیگنال کلاک سیستم می‌باشد.

DES_TB/Din: داده ورودی الگوریتم رمزنگاری DES می‌باشد.

DES_TB/Key: کلید مورد نظر برای انجام عملیات رمزنگاری DES می‌باشد.

DES_TB/Dout: داده خروجی الگوریتم رمزنگاری DES و به عبارتی رمزشده داده ورودی می‌باشد.

DES_TB/Trojan Enable: سیگنال فعال‌سازی تروجان می‌باشد که با فعال‌شدن این سیگنال، تروجان طراحی شده شروع به کار می‌کند.

در ادامه جزییات چهار تروجانی که در این تحقیق پیاده‌سازی کرده‌ایم، بیان و نتایج آن آورده شده است.

۴-۱- تروجانی با عملکرد استخراج متن اصلی

یکی از متداول‌ترین تروجان‌ها، تروجانی است از دسته نوع عملکرد که کارکرد آن انتقال اطلاعات است. هدف از رمزنگاری حفظ امنیت متن اصلی و غیر قابل استفاده

کردن آن برای افراد غیر مجاز است. حال اگر دسترسی به متن اصلی امکان‌پذیر باشد، رمزنگاری با شکست مواجه شده و اثر آن از بین رفته است. در این تروجان، هنگام فعال‌سازی تروجان، عملکرد مدار تغییر کرده و به جای رمز شده، متن اصلی به پورت خروجی ارسال می‌شود. در قسمت اول شکل ۴ نتایج این تروجان نمایش داده شده است. دایره قرمز اول (DES_TB/Din) متن ورودی به سیستم می‌باشد که باید رمز شود و در خروجی برگردانده شود. هنگامی که پایه فعال‌ساز تروجان فعال شود، متن اصلی بدون اینکه رمز شود به خروجی منتقل می‌شود. دایره قرمز دوم (DES_TB/Dout) خروجی سیستم رمزنگاری را نشان می‌دهد که بعد از فعال‌شدن تروجان، در صورتی که باید رمزشده متن اصلی را به خروجی منتقل دقیقا متن ورودی را به خروجی منتقل کرده و این به معنی افشای متن ورودی و شکست عملیات رمزنگاری می‌باشد.

۴-۲- تروجانی با عملکرد استخراج کلید رمز

تروجان دوم نیز عملکردی مانند تروجان اول داشته و وظیفه انتقال اطلاعات را بر عهده دارد. امنیت الگوریتم و دستگاه رمز نگار بستگی به کلید و عدم دسترسی به آن دارد. حال اگر یافتن کلید امکان پذیر باشد، حمله موفقی به سیستم شده است. در این نمونه تروجان، سیگنالی به نام Trojan_Enable در نظر گرفته شده است که با فعال بودن آن تروجان طراحی شده فعال می‌شود. در قسمت دوم شکل ۴، دایره قرمز اول (DES_TB/Key) نمایانگر کلید سیستم رمزنگاری است. هنگامی که تروجان فعال می‌شود، خروجی مدار به جای متن رمز شده کلید رمزنگاری خواهد بود. دایره قرمز رنگ دوم (DES_TB/Dout) پورت خروجی سیستم رمز نگاری را نشان می‌دهد که پس از فعال‌سازی تروجان به‌جای متن رمز شده، حاوی کلید سیستم رمزنگاری می‌باشد. در نتیجه کلید رمزنگاری افشا شده و با در اختیار داشتن آن، کنترل سیستم را در اختیار خواهیم داشت.

۴-۳- تروجانی با عملکرد تغییر کلید رمز

همان طور که گفته شد، کلید پارامتر مهم رمزنگاری است. در نتیجه یکی از اهداف، بدست آوردن کلید است. در این تروجان مدار به فعالیت عادی خود ادامه می‌دهد ولی زمانی که سیگنال Trojan_Enable فعال شود، کلید رمز با کلید مورد نظر حمله کننده جابجا می‌شود. در نتیجه با داشتن متن اصلی و کلید رمز، کنترل وسیله رمز نگار در اختیار حمله کننده خواهد بود. در قسمت سوم شکل ۴ نتایج این تروجان نشان داده شده است. دایره قرمز رنگ اول (DES_TB/Key) کلید اصلی سیستم رمز نگاری می‌باشد که سیستم با این کلید متن ورودی را رمز می‌کند. دایره سبز رنگ مشخص شده در شکل (DES_TB/Key2)، کلید مورد نظر تروجان است که پس از فعال‌سازی تروجان این کلید جای کلید اصلی سیستم رمزنگاری قرار گرفته و با در اختیار داشتن کلید، کنترل سیستم در اختیار حمله‌کننده قرار می‌گیرد.این تروجان به‌گونه‌ای طراحی شده است که پس از غیرفعال شدن تروجان به صورت عادی به فعالیت خود ادامه دهد. بدین منظور کلید اصلی سیستم در حافظه سیستم ذخیره شده و پس از غیرفعال شدن تروجان، جایگزین کلید تروجان شده و سیستم با روند عادی به فعالیت خواهد پرداخت. دایره قرمز رنگ دوم (DES_TB/Key1) نشان‌دهنده کلید اصلی ذخیره شده است.

۴-۴- تروجانی با ایجاد اختلال در عملکرد معمولی وسیله رمزنگار

علاوه بر نشت اطلاعات، همانطور که در دسته بندی‌ها اشاره شد، تغییر عملکرد و از کار انداختن وسیله نیز از اقسام تروجان‌ها می‌باشد. به طور مثال قرار دادن قسمت رمز نگار در یک حلقه نامحدود و انجام مداوم عمل رمز دو پیامد را در بر دارد:

۱. مختل کردن رفتار عادی وسیله

۲. آماده کردن شرایط برای حمله سرریز بافر

قسمت چهارم شکل ۴ نتایج پیاده‌سازی این نوع تروجان است. زمانی که با سیگنال فعال‌ساز (DES_TB/Trojan Enable) یک شود، تروجان فعال شده و با یک عملیات نامحدود رمزنگاری سیستم را از حالت عادی خارج کرده و تا از کارانداختن منابع سیستم به فعالیت خود ادامه می‌دهد. دوایر قرمز رنگ نمایانگر انجام نامحدود عملیات رمزنگاری می‌باشد.

جدول ۱: مشخصات تروجان‌های پیاده سازی شده

شماره تروجان	نوع عملکرد	چگونگی عملکرد	فعال‌ساز پیشنهادی	احتمال کشف تصادفی
تروجان ۱	انتقال اطلاعات حساس	نشت متن اصلی	دو ورودی خاص	10^{-4}
تروجان ۲	انتقال اطلاعات حساس	نشت کلید	ورودی‌های خاص + زمان	10^{-42}
تروجان ۳	تغییر اطلاعات حساس	تغییر کلید	سنسور حرارتی	ناچیز
تروجان ۴	اختلال در مدار	حلقه نامحدود	همیشه فعال	ناچیز

شکل ۴: شکل موج چهار تروجان پیاده سازی شده

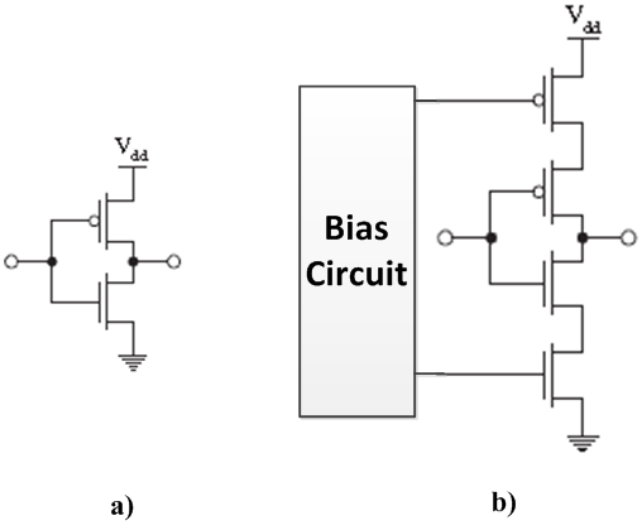
۵- بررسی حلقه نوسانگر و عوامل تاثیرگذار

حلقه نوسانگر شامل تعدادی فرد از گیت وارونگر می‌باشد که به صورت حلقه‌ای به هم متصل هستند. حلقه نوسانگر با یک فرکانس مشخص که به تاخیر هر وارونگر بستگی دارد نوسان می‌کند. فرکانس آن طبق فرمول ۱ بدست می‌آید. در این فرمول n تعداد گیت‌های وارونگر و t تاخیر ناشی از هر گیت می‌باشد[۲۴].

$$f = \frac{1}{2*n*t} \quad (۱)$$

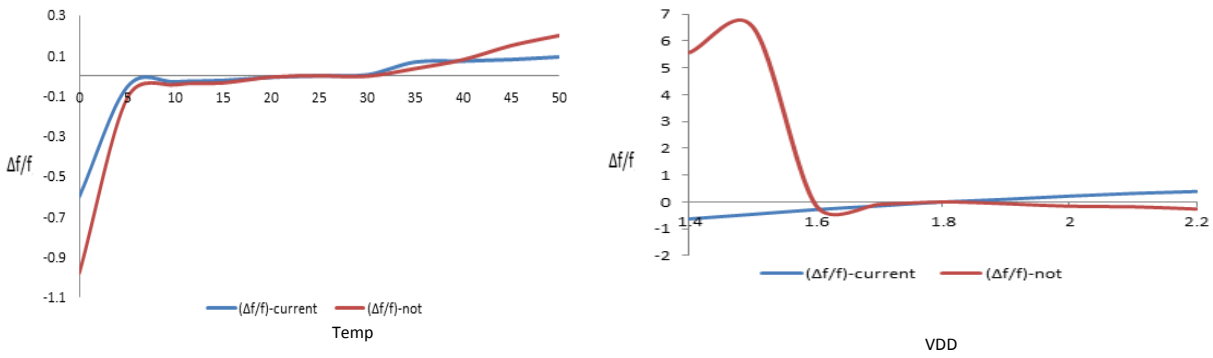
در طراحی حلقه‌های نوسانگر با توجه به کاربرد آن پارامترهای گوناگونی مانند مصرف توان، دقت فرکانس، تاثیرات دما، ولتاژ و ... می‌توانند حائز اهمیت باشند که با توجه به نوع طراحی، نوع گیت‌های وارونگر، تعداد طبقات و ... تنظیم می‌شوند. یکی از انواع حلقه‌های نوسانگر، کنترل شونده با ولتاژ (VCO) می‌باشند که کاربردهای فراوانی از جمله مدارهای بازیابی کلاک و داده دارند. همان طور که گفته شد، فرکانس این حلقه‌های نوسانگر نیز تابع عوامل محیطی بوده و لذا چگونگی طراحی آن‌ها از اهمیت بالایی برخوردار است. یکی ازعناصر مهم در ساخت حلقه نوسانگر، نوع گیت وارونگر است. در منابع [۲۵]و[۲۶] انواع متداولی از آن‌ها معرفی شده است. در شکل ۵، دو نوع از این گیت‌ها نشان داده شده‌اند. شکل ۵- b گیت وارونگر Current starved می باشد که جریان شارژ و دشارژ خازن خروجی توسط مدار راه‌انداز تنظیم می‌شود.

از وارونگرهای متفاوت برای جبران تاثیر عوامل محیطی بر روی حلقه‌های نوسانگر می‌باشد. وارونگرهای متفاوتی طراحی شده است که بر پایه آن‌ها می‌توان حلقه‌های نوسانگر متفاوتی طراحی کرد. ساخت حلقه نوسانگر با هر یک از این وارونگرها رفتار متفاوتی در برابر تغییر شرایط محیطی از خود نشان می‌دهد.



شکل۵: وارونگر : a) ساده b) Current starved

استفاده از وارونگر current starved with output-switching(CV) در حلقه‌های نوسانگر پایداری فرکانس در برابر تغییرات شرایط محیطی را افزایش خواهد داد. در شکل‌های ۶ تاثیر دما و ولتاژ بر روی فرکانس حلقه نوسانگر ساخته شده با وارونگر CV در مقابل حلقه نوسانگر ساخته شده با وارونگر معمولی نشان‌داده شده‌است. همان‌طور که در شکل مشاهده می‌شود تاثیر دما و ولتاژ بر روی فرکانس حلقه نوسانگر ساخته شده با وارونگر CV کمتر بوده و تغییرات فرکانسی کمتری از خود نشان می‌دهند. به عبارتی پایداری فرکانسی این نوع حلقه نوسانگر در مقایسه با حلقه نوسانگر ساخته شده با وارونگر معمولی بیشتر می‌باشد. در این شکل نمودار قرمز رنگ، تغییرات فرکانس حلقه نوسانگر ساخته شده با وارونگر معمولی در برابر عوامل محیطی را نشان می‌دهد و نمودار آبی رنگ مربوط به حلقه نوسانگر ساخته شده با وارونگر CV می‌باشد.

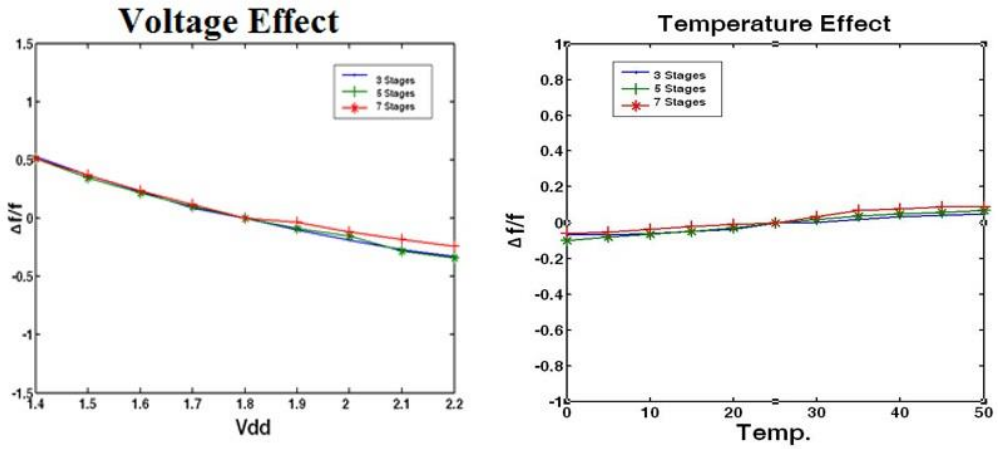


a) b)

شکل۶ : تاثیر عوامل محیطی بر روی فرکانس حلقه‌های نوسانگر مختلف a) تاثیر ولتاژ b) تاثیر دما

به منظور بررسی بیشتر تاثیر عوامل محیطی بر روی فرکانس حلقه نوسانگر ساخته شده با وارونگر CV، سه حلقه نوسانگر به ترتیب متشکل از ۳، ۵ و ۷ گیت وارونگر ساخته شده و تغییرات فرکانسی هریک از این حلقه‌ها در برابر عوامل محیطی مورد ارزیابی قرار گرفتند.

با توجه به شکل ۷، علاوه بر پایداری فرکانسی بیشتر این نوع حلقه‌های نوسانگر در برابر تغییرات دما و ولتاژ، تاثیر تعداد گیت‌های وارونگر به کاررفته در ساخت حلقه نوسانگر نیز قابل مشاهده می‌باشد.

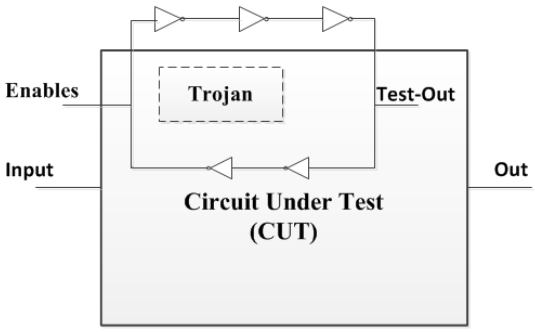


(a) (b)

شکل ۷: تاثیر عوامل محیطی بر روی فرکانس حلقه‌های نوسانگر ساخته شده با a CV) تاثیر ولتاژ b) تاثیر دما

۱-۵- کاربرد حلقه نوسانگر

در این مدل هر مدار را می‌توان یک چندگانه به صورت <Tech,G,F,RO> در نظر گرفت. منظور از Tech پارامترهای تکنولوژی مانند W و L است. G معرف گراف و توپولوژی مدار وF منطق و عملکرد مدار می‌باشد. RO نیز حلقه‌های نوسانگری هستند که برای تست به مدار اضافه شده‌اند. با توجه به حساسیت فرکانس حلقه نوسانگر، می‌توان از آن برای کشف هر گونه تغییری در مدار استفاده کرد. بدین صورت که اگر مسیرهای مدار، داخل یک حلقه نوسانگر قرار گیرند، حلقه نوسانگر با توجه به تاخیر موجود در مسیر با فرکانس مشخصی نوسان می‌کند و در نتیجه اگر تغییری در مدار صورت گیرد، فرکانس تغییر کرده و باعث کشف تروجان می‌شود. مدل مفهومی استفاده از حلقه نوسانگر در کشف تروجان سخت‌افزاری در شکل ۸ نمایش داده شده‌است.



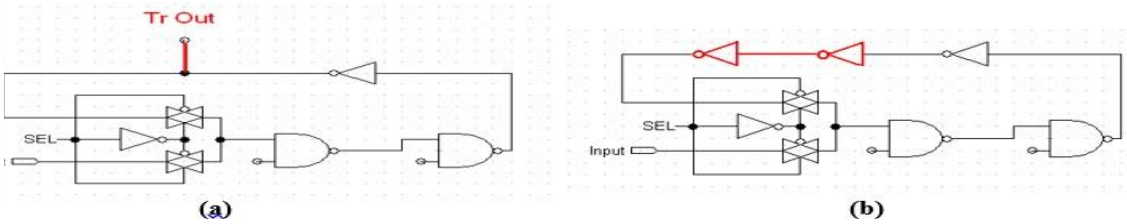
شکل ۸: مدل مفهومی کشف تروجان

قراردادن تروجان در مدار در هر یک از مراحل طراحی، ساخت، تست و ... امکان‌پذیر است. اما هدف حلقه نوسانگر تروجان‌هایی است که در مرحله ساخت در مدار تعبیه می‌شوند. در این مرحله نیز قادر به کشف تروجان‌هایی است که یا از نوع اضافه کردن گیت هستند یا از نوع تغییر ساختار گیت‌های حاضر می‌باشند. حلقه نوسانگر قادر به کشف کوچکترین تروجان‌ها از نوع gate-level می‌باشد. به عبارتی این روش مراحل قسمت Mask به بعد در شکل ۱ را امن کرده و تروجان‌های طراحی‌شده در این مراحل را کشف خواهد کرد. از دیگر مزایای حلقه نوسانگر این است که اگر تروجان در بخشی از تراشه‌ها نیز قرار داشته باشند، این روش موثر است.

۲-۵- مثالی از عملکرد حلقه نوسانگر

در ادامه چگونگی عملکرد حلقه نوسانگر بر روی مدار نمونه C17 نشان داده شده است. برای قرار دادن حلقه نوسانگر می‌توان از روشی که rijendran و همکارانش معرفی کرده‌اند استفاده کرد[۲۷]. در این روش در هر مرحله مسیری با بیشترین گیت انتخاب شده و داخل یک حلقه نوسانگر قرار گرفته و امن تلقی می‌شود. همچنین الگوی ورودی مناسب برای تحریک آن نیز محاسبه می‌شود. این کار تا امن شدن تمام گیت‌ها ادامه پیدا می‌کند.

برای چگونگی عملکرد مدار تست دو نوع تروجان طراحی کرده و در حلقه اول نوسانگر قرار داده و در نتیجه اثرات این روش بر روی آن‌ها مورد بررسی قرار گرفته است. تروجان نوع اول تروجان فعال‌ساز نام دارد. به این صورت که سیم‌های فعال‌ساز تروجان به مدار اصلی وصل شده و در نتیجه باعث افزایش خازن کل مسیر می‌شود. تروجان نوع دوم را سربار نامیده و به این صورت است که دو گیت وارونگر به مدار اضافه می‌کند. شکل‌های ۹ دو نوع تروجان را نشان می‌دهد.

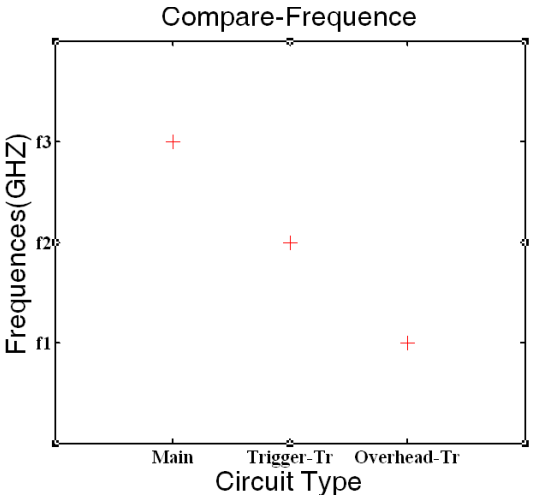


شکل۹: تروجان های a) سربار b) فعال ساز

$$f = \frac{1}{T} \quad (۲)$$

$$\begin{cases} \text{if } |f1 - f2| < e \longrightarrow trojanun\ det\ ected \\ \text{if } |f1 - f2| > e \longrightarrow trojan\ det\ ected \end{cases} \quad (۳)$$

در فرمول ۳ منظور از e اختلاف فرکانسی است که بر اثر تغییرات پردازش بوجود می‌آید. این مقدار بر اساس پژوهش‌ها بیشینه مقدار ۶٫۶٪ دارد[۲۸]. همچنین منظور از f1 و f2 به ترتیب فرکانس اصلی مدار و فرکانس مدار در حضور تروجان می‌باشد.



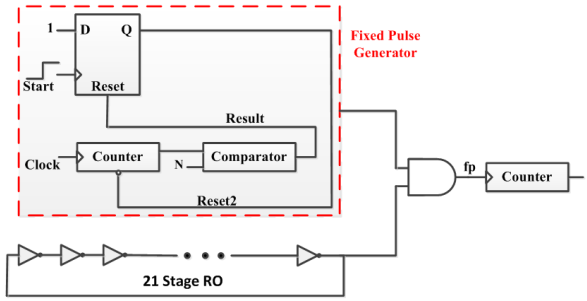
شکل۱۰: فرکانس در حالت اصلی و در حضور تروجان‌ها

در شکل ۱۰ فرکانس اصلی مدار بدون حضور تروجان (f3) و فرکانس‌های مدار در حضور هر یک از تروجان‌های طراحی شده در شکل ۹ (f1 و f2) نشان داده شده‌اند. همان‌طور که مشخص است با تغییر در مدار اصلی فرکانس حلقه نوسانگر تغییر کرده و وجود تغییر مشخص می‌شود.

۶- بررسی تغییرات پروسس

تغییرات پروسس یک تغییر طبیعی مدار می‌باشد که از پارامترهای مختلف ترانزیستور مانند ولتاژ آستانه، ضخامت لایه اکسید، طول و عرض کانال و غیره در فرآیند ساخت مدارهای مجتمع ناشی می‌شود. Shockly برای نخستین بار در هنگام آزمایشات خود به تغییرات تصادفی در قطعات نیمه هادی پی برد. او معتقد بود تاثیرات نوسانات یون‌های گیرنده و دهنده با توزیع پوآسون توزیع می‌شوند. در طی سال‌های بعد دانشمندان زیادی بر روی این پدیده تحقیق کرده و عوامل گوناگونی را در ایجاد تغییرات پروسس موثر دانستند. مدیریت این تغییرات نقش مهمی در تکنولوژی ایفا می‌کند و همچنین تحقیقات نشان داده است که این تغییرات پارامتر حساس وتاثیرگذاری در ساخت نیمه‌هادی‌ها می‌باشد.

Chen سنسوری به نام سنسور تغییرات پردازش معرفی کرده است که اطلاعات مفیدی از شرایط ساخت و محیط در اختیار قرار می‌دهد[۲۲]. این سنسور در شرایط Zero Temperature Coefficient(ZTC) طراحی شده است. در ولتاژ ۰٫۵ تاخیر گیت وارونگر وابسته به دما نخواهد بود، زیرا در آن ولتاژ جریان ترانزیستور NMOS افزایش و جریان ترانزیستور PMOS کاهش خواهد یافت و در نتیجه فرکانس حلقه نوسانگر ثابت خواهد ماند. مدار تولید کننده پالس ثابت مستقل از دما، ولتاژ و تغییرات پروسس می‌باشد. جزییات این مدار در شکل ۱۱ نشان داده شده است. اجزای تشکیل دهنده آن دی فلیپ فلاپ، شمارنده ومقایسه‌گر می‌باشد. وقتی سیگنالStart با تاخیر T1 افزایش می‌یابد، خروجی دی فلیپ فلاپ نیز بالا می‌رود و هنگامی که سیگنال Result با تاخیر T2افزایش می‌یابد، دی فلیپ فلاپ به صفر ریست خواهد شد. هر دو تاخیر T1 و T2 تحت شرایط دما، ولتاژ و تغییرات پروسس یکسانی هستند، درنتیجه اثر آن‌ها حذف خواهد شد و خروجی مدار سیگنالی مستقل از تغییرات گفته شده خواهد بود [۲۲]. سنسور تغییرات پروسس در شکل ۱۱ نشان داده شده است.



شکل ۱۱: سنسور تغییرات پروسس [۲۲]

۷- سخت‌افزار پیشنهادی برای کشف تروجان

در قسمت ۵ توانایی حلقه نوسانگر در تشخیص تروجان‌های مورد نظر نشان داده شد. در این قسمت روشی برای چگونگی استفاده از نتایج حلقه نوسانگر به منظور تشخیص تروجان ارائه شده است. بدین منظور یک سخت‌افزاری در نظر گرفته می‌شود که ورودی آن فرکانس حلقه‌های نوسانگر و خروجی آن تولید یک رشته بیت است. با اعمال یک بردار ورودی مد نظر که رشته بیت خروجی آن را می‌دانیم، رشته بیت خروجی از مدار تست را بدست می‌آوریم و مقایسه رشته بیت خروجی با رشته بیت مورد نظر صحت تراشه را مشخص می‌کند.

در این بخش نویسندگان مقاله با به کار گیری چند تکنیک، یک طراحی جدید کشف تروجان پیشنهاد داده‌اند. خروجی حلقه‌های نوسانگر یک مجموعه فرکانس می‌باشد که روابط زیر برقرار است:

$$F = \{f_1, f_2, \ldots, f_m\} \quad (۴)$$

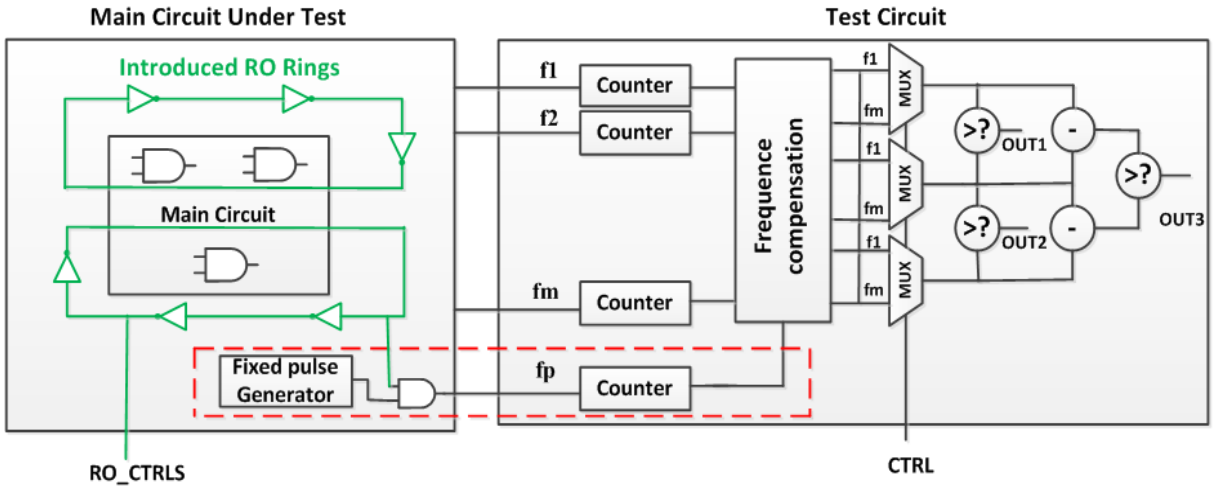
$$f_1 = \min\{f_i \mid i=1 \text{ to } m\} \quad (۵)$$

$$f_m = \max\{f_i \mid i=1 \text{ to } m\} \quad (۶)$$

هر فرکانس به صورت زیر مدل می‌شود:

$$f_i = f_{main} + \Delta f_{pv} + \Delta f_{env} \quad (۷)$$

سخت افزار پیشنهادی با استفاده از خروجی‌های نوسانگرها در شکل ۱۲ نشان داده شده است:



شکل ۱۲: مدار پیشنهادی برای کشف تروجان

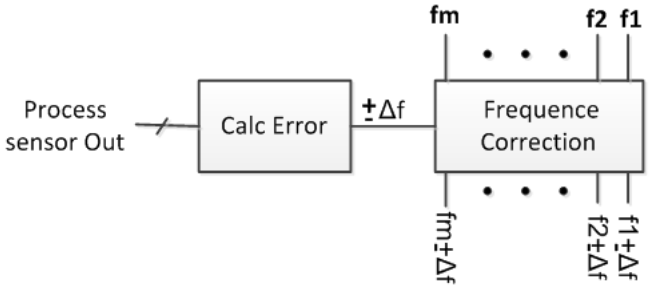
مدار طراحی شده به این صورت عمل می‌کند که فرکانس‌های خروجی از مدار تحت تست را گرفته و به واحد جبران فرکانس می‌دهد. در این واحد که در بلوک دیاگرام آن در شکل ۱۳ نشان داده شده است، خروجی سنسور تغییرات پروسس به واحد محاسبه خطا می‌رود. در این واحد میزان تغییر فرکانس ناشی از تغییرات پروسس محاسبه می‌شود و سپس این مقدار به واحد تصحیح فرکانس انتقال می‌یابد تا با اعمال آن، تغییرات را جبران کند. بدین صورت اثر تغییرات پروسس بر روی فرکانس از بین رفته و فرکانس‌های مورد انتظار در مرحله طراحی را خواهیم داشت. در ادامه فرکانس‌های خروجی به مالتی پلکسرها برای تولید پاسخ متناظر با چالش داده شده رفته وطبق رابطه ۸ یک خروجی سه بیتی به نام OUT تولید می‌کند. برای تولید دو بیت اول، با توجه به سیگنال کنترلی مالتی پلکسرها، دو فرکانس انتخاب شده و با استفاده از فرمول ۹ دو بیت OUT1 و OUT2 محاسبه می‌شوند.

$$\mathrm{OUT} = [OUT_3][OUT_2]\,[OUT_1] \qquad (۸)$$

$$OUT_{1,2} = \begin{cases} 1 & f_a > f_b \\ 0 & O.W \end{cases} \qquad (۹)$$

بیت سوم از رابطه ۱۰ بدست می‌آید:

$$OUT_3 = \begin{cases} 1 & (f_a - f_b) > (f_b - f_c) \\ 0 & O.W \end{cases} \qquad (۱۰)$$



شکل ۱۳: بلوک دیاگرام مدار جبران کننده فرکانس

۷-۱- نتایج آزمایشات و بررسی میزان دقت روش پیشنهادی

در صورت وجود تروجان رابطه زیر برای فرکانس حاکم خواهند بود. f_i' فرکانس حلقه در صورت وجود تروجان بوده که به دلیل وجود تروجان به اندازه f_{trj} تغییر مقدار داده است.

$$f_i' = f_i + f_{trj} \qquad (۱۱)$$

برای بررسی احتمال و دقت کشف تروجان باید به روابط زیر توجه کرد:

$$\Delta d_i = \min\{(f_{i+1} - f_i), (f_i - f_{i-1})\} \qquad (۱۲)$$

$$\Delta e_i = \Delta f_{pv} + \Delta f_{env} \qquad (۱۳)$$

$$\text{If } f_{trj} > |\Delta d_i| + |\Delta e_i| \text{ -> Trojan will be Detected} \qquad (۱۴)$$

در فرمول ۱۲، Δd_i بیانگر حداقل مقدار تفاضل فرکانس‌ها می‌باشد. فرکانس حلقه نوسانگر با توجه به تغییر شرایط محیطی مانند دما و ولتاژ تغییر می‌کند. این مطلب در فرمول ۱۳ به صورت Δf_{env} نشان داده شده است که خطای محیطی بوده ودر حالت ایده آل باید به صفر برسد. فرمول ۱۴ توانایی سخت‌افزار پیشنهادی در کشف تروجان را نشان می‌دهد. در صورتی که مقدار تغییر فرکانس ناشی از وجود تروجان از مجموع دو پارامتر ذکر شده در فرمول‌های ۱۲ و۱۳ بیشتر باشد، تروجان کشف خواهد شد. در نتیجه با حداقل کردن هریک ازدو پارامتر Δd_i و Δe_i دقت سیستم طراحی شده افزایش می‌یابد. راه پیشنهادی برای حداقل کردن خطای محیطی(Δe_i)، استفاده از وارونگرهای معرفی شده در شکل ۵ هستند.

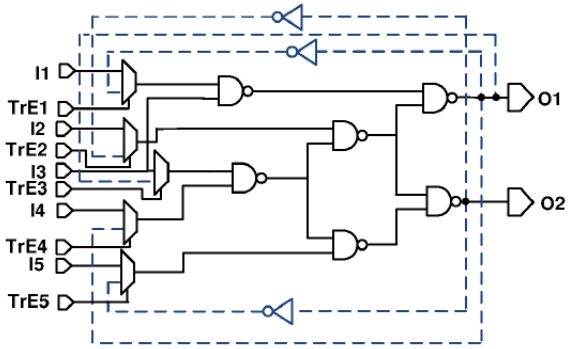
۷-۲- تاثیر روش پیشنهادی

همان‌طور که گفته شد برای افزایش دقت کشف علاوه بر کاهش Δe_i ، Δd_i نیز باید کاهش یابد. وجود بیت سوم در خروجی سخت‌افزار تست به همین علت است. برای اثبات این موضوع ادعای مطرح شده بر روی دو مدار متفاوت آزمایش شده است.

۷-۲-۱- مدار C17

شکل ۱۴ مدار C17 را که با ۵ حلقه نوسانگر امن شده است نشان می‌دهد. مطلب فوق با طراحی تروجانی از نوع

اول که در بخش ۲-۵- توضیح داده شده‌است، مورد بررسی قرار گرفته است.



شکل ۱۴: مدار C17 با پنج حلقه نوسانگر با الگوریتم پیشنهادی Rajendran [27]

بدین منظور، شرایطی را در نظر بگیرید که تغییر فرکانس منجر به تغییر مقایسه فرکانس‌ها و در نتیجه تغییر دو بیت اول خروجی نشود. فرض کنید که ترتیب سه فرکانس fi، fj و fk به صورت fi<fj<fk باشد. اگر fj تغییر کند ولی ترتیب سه فرکانس عوض نشود، در نتیجه حاصل مقایسه دو بیت اول خروجی تغییر نخواهد کرد و در صورت عدم حضور بیت سوم، این به معنی شکست روش تست می‌باشد. در این بررسی فرکانس حلقه‌های ۱، ۳ و ۵ اندازه‌گیری شد که نتایج آن در جدول ۲ گردآوری شده است.

جدول ۲ : اطلاعات حلقه‌های نوسانگر مدار C17

شماره حلقه	دوره تناوب (PS)	فرکانس (GHZ)	اختلاف فرکانس با حلقه اول	اختلاف فرکانس با حلقه سوم
حلقه اول	190	5.26	0	2.03
حلقه سوم	310	3.23	2.03	0
حلقه پنجم	225	4.45	0.81	1.22
حلقه پنجم با حضور تروجان	240	4.16	1.1	0.93

در ابتدا روابط زیر برقرار بودند:

$$|f5-f3|>|f5-f1| \text{ و } f3<f5<f1 \qquad (۱۵)$$

در این صورت اگر سیگنال کنترلی مالتی پلکسرها به گونه‌ای باشد که خروجی مالتی پلکسرها به ترتیب f5،f1 و f3 باشند، آنگاه بیت اول و بیت دوم خروجی برابر ۱ و بیت سوم برابر صفر خواهند شد. بعد از افزودن تروجان در حلقه شماره ۵، فرکانس f5 تغییر کرده و روابط زیر برقرار هستند.

$$f3<f5^*<f1 \text{ و } |f5-f3|<|f5-f1| \qquad (۱۶)$$

با توجه به رابطه بالا به دلیل عدم تغییر ترتیب فرکانس‌ها، بیت‌های اول و دوم همچنان برابر ۱ خواهند ماند ولی بیت سوم تغییر کرده و برابر ۱ خواهد شد به عبارتی دقت اندازه‌گیری حداقل برابر e در رابطه ۱۷ خواهد شد.

$$\begin{cases} fj \xrightarrow{change} fj+e \\ if\ (e<\dfrac{\|(fk-fj)|-|(fj-fi)\|}{2} \longrightarrow trojanun\ \det ected \end{cases} \qquad (۱۷)$$

دقت اندازه‌گیری در آزمایش انجام شده برای حالتی که خروجی سه بیت باشد، در مقایسه با وقتی که خروجی دو بیت باشد بیش از ۵ برابر است. هدف از قرار دادن دو بیت اول علاوه بر یک تست اولیه، افزایش حالت‌های ممکن قابل وقوع و در نتیجه کاهش احتمال حملات به سخت‌افزار تست است. در نتیجه با راه‌حل‌های گفته شده هر دو پارامتر Δd_i و Δe_i کاهش یافته‌است.

۲-۲-۷- مدار 74LS181

به منظور اثبات ادعای مدار پیشنهادی و تعمیم آن به سایر مدارها، علاوه بر مدار آزمایشی C17، مدار پیچیده‌تر و پرکاربرد 74LS181 برای انجام آزمایش انتخاب شده و سه مسیر از این مدار با قرادادن حلقه نوسانگر امن شدند. شکل ۱۵ مدار اصلی و مسیرهای انتخاب شده را نشان می‌دهند. در این مدار نیز فرکانس هر سه مسیر اندازه-گیری شده و در مسیر سوم تروجان نوع اول بخش ۵،۲ تعبیه گردید. نتایج آزمایش انجام شده در جدول ۳ نمایش داده شده‌است.

جدول ۳ : اطلاعات حلقه‌های نوسانگر مدار 74LS181

شماره حلقه	دوره تناوب (PS)	فرکانس (GHZ)	اختلاف فرکانس با حلقه دوم	اختلاف فرکانس با حلقه سوم
حلقه اول	510	1.96	0.44	0.59
حلقه دوم	657	1.52	0	1.03
حلقه سوم	392	2.55	1.03	0
حلقه اول با حضور تروجان	487	2.05	0.53	0.50

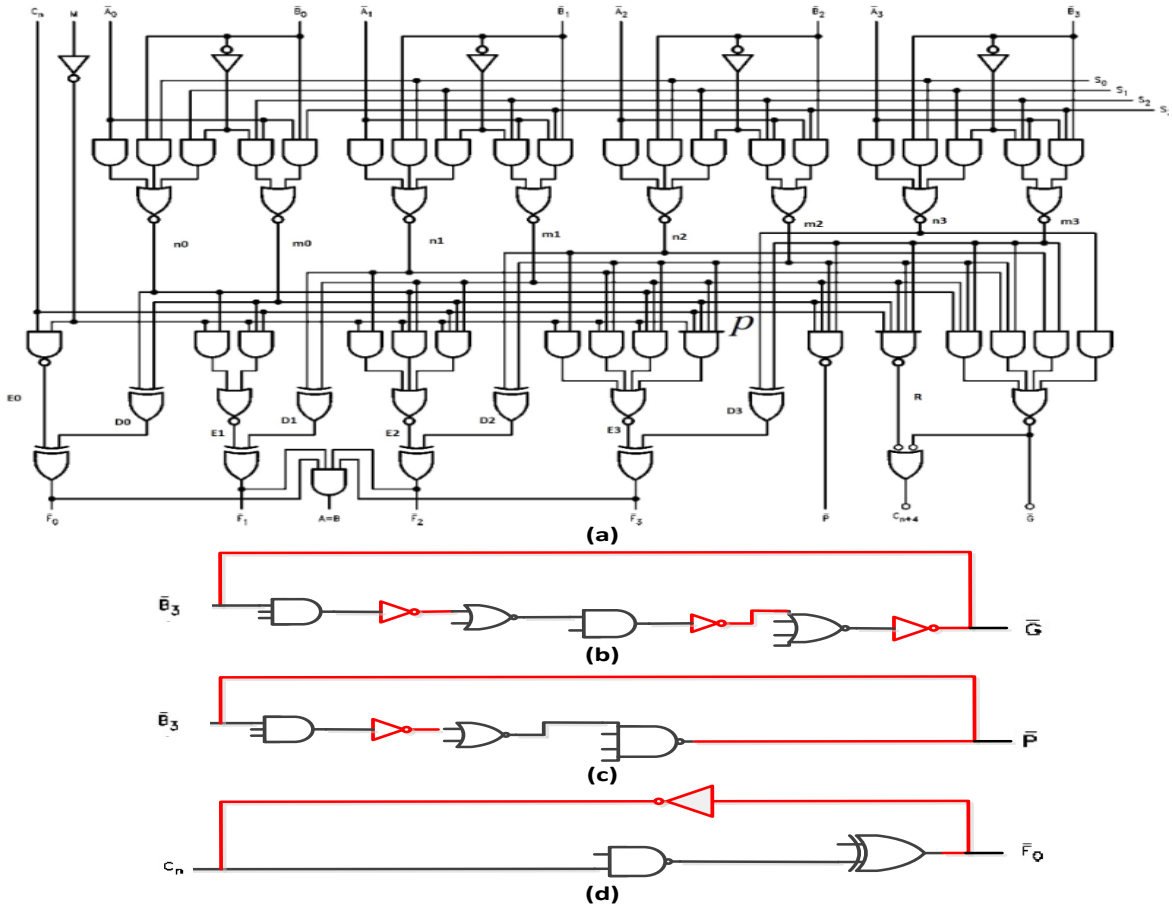
در ابتدا روابط زیر برقرار بودند:

$$f2<f1<f3 \quad \text{و} \quad |f1-f3|>|f1-f2| \qquad (۱۸)$$

در این صورت اگر سیگنال کنترلی مالتی پلکسرها به گونه‌ای باشد که خروجی مالتی پلکسرها به ترتیب f1،f3 و f2 باشند، آنگاه بیت اول و بیت دوم خروجی برابر ۱ و بیت سوم برابر صفر خواهند شد. بعد از افزودن تروجان در حلقه شماره 1 فرکانس f1 تغییر کرده و روابط زیر برقرار هستند.

$$F2<f1*<f3 \quad \text{و} \quad |f1-f3|<|f1-f2| \qquad (۱۹)$$

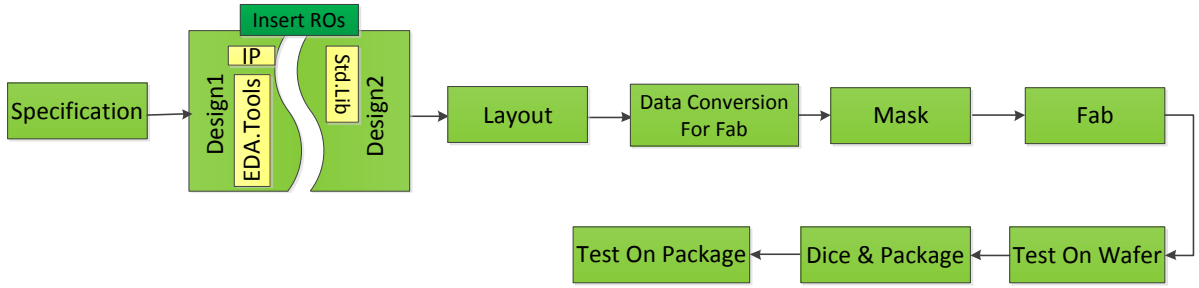
با توجه به رابطه بالا به دلیل عدم تغییر ترتیب فرکانس‌ها، بیت‌های اول و دوم همچنان برابر ۱ خواهند ماند ولی بیت سوم تغییر کرده و برابر ۱ خواهد شد.



شکل ۱۵: a) مدار 74LS181 b) حلقه اول c) حلقه دوم d)حلقه سوم

۳-۷- امن کردن مرحله طراحی

مدار پیشنهادی که با استفاده از حلقه‌های نوسانگر روشی برای کشف تروجان سخت‌افزاری ارائه داد، برای امن ساختن و تشخیص تروجان در مراحل بعد از طراحی کارامد می‌باشد و همچنان مرحله طراحی مستعد حضور تروجان سخت‌افزاری خواهد بود. نویسندگان مقاله به منظور رفع این مشکل تمهیدی برای این مرحله پیشنهاد داده‌اند. به این صورت که مرحله طراحی به چندین فاز شکسته شود، به طوری که هر مرحله به مرحله بعدی مرتبط بوده و در عین حال هر مرحله توسط طراح مجزا و بدون ارتباط با فازهای دیگر انجام شود. بدین صورت احتمال تعبیه تروجان سخت‌افزاری در مرحله طراحی نیز کاهش می‌یابد. شکل ۱۶ امنیت مراحل مختلف ساخت یک مدار مجتمع پس از اعمال طرح‌های پیشنهادی را نشان می‌دهد.



شکل ۱۶: امن شدن مراحل ساخت مدارمجتمع پس از اعمال طرح‌های پیشنهادی

۸- نتیجه‌گیری

در این پژوهش ابتدا تروجان‌های سخت‌افزاری و نقش آن‌ها در حمله به سیستم‌های امنیتی مورد بررسی قرار گرفته و دسته‌بندی انواع آن‌ها ارائه شده است. روش‌های کشف و راه‌های مقابله با این تروجان‌ها از نظر امنیت سیستم‌های سخت‌افزاری، نرم‌افزاری، رمزنگاری و در کل امنیت داده، روز به روز حائز اهمیت بیشتری خواهد شد. به همین دلیل در این مقاله پس از معرفی و دسته‌بندی راه‌های کشف و مقابله با تروجان، با توجه به ساختار حلقه نوسانگر، سخت‌افزار جدیدی توسط نویسندگان مقاله پیشنهاد شد که با استفاده از فرکانس این حلقه‌های نوسانگر و با دقت بالا یک رشته بیت واحد برای هر سخت‌افزار تولید می‌کند که در صورت وجود تروجان این رشته بیت تغییر کرده و تروجان کشف خواهد شد. دقت روش پیشنهادی با اثبات بر روی دو مدار با کاربردهای گوناگون و قابلیت تعمیم به سایر مدارها به اثبات رسید. همچنین با بررسی عوامل موثر بر فرکانس حلقه نوسانگر و پیشنهاد حلقه نوسانگر مناسب، رشته بیت تولید شده توسط سخت‌افزار طراحی شده دقت بیشتری داشته و احتمال کشف تروجان افزایش می‌یابد. راه پیشنهادی مبنی بر افزودن حلقه‌های نوسانگر، مراحل بعد از طراحی را امن می‌کند. در آخر نویسندگان راه‌حلی برای امنیت مرحله طراحی نیز پیشنهاد کرده‌اند.

منابع

1. D. Agrawal et al., ‘‘Trojan Detection Using IC Finger printing ,’’Proc. IEEE Symp. Security and Privacy (SP 07), IEEE CS Press, 2007, pp. 296-310.
2. X. Wang et al., ‘‘Hardware Trojan Detection and Isolation Using Current Integration and Localized Current Analysis,’’Proc. IEEE Int’l Symp. Defect and Fault Tolerance of VLSI Systems (DFT 08), IEEE CS Press, 2008, pp. 87-95.
3. R. Rad et al., ‘‘Power Supply Signal Calibration Techniques for Improving Detection Resolution to Hardware Trojans,’’ Proc. IEEE/ACM Int’l Conf. Computer-Aided Design (ICCAD 08), IEEE CS Press, 2008, pp. 632-639.
4. Y. Alkabani and F. Koushanfar, ‘‘Consistency-Based Characterization for IC Trojan Detection,’’ Proc. IEEE/ ACM Int’l Conf. Computer-Aided Design (ICCAD 09), IEEE CS Press, 2009.
5. J. Li and J. Lach, ‘‘At-Speed Delay Characterization for IC Authentication and Trojan Horse Detection,’’ Proc. IEEE Int’l Workshop Hardware-Oriented Security and Trust (HOST 08), IEEE CS Press, 2008, pp. 8-14.
6.Y. Jin and Y. Makris, ‘‘Hardware Trojan Detection Using Path Delay Fingerprint,’’ Proc. IEEE Int’l Hardware-Oriented Security and Trust (HOST 08), IEEE CS Press, 2008, pp. 51-57.
7.S. Jha and S.K. Jha, ‘‘Randomization Based Probabilistic Approach to Detect Trojan Circuits,’’ Proc. 11th IEEE High Assurance Systems Engineering Symp., IEEE Press, 2008, pp. 117-124.
8.F. Wolff et al., ‘‘Towards Trojan Free Trusted ICs: Problem Analysis and Detection Scheme,’’ Proc. Design, Automation and Test in Europe Conf. (DATE 08), ACM Press, 2008, pp. 1362-1365.
9.M. Banga and M. Hsiao, ‘‘A Region Based Approach for the Identification of Hardware Trojans,’’ Proc. IEEE Int’l Workshop Hardware-Oriented Security and Trust (HOST 08), IEEE CS Press, 2008, pp. 40-47.
10. M. Banga and M. Hsiao, ‘‘A Novel Sustained Vector Technique for the Detection of Hardware Trojans,’’ Proc. 22nd Int’l Conf. VLSI Design, IEEE CS Press, 2009, pp. 327-332.
11. G.E. Suh, D. Deng, and A. Chan, ‘‘Hardware Authentication Leveraging Performance Limits in Detailed Simulations and Emulations,’’ Proc. 46th Design Automation Conf. (DAC 09), ACM Press, 2009, pp. 682-687.
12. G. Bloom, B. Narahari, and R. Simha, ‘‘OS Support for Detecting Trojan Circuit Attacks,’’ Proc. IEEE Int’l Workshop Hardware-Oriented Security and Trust (HOST 09), IEEE CS Press, 2009, pp. 100-103.
13. H. Salmani, M. Tehranipoor, and J. Plusquellic, ‘‘New Design Strategy for Improving Hardware Trojan Detection and Reducing Trojan Activation Time,’’ Proc. IEEE Workshop Hardware-Oriented Security and Trust (HOST 09), IEEE CS Press, 2009, pp. 66-73.
14. M. Banga and M. Hsiao, ‘‘VITAMIN: Voltage Inversion Technique to Ascertain Malicious Insertion in ICs,’’ Proc. 2nd IEEE Int’l Workshop Hardware-Oriented Security and Trust (HOST 09), IEEE CS Press, 2009, pp. 104-107.
15. M. Abramovici and P. Bradley, ‘‘Integrated Circuit Security: New Threats and Solutions,’’ Proc. 5th Ann. Workshop Cyber Security and Information Intelligence Research: Cyber Security and Information Challenges and Strategies (CSIIRW 09), ACM Press, 2009, article 55.
16. R.S. Chakraborty, S. Paul, and S. Bhunia, ‘‘On- Demand Transparency for Improving Hardware Trojan Detectability,’’ Proc. IEEE Int’l Workshop Hardware

Oriented Security and Trust (HOST 08), IEEE CS Press, 2008, pp. 48-50
17. J. Rajendran et al., “Reconfiguration of Functional Logic into Trojan Detecting Ring Oscillators and Test-for-Trust Cost Analysis,” to appear in Proc. 29th IEEE VLSI Test Symp. (VTS 11), IEEE CS Press, 2011.
18. I. Verbauwhede and P. Schaumont, ‘‘Design Methods for Security and Trust,’’ Proc. Design, Automation and Test in Europe Conf. (DATE 07), EDA Consortium, pp. 672-677.
19. DARPA, “TRUST in Integrated Circuits (TIC) - Proposer Information Pamphlet”, 2007. [Online]. Available: http://www.darpa.mil/MTO/solicitations/baa07-24/index.html
20. M. Tehranipoor and F. Koushanfar, “A Survey of Hardware Trojan Taxonomy and Detection,” IEEE Design & Test of Computers, Jan. 2010, pp. 10-25.
21. SK. Subideh ALI, R. Subhra, D. Mukhopadhyay, S.Bhunia, "Multi-Level Attacks: An Emerging Security Concern for Cryptographic Hardware," proceedind of IEEE, 2011.
22. Shi-Wen Chen, Ming-Hung Chang, Wei-Chih Hsieh, and Wei Hwang, Fully On-Chip Tempterature,Process,and Voltage Sensors, IEEE 2010.
23. X. Wang, M. Tehranipoor, and J. Plusquellic, ‘‘Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions,’’ Proc. IEEE Int’l Workshop Hardware-Oriented Security and Trust
24. (HOST 08)IEEE CS Press, 2008, pp. 15-19.
25. X.Zhang and M.Tehranipoor,” RON: An On-Chip Ring Oscillator Network for Hardware Trojan Detection” Proc. IEEE 2011.
26. O.C CHEN, R. SHEEN, A Power-Efficient Wide-Range Phase-Locked Loop, IEEE Journalof Solid State Circuits, vol.37, 1, (2002).
27. G. Jovanovi´c, M. Stoj˘cev, Z. Stamenkovic, “A CMOS Voltage Controlled Ring Oscillator with Improved Frequency Stability” SCIENTIFIC PUBLICATIONS OF THE STATE UNIVERSITY OF NOVI PAZAR SER . A: APPL. MATH. INFORM. AND MECH. vol. 2, 1 (2010), 1-9.
28. J. Rajendran et al., “Reconfiguration of Functional Logic into Trojan Detecting Ring Oscillators and Test-for-Trust Cost Analysis,” to appear in Proc. 29th IEEE VLSI Test Symp. (VTS 11), IEEE CS Press, 2011.
29. Y. Jin and Y. Makris, “Hardware Trojan Detection Using Path Delay Fingerprint,” IEEE Int.Hardware-Oriented Security and Trust(HOST),2008.
۳۰. صادق حاجی محسنی، دکتر محمدعلی دوستاری، دکتر محمد باقر غزنوی قوشچی "تروجان‌های سخت‌افزاری، شناخت آن‌ها، دسته‌بندی، پیاده‌سازی و راه‌های مقابله" چهارمین کنفرانس فناوری اطلاعات و دانش، دانشگاه صنعتی بابل، خرداد ۱۳۹۱

در سال ۱۹۸۵ پاراسورامان [1] و همکاران در یک