بسمه تعالی

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر
مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

معرفی تروجان‌های سخت‌افزاری، چالش‌ها و روش‌های مقابله

مستند مرجع

نوع سند ..... مستند مرجع
شماره نگارش ۱
تاریخ نگارش ۱۴۰۲/۰۷/۲۶

تهران، خیابان شهید بهشتی- بین بزرگراه شهید مدرس و خیابان احمد قصیر- پلاک۲۶۷
(۰۲۱) ۸۸۱۱۵۷۰۵ (۰۲۱) ۸۸۱۱۵۷۲۴ cert.ir

چکیده:

امروزه با توجه به فراگیر بودن استفاده از تراشه‌های دیجیتال در سیستم‌های مختلف و نیاز مبرم به تولید سالانه میلیون‌ها تراشه روش برونسپاری و توزیع فرایند ساخت برای کوتاه کردن بازه طراحی تا تولید و کاهش هزینه‌ها مورد توجه قرارگرفته است. باوجود مزیت‌های مذکور، این روش تولید تراشه‌های دیجیتال منجر به ایجاد حفره-های امنیتی شده است که افراد مهاجم برای قرار دادن تروجان‌های سخت‌افزاری در داخل تراشه از آن بهره می برند. با توجه به وجود میلیون‌ها گیت منطقی (چند میلیارد ترانزیستور) در تراشه‌های دیجیتال مدرن، معمولا امکان آزمودن تمامی بخش‌ها برای کشف وجود تروجان امکان‌پذیر نمی‌باشد، لذا بهره بردن از روش‌های طراحی بر مبنای امنیت که از همان مراحل نخست امکان قراردادن تروجان‌ها در مدار را کاهش می دهد، می‌تواند بسیار کارا باشد.

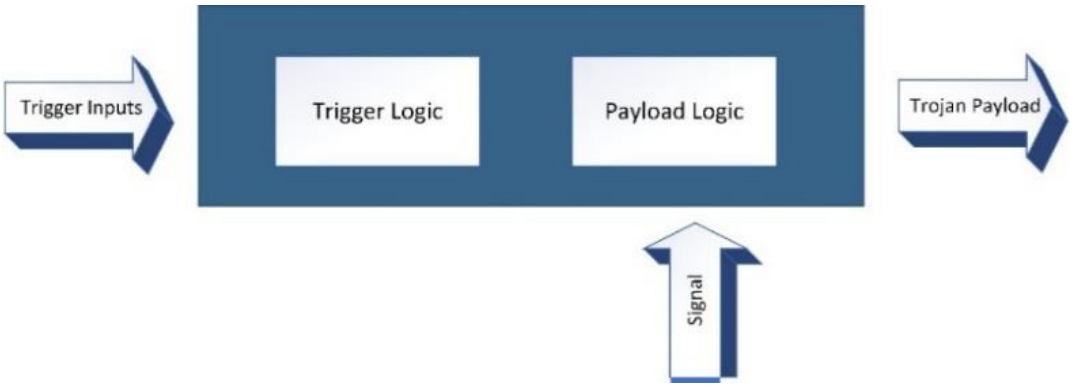
. با توجه به اهمیت بسیار زیاد تراشه‌های دیجیتال در سیستم‌های حساس، بررسی جنبه‌های امنیتی سخت‌افزار جهت جلوگیری از هرگونه نشت اطلاعاتی یا شکست سیستم ضروری به‌نظر می‌رسد. در این نوشتار سعی برآن است که ضمن معرفی ساختار تروجان های سخت‌افزاری که از جمله مهمترین تهدیدات امنیتی در سطح سخت‌افزار سیستم‌ها می‌باشند، روش‌های مختلفی که برای آشکارسازی وجود آن ها در تراشه‌ها و همچنین روش‌های طراحی مبتنی بر امنیت به صورت مختصر معرفی شوند. در پایان چالش‌ها و همچنین رهیافت‌های پیش‌رو در زمینه‌ی تعامل با تروجان‌های سخت افزاری مورد بحث قرار می‌گیرد.

۱-شناخت تروجان‌های سخت افزاری

صنعت ساخت تراشه های دیجیتال در دهه های اخیر به صورت چشمگیری توسعه یافته است و عملکرد بسیاری از سیستم های مدرن (از سامانه های صوتی و تصویری تا ماشین های خودران) وابسته به تراشه هایی است که در قلب سیستم های پردازشی آنها قرار دارند. از دیدگاه امنیت، حملات برمبنای سخت افزار می تواند منجر به نشت اطلاعات در سیستم‌های با درجه امنیت بالا (مانند زیرساخت‌های اینترنتی) و یا شکست در واحدهای کنترلی مربوط به سیستم های بسیار حساس (مانند هواپیماها) شوند. مشهورترین نوع حملات برمبنای سخت افزار، تروجان های سخت افزاری می باشند [۱]. تروجان‌های سخت‌افزاری شامل تغییرات مخرب در عملکرد مورد انتظار مدارهای سخت‌افزاری می‌باشد. این تغییرات برای طراح سخت‌افزار، ناشناس و نامطلوب می‌باشد و معمولا تاثیرات مخرب بر عملکرد کل سیستم دارد[۲]. سه شاخص اصلی تروجان های سخت‌افزاری عبارتند از هدف خرابکارانه، گریز از آشکارشدن و به ندرت فعال شدن. هدف مشترکی بین تمام انواع تروجان‌های سخت-افزاری وجود دارد: انجام فعالیت‌های مخرب در راستای به چالش کشیدن محرمانگی، یکپارچگی و سندیت تراشه‌ی سخت‌افزاری [۳]. این عملکرد می‌تواند منجر به کاهش طول عمر سخت‌افزار (مثلا از ۱۰ سال به ۲ سال) و یا شکست کامل سیستم در هنگام فعال‌سازی تروجان شود. همچنین از دیگر اهداف قراردادن تروجان-های سخت‌افزاری آن است که عامل مهاجم بتواند به نحوی مخفیانه به سیستم دسترسی پیدا کند و یا به نشت اطلاعات محرمانه (مانند کلیدهای مربوط به الگوریتم‌های رمزنگاری سیستم) منجر شود. این امر درنهایت منجر به آسیب رساندن به شهرت کارخانه سازنده تراشه دیجیتال خواهد شد.

در گذشته در ساختار یک سیستم دیجیتال فرض براین بود که بستر سخت‌افزاری موجود کاملا قابل اطمینان است و تنها عدم اطمینان ناشی از حمله به بستر نرم‌افزاری سیستم می‌شود که بر روی سخت‌افزار سوار است[۴]. درحال حاضر با دخالت انواع مختلف تروجان‌های سخت‌افزاری، اطمینان به لایه سخت‌افزار نیز دچار خلل جدی شده است. تمام عناصری (مانند کارکنان، تیم طراحی، زنجیره تامین و ...) که در مراحل مختلف تولید تراشه‌ی دیجیتال دخالت دارند، می‌توانند به عنوان عامل تهدید سخت‌افزاری محسوب شوند. لذا طراحی با رویکرد ایجاد امنیت در تراشه‌های دیجیتال باید به عنوان یک گفتمان غالب در تمام فرایند طراحی تا ساخت مورد توجه قرار گیرد.

توجه به دو نکته در مورد تروجان‌های سخت‌افزاری ضروری به‌نظر می‌رسد. نخست تفاوت آن با نقص‌ها و خطاهای ایجاد شده در تراشه می‌باشد که به صورت ناخواسته بوجود می‌آیند. این درحالی ست که تروجان‌های سخت‌افزاری به صورت عمدی توسط عامل مهاجم در ساختار تراشه قرارداده می‌شوند. نکته‌ی دیگر درمورد تفاوت تروجان‌های سخت‌افزاری و نرم‌افزاری می باشد. تروجان‌های نرم‌افزاری معمولا بعد از آشکارسازی با استفاده از روش‌های نرم‌افزاری از بین می‌روند، در حالی که امکان از بین بردن تروجان‌های سخت‌افزاری حتی پس از آشکارشدن وجود ندارد و لذا هزینه‌ی بسیار بیشتری را به سیستم تحمیل می‌کنند [۵].



شکل ۱- ساختار کلی تروجان های سخت افزاری

تروجان‌های سخت‌افزاری به‌صورت کلی از دوبخش تریگر و بار مفید (payload) تشکیل شده‌اند (شکل ۱). تریگر معمولا با رخداد حالت بسیار نادری در وضعیت مدار دیجیتال فعال می شود و به بخش بار مفید اجازه می‌دهد که شروع به انجام عملیات مخرب کند. اندازه تروجان‌های سخت‌افزاری می‌تواند نسبت به اندازه کل مدار دیجیتال کوچک (در حد چند ترانزیستور) یا بزرگ (صداها ترانزیستور در تراشه‌های پیچیده) باشد[۶]. تروجان‌های سخت‌افزاری انواع گوناگونی دارند و تریگر آن‌ها با استفاده از مدارهای ترکیبی و یا ترتیبی و یا مخلوطی از هردو نوع مدار انجام می‌شود همچنین در بعضی از تراشه‌ها از تریگرهای آنالوگ نیز استفاده می‌شود. بخش بارمفید نیز می‌تواند به صورت مدار دیجیتال یا آنالوگ طراحی شود و در هنگام فعال شدن، اثر مخرب خود را برروی عملکرد تراشه بجای بگذارد.

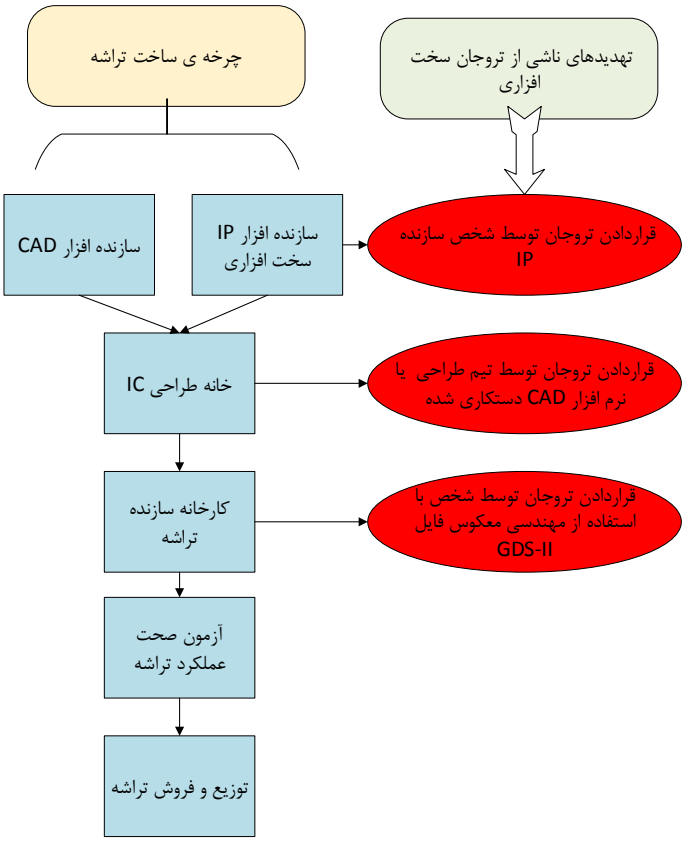
تروجان‌های سخت‌افزاری معمولا به وسیله‌ی فرآیندهای آزمودن مدارهای دیجیتال قابل آشکارسازی نیستند که دلیل آن عدم تمرکز این روش‌های آزمون برروی عملکرد ویژه‌ای از مدار است. از طرفی دیگر آزمودن تمام عملکردهای مدار با توجه به پیچیدگی تراشه‌های دیجیتال مستلزم صرف هزینه و زمان بسیار است. معمولا تروجان‌های سخت‌افزاری در گره‌هایی با فعالیت بسیار پایین قرارداده می‌شوند که احتمال مشاهده‌پذیری آن‌ها در زمان اجرای آزمون‌های عادی بسیار کم است[۷]. روش‌های خاصی برای آشکارسازی تروجان‌های سخت-افزاری مورد استفاده قرار می‌گیرند که تعدادی از آنها مخرب (مانند مهندسی معکوس) و تعدادی غیر مخرب (مانند بررسی کانال‌های جانبی) می باشند. همچنین در بسیاری از روش‌های آشکارسازی، فرآیند نیازمند استفاده از تراشه‌ی طلایی (بدون تروجان) می‌باشد که خود هزینه‌ی اضافی را تحمیل می‌کند[۸].

۱-۱- فرآیند ساخت تراشه و خطرپذیری در برابر تروجان های سخت افزاری

در دهه‌های گذشته تغییرات عمده‌ای در سیاست‌های شرکت‌های سازنده تراشه‌های الکترونیکی صورت پذیرفته است. در ابتدای دوران ساخت تراشه‌ها معمولا تمام مراحل طراحی، ساخت و پکیج‌بندی در یک مجموعه‌ی بسیار بزرگ صنعتی انجام می‌شد و لذا با توجه به کنترل‌های شدید در این مجموعه تقریبا اطمینان کامل در مورد امنیت سخت‌افزار ایجاد می‌شد. اما به تدریج برای کاهش هزینه‌های ساخت و همچنین کاهش زمان ارائه

محصولات جدید به بازار، برون‌سپاری به عنوان یک سیاست جدید در صنایع ساخت تراشه‌ها ظهور کرد. در حال حاضر بسیاری از شرکت‌های فعال در زمینه‌ی طراحی دیجیتال به صورت fabless عمل می‌کنند، یعنی پس از تکمیل طراحی و انجام بهینه‌سازی‌های لازم نهایتا لی‌اوت[1] حاصل به کارخانه‌های بزرگ سازنده تراشه مانند TSMC[2] فرستاده می‌شود و بدین ترتیب نگرانی شرکت‌های طراح از توسعه کارخانه‌های تولید تراشه (با هزینه‌های چند میلیارد دلاری) با تکنولوژی به‌روز و همچنین نگرانی بابت ایجاد خطا در فرآیند ساخت برطرف می‌گردد[۹].

غیر متمرکز شدن مراحل طراحی و ساخت تراشه‌های دیجیتال، علی‌رغم صرفه‌های اقتصادی و تجاری منجر به ازبین رفتن اطمینان امنیتی در بخش سخت‌افزار سیستم می‌شود. این امر حتی برای شرکت‌های طراحی سخت‌افزار که از هسته‌های ازپیش طراحی شده بوسیله شرکت‌های دیگر (3PIP[3]) استفاده می‌کنند، به مراتب بحرانی‌تر می‌شود. در شکل ۲ مراحل تولید تراشه‌های سخت‌افزاری و چگونگی امکان قراردادن تروجان‌های سخت‌افزاری در مراحل مختلف نشان داده شده است [۳].



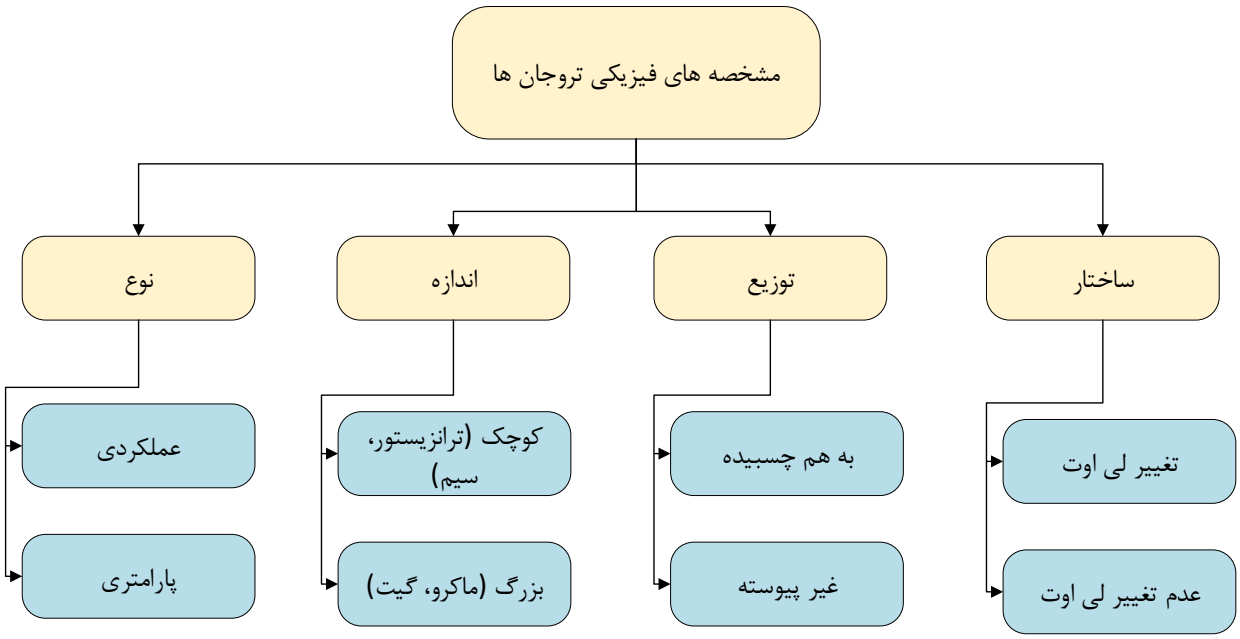
شکل ۲- مراحل ساخت تراشه و امکان قرارگیری تروجان در مراحل مختلف

[1] layout
[2] Taiwan Semiconductor Manufacturing Company
[3] Third Party Intellectual Property

۲-۱ دسته بندی انواع تروجان های سخت افزاری در تراشه های دیجیتال

به طور کلی تروجان‌های سخت‌افزاری بر اساس سه قاعده دسته‌بندی می‌شوند: مشخصه‌های فیزیکی، مشخصه-های فعالسازی و مشخصه‌های عملکردی[۱۰]. ما در ادامه به بررسی این سه دسته می‌پردازیم.

دسته‌بندی تروجان‌ها براساس ویژگی‌های فیزیکی بر مبنای چهار مشخصه‌ی نوع، اندازه، نحوه‌ی پراکندگی و ساختار انجام می‌شود (شکل ۳). در مورد مشخصه‌ی *نوع*، تروجان‌ها به دو دسته‌ی عملکردی و پارامتری تقسیم-بندی می‌شوند. در نوع عملکردی تعدادی از گیت‌های منطقی یا سایر اجزاء به‌گونه‌ای تغییر می‌یابند که در هنگام فعال شدن تروجان عملکرد مورد نظر فرد مهاجم را در تراشه ایجاد کنند. ولی در نوع پارامتری، معمولا تغییر ساختار انجام نمی‌شود، بلکه با تغییر پارامترهای فیزیکی ترانزیستورها و سیم‌های مدار اصلی (مانند ضخامت سیم‌ها و یا تغییر نسبت عرض به طول ترانزیستورها) برروی عملکرد تراشه در زمان اجرا تاثیر گذاشته می‌شود.



شکل ۳- مشخصه‌های فیزیکی تروجان های سخت افزاری

در مورد مشخصه اندازه، تروجان‌ها به دو نوع کوچک (سیم و ترانزیستور) و یا بزرگ (مانند ماکروبلاک و گیت) تقسیم بندی می‌شوند. نوع بزرگ تروجان‌ها معمولا منجر به تخریب بزرگتر در سیستم می‌شود ولی امکان آشکارسازی آن به دلیل ایجاد سربار زیاد در توان مصرفی آسانتر است. در مقابل تروجان‌های کوچک اثر نامطلوب کمتری بر روی تراشه دارند و نیز امکان آشکارسازی آن‌ها با روش‌های معمولی بسیار سخت‌تر است.

مشخصه‌ی توزیع، مربوط به نحوه‌ی قرارگیری اجزاء تشکیل دهنده‌ی تروجان سخت‌افزاری در سطح تراشه می‌باشد. توزیع به‌هم چسبیده[4] به معنای قرارگیری منابع سخت‌افزاری تروجان در کنارهم در سطح تراشه و توزیع غیرپیوسته[5] مربوط به پراکنده بودن اجزای مختلف تروجان در موقعیت‌های مختلف است. معمولا انتخاب توزیع منابع سخت‌افزاری تروجان با توجه به لی‌اوت نهایی مدار صورت می‌گیرد.

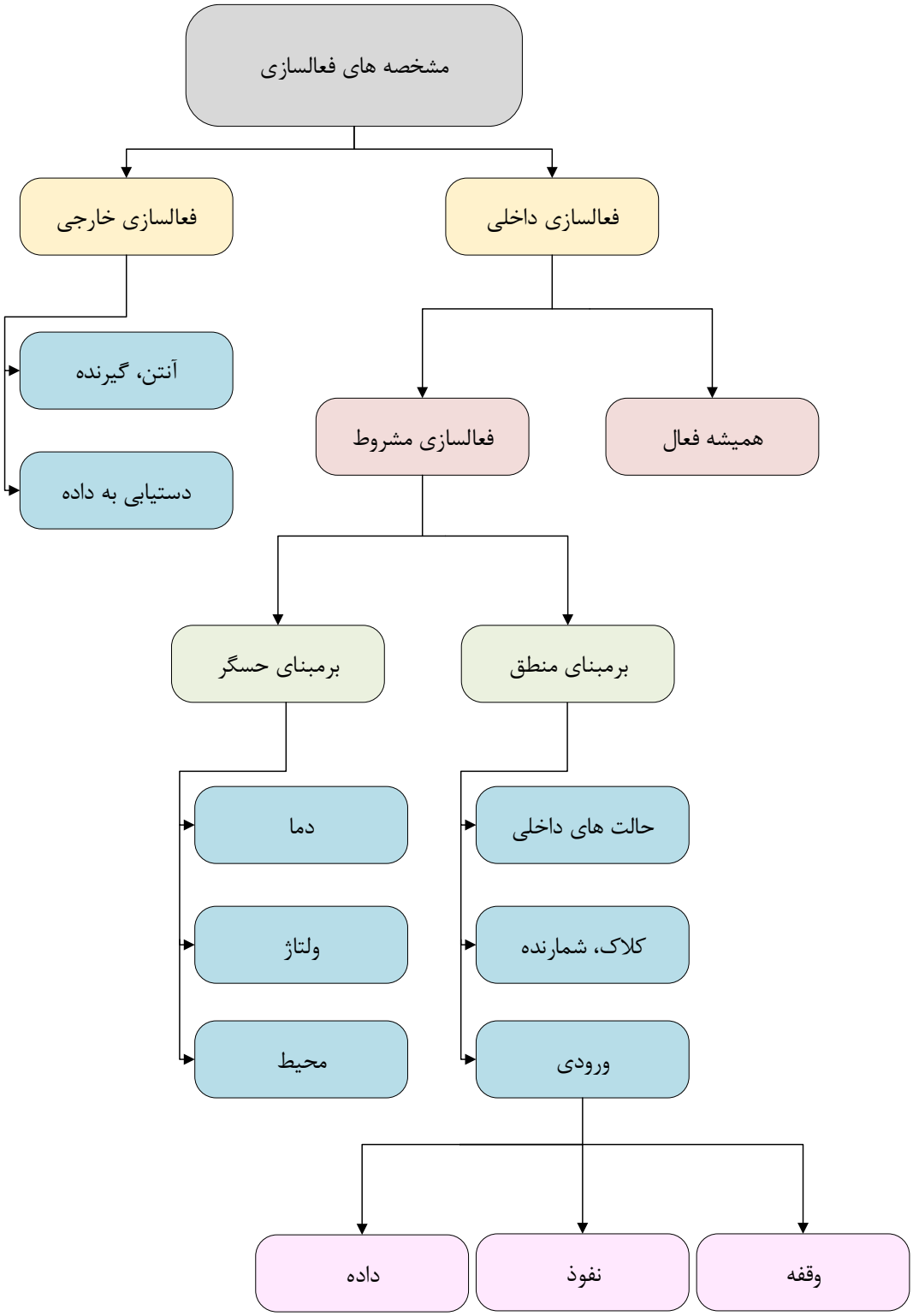
مشخصه ساختار تروجان‌های سخت‌افزاری ناظر به این مساله است که قرارگیری تروجان‌ها منجر به تغییر لی‌اوت اصلی مدار می‌شود یا نه. معمولا تغییر لی‌اوت مدار اصلی منجر به تغییر شاخصه‌های مختلف تراشه مانند توان مصرفی و تاخیر در مدار پیاده‌سازی شده می‌گردد و لذا امکان آشکارسازی تروجان را افزایش می‌دهد. بنابراین عنصر مهاجم سعی می‌کند از تغییر لی‌اوت تاحد ممکن بپرهیزد. اگر فضاهای خالی گسترده‌ای در سطح تراشه موجود نباشد، از تروجان‌ها با اندازه‌ی کوچکتر استفاده می‌شود و یا سعی می‌شود که تروجان‌ها با توزیع غیرپیوسته در سطح تراشه پیاده‌سازی شوند[۱۱].

دسته بندی تروجان‌های سخت‌افزاری بر اساس فرآیند فعالسازی به صورت نشان داده شده در شکل ۴ انجام می‌شود. در نوع فعالسازی خارجی، عمل تریگر کردن بارمفید در تروجان از طریق یک یا چند پایه تراشه انجام می‌شود و وظیفه‌ی فعالسازی در این روش به کاربر مهاجم سپرده می‌شود. ارتباط با تراشه می‌تواند از طریق انتشار سیگنال تریگر و دریافت آن توسط سیستم آنتن بخش گیرنده باشد و یا می‌تواند از طریق دسترسی داده بر بستر شبکه‌های مخابراتی/اینترنتی انجام پذیرد.

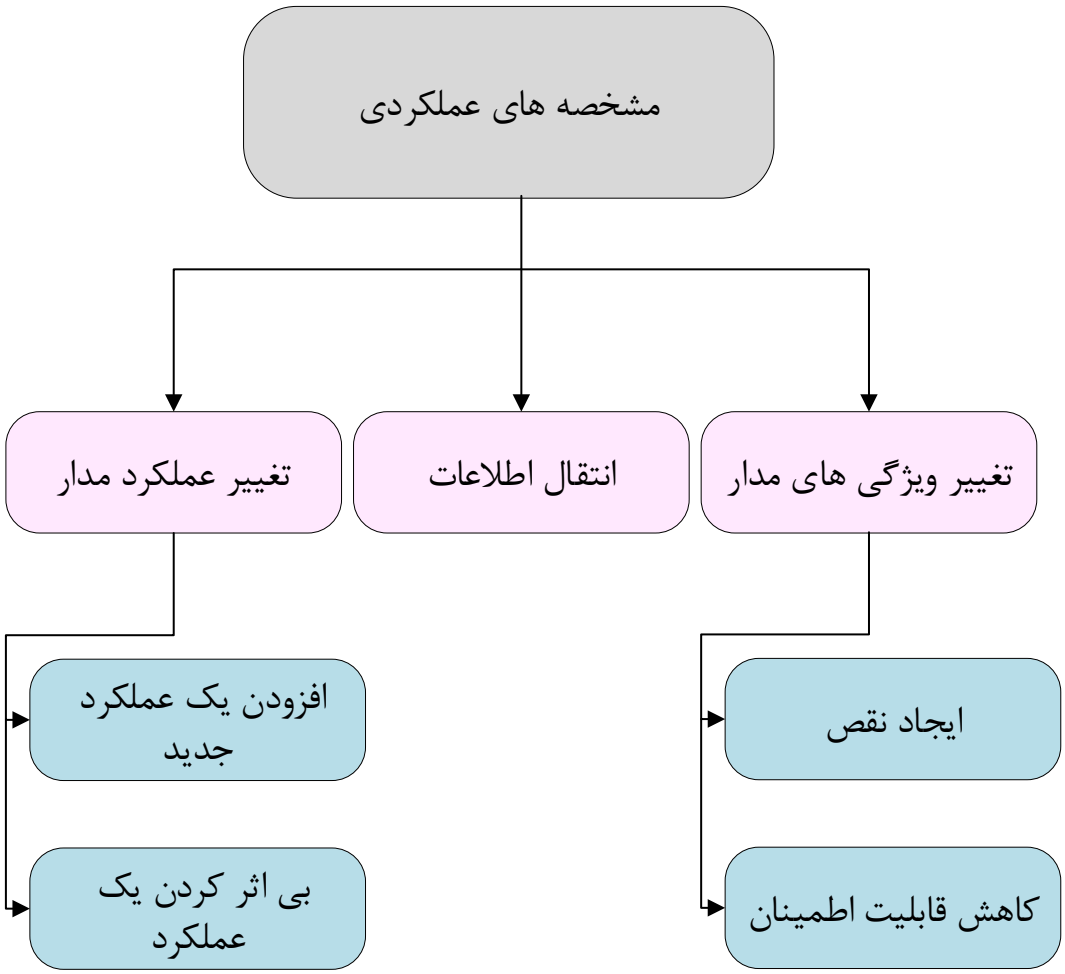
در نوع فعالسازی داخلی، شرایط فعالسازی از طریق بررسی وضعیت داخلی مدار دیجیتال استخراج می شود. تروجان‌های این دسته خود به دو زیرگروه تقسیم‌بندی می‌شوند. دسته ی اول تروجان های همیشه فعال هستند. تغییر نسبت عرض به طول ترانزیستورها و یا عرض سیم ها، از جمله تروجان های همیشه فعال هستند که تنها در صورتی برعملکرد مدار تاثیر مخرب می‌گذارند که شرایط الکتریکی لازم برای آن ها فراهم گردد. دسته‌ی دوم از تروجان ها که بسیار هوشمندانه‌تر عمل می‌کنند فعالسازی شرطی دارند. این نوع تروجان ها برای فعال شدن منتظر می مانند که مدار دیجیتال وارد حالت خاصی از عملکرد خود شود و یا گره های خاصی از مدار، مقدار منطقی خاصی به خود بگیرند. بر اساس نوع شرایط تریگر شدن، این تروجان ها به دو نوع حسگر-مبنا و منطق-مبنا تقسیم بندی می شوند. در نوع تریگر حسگر-مبنا، تروجان سخت افزاری با استفاده از داده های دریافتی حسگر (مانند: دما، فشار ، ولتاژ، رطوبت و ...) شروع به فعالیت می کند. درتروجان های منطق-مبنا، تریگر به صورت هوشمندانه ای وضعیت رجیسترها و مقدار منطقی گره‌های خاصی از مدار را زیرنظر دارد و به محض فراهم شدن شرایط، دستور لازم برای فعالیت قسمت بار مفید را در سخت افزار تروجان تولید می کند. نمونه های از این نوع تروجان را در شکل ۴ نشان داده شده است.

---

[4] tight
[5] loose



شکل ۴- مشخصه‌های نحوه‌ی فعالسازی تروجان های سخت افزاری



شکل ۵- مشخصه‌های نوع فعالیت تروجان های سخت افزاری

در شکل ۵ دسته بندی تروجان های سخت افزاری براساس نوع عملکرد آنها نشان داده شده است. در زیر گروه تغییر عملکرد، تروجان های سخت افزاری با حذف کردن بخشی از مدار منطقی و یا غیرفعال کردن بخشی از مدار، سعی در ایجاد خطا در عملکرد تراشه و یا ایجاد نقص در ساختار مدار را دارند. همچنین بعضی از آن ها می توانند با اضافه کردن بخشی به منطق مدار عملکردهای ناخواسته ای را به کل تراشه تحمیل کنند. در زیرگروه تغییر مشخصه، تروجان‌ها با تغییر در ویژگی های فیزیکی مدار سعی در ایجاد نقص در عملکرد مدار و یا تغییر در تاخیر و قابلیت اطمینان تراشه‌ی دیجیتال را دارند. در نهایت در زیرگروه انتقال اطلاعات، تروجان های سخت افزاری بدون ایجاد تغییر در عملکرد مدار سعی دارند با استفاده از راهکارهای مخفیانه اطلاعات امنیتی سیستم (کلیدها در رمزنگاری) را دزدیده و برای فرد مهاجم ارسال کنند.

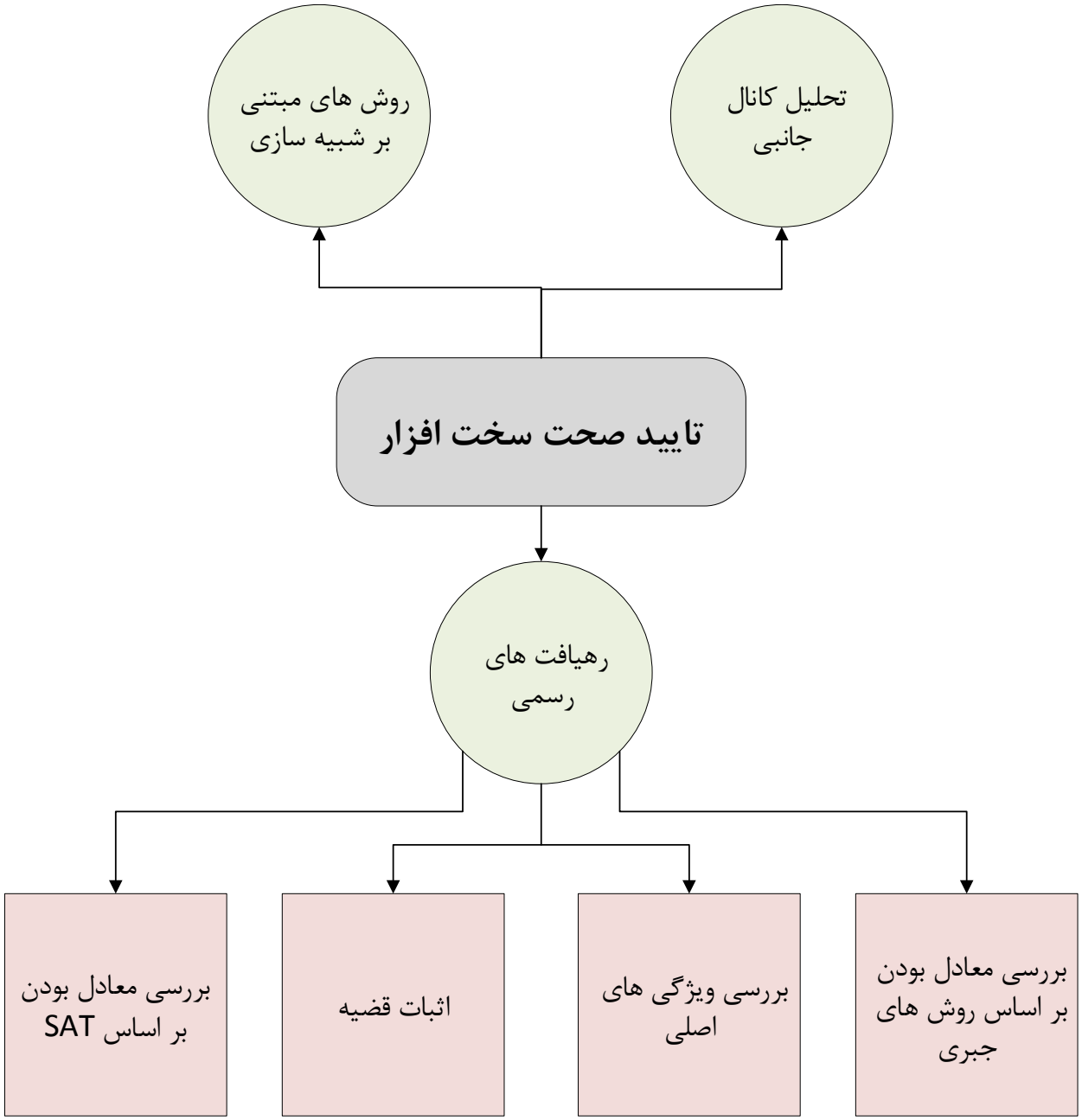
۲- آشکارسازی تروجان های سخت افزاری

۲-۱ آشکارسازی با استفاده از آزمون مدارهای دیجیتال

در روش های مبتنی بر استفاده از آزمون مدارهای دیجیتال، برای آشکارسازی تروجان های سخت‌افزاری، ابتدا گره هایی از مدار که احتمال فعالسازی بسیار پایینی دارند، شناسایی می‌شوند. همان‌گونه که پیشتر گفته شد، این گره‌ها معمولا به عنوان تریگر در پیاده‌سازی تروجان‌های سخت‌افزاری مورد استفاده قرار می‌گیرند. در مرحله‌ی بعد، بردارهای آزمونی که توانایی کنترل مقدار منطقی این گره‌ها را دارند، شناسایی می‌شوند و آن دسته از بردارهای شناسایی شده که قابلیت تغییر منطق حداقل یکی از خروجی‌های مدار را داشته باشند، به عنوان برداری که قادر به آشکارسازی تروجان تریگر شده با گره موردنظر است، معرفی می‌گردد[۱۲].

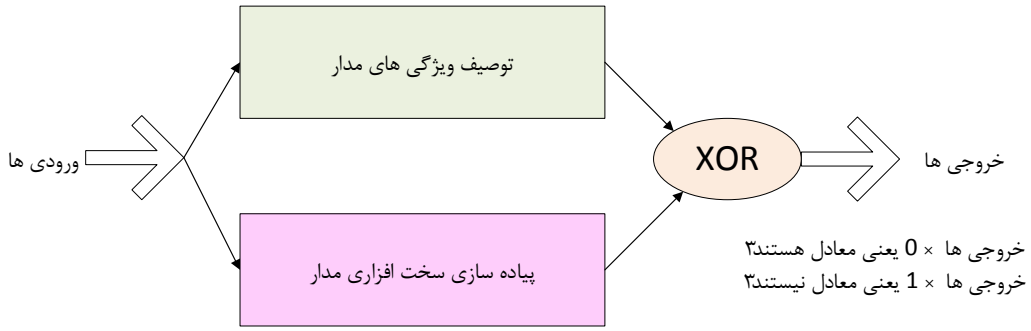
از جمله مشکلات پیش‌روی روش‌های آشکارسازی تروجان برمبنای آزمون مدارهای دیجیتال می‌توان به پیچیدگی یافتن بردارهای آزمونی که توانایی کنترل گره‌های با فعالیت پایین را دارند، اشاره کرد. این مشکل هنگامی بغرنج‌تر می‌شود که طراح تروجان سخت‌افزاری به‌جای استفاده از یک گره با فعالیت کم، از ترکیب چند گره معمولی (با فعالیت متوسط) برای ساختن سیگنال تریگر استفاده کند. از سوی دیگر، برای آشکارسازی تروجان فقط فعال کردن تریگر کافی نیست و باید اثر بار مفید از طریق ایجاد مسیر مناسب به یکی از خروجی-های اصلی مدار رسانده شود[۱۳].

از سوی دیگر استفاده از روش های درستی سنجی مدارهای دیجیتال، می تواند به آشکارسازی رفتار نامطلوب (که معمولا ناشی از وجود تروجان های سخت افزاری) است، منجر شود. روش های به کار رفته برای درستی سنجی مدارهای دیجیتال در شکل ۶ نشان داده شده است.



شکل ۶- روش‌های درستی سنجی سخت‌افزارها

روش تشخیص معادل بودن بر مبنای SAT: هدف این روش آن است که با استفاده از ابزارهای Boolean Satisfiability بررسی شود که آیا عملکرد مدارپیاره سازی شده با عملکرد ویژگی های مورد انتظار یکسان است یا نه. استفاده از ابزارهای مذکور مستلزم تغییر سیستم نشان داده در شکل ۷ به یک مدل رسمی (CNF) است که قابل فهم توسط SAT-solver باشد[۱۴].



شکل ۷- سیستم چند بخشی برای درستی سنجی سخت افزار

روش آزمون ویژگی های تروجان: در این روش یک ابزار بررسی مدل[۶]، رفتار تروجان سخت افزاری در طی چند تغییر حالت متناهی از مدار را بررسی می کند، که درصورت مشاهده چنین رفتاری اعلام می کند که وجود تروجان موردنظر در تراشه کشف شده است[۱۵].

روش اثبات قضایا: در این روش بر اساس تعدادی اصول موضوعه و قضایای بنیادی، ابزار توسعه داده شده سعی می کند که وجود تروجان سخت افزاری را با تعریف یک قضیه و تلاش برای اثبات آن کشف کند.

روش تشخیص معادل بودن بر مبنای جبر نمادها: در این روش مدار پیاده سازی شده و بخش ویژگی های مورد انتظار، با استفاده از تئوری Grobner به دو چندجمله ای تبدیل می شوند و از جبر نمادها برای بررسی معادل بودن این چند جمله ای ها استفاده می شود. در صورت کشف معادل نبودن این دو چندجمله ای وجود تروجان در ساختار مدار پیاده سازی شده آشکار می شود.

در روش های معمولی برای آشکارسازی تروجان‌های سخت افزاری باید یک، به اصطلاح، تراشه‌ی طلایی وجود داشته باشد که از نبودن تروجان در آن اطمینان کامل داشته باشیم. ولی در عمل با توجه به زنجیره‌ی توزیع شده طراحی و ساخت تراشه‌های دیجیتال، تولید چنین تراشه‌های طلایی تقریبا غیرممکن است. در مرحله طراحی به دلیل وجود اعضای متعدد تیم طراحی ممکن است تروجان سخت افزاری توسط یکی از اعضا به‌گونه‌ای در لی‌اوت گنجانده شود که مراحل آزمون و درستی سنجی را به سلامت طی کند. از طرف دیگر با فرض خالی از تروجان بودن طراحی تراشه، در مرحله تولید در کارخانه ممکن است تروجان سخت افزاری در پیاده‌سازی نهایی قرارداده شود. بنابراین تضمین وجود تراشه‌های طلایی به سختی امکان‌پذیر است. هرچند می‌توان با انجام انواع آزمون‌های سخت‌گیرانه و اعمال انواع روش‌های آشکارسازی درصدد تعیین یک تراشه به عنوان تراشه‌ی طلایی برآمد. لیکن تضمین عدم وجود تروجان سخت‌افزاری با توجه به تنوع آن‌ها و شرایط مختلف برای تریگر کردن آن‌ها همواره این ترس را ایجاد می‌کند که تروجان موردنظر از آزمون‌های اعمال شده به سلامت عبور

[6] Model Checking

کرده باشد. این مشکلات سبب شده است که پژوهشگران به دنبال راه‌های آشکارسازی تروجان‌های سخت‌افزاری بدون استفاده از تراشه‌های طلایی باشند. در ادامه به بعضی از این روش‌ها اشاره خواهد شد.

در دسته‌ی اول از روش‌های بدون تراشه‌ی طلایی، از مهندسی معکوس و استفاده از تصویربرداری لایه به لایه‌ی لی‌اوت برای تشخیص وجود تروجان در تراشه استفاده می‌شود. روش دیگر تحلیل ارجاع به خود است که در آن در زمان‌های مختلف مقدار جریان، ولتاژ و حتی تاخیر در بخش‌های مختلف تراشه اندازه‌گیری می‌شوند و از تغییرات ایجاد شده در این مشخصه‌ها برای تشخیص وجود تروجان در سطح تراشه استفاده می‌شود. البته در این نوع اندازه‌گیری‌ها باید عامل تغییرات جزئی به دلیل وجود "تغییرات ناشی از فرآیند ساخت[۷]" توجه شود که با اثر ناشی از تروجان اشتباه گرفته نشوند. معمولا برای رفع این مشکل از مدارهای ساده‌ای به نام PCM[8] استفاده می‌شود که از نوسان‌سازهای حلقه‌ای تشکیل می‌شوند و با توجه به فرکانس کار آن‌ها می‌توان میزان تغییر ناشی از فرآیند ساخت را به‌صورت تقریبی تخمین زد. یک روش برای آشکارسازی تروجان‌های سخت‌افزاری در سطح یک تراشه، کاشت حسگرهای تاخیر و توان مصرفی در نقاط مختلف تراشه است. این حسگرها کاملا مستقل از مدار طراحی شده می‌باشند و به راحتی قادر هستند که اطلاعات مربوط به تاخیر و توان مصرفی در نقاط مختلف تراشه را جمع‌آوری و به مرکز کنترل، جهت بررسی انتقال دهند. این تغییرات در صورتی که از میزان تغییر مربوط به تغییر ناشی از فرآیند ساخت فراتر رود، معمولا به عنوان فعال شدن تروجان سخت‌افزاری لحاظ خواهند شد[۱۶].

۲-۲- آشکارسازی با استفاده از کانال های جانبی

کانال‌های جانبی به تکنیک‌های دسترسی و اندازه‌گیریی اشاره دارد که از روش‌های معمولی -که در آن‌ها از ورودی-خروجی تراشه‌ها انجام می‌شوند- استفاده نمی کنند. کانال‌های جانبی می‌توانند برای آشکارسازی تروجان‌های سخت‌افزاری مورد استفاده قرارگیرند. برای مثال جریان نشتی (I_{DDQ}) و یا جریان گذرا (I_{DDT}) همان‌طور که پیشتر برای آشکارسازی وجود نقص‌های مختلف در تراشه‌ها مورداستفاده قرارگرفته‌اند، می‌توانند به عنوان کانال‌های جانبی برای آشکارسازی تروجان‌های سخت‌افزاری نیز مورد استفاده واقع شوند[۱۷].

سیگنال‌های مربوط به کانال‌های جانبی، معمولا آنالوگ هستند و می‌توانند با قدرت تفکیک بسیار بالا اطلاعات مربوط به زمان‌بندی گره‌های مدار و سایر اطلاعات رفتاری آن‌ها را نشان دهند. به عنوان مثال اندازه‌گیری I_{DDT} منعکس‌کننده شاخصه‌ی کارایی هرکدام از گیت‌های منطقی در هنگام عبور یک سیگنال گذرا از مسیرهای مشخص مدار هستند. این‌گونه اندازه‌گیری‌ها می‌تواند با استفاده از مقایسه با عملکرد قابل انتظار گیت‌ها، که معمولا از طریق شبیه‌سازی بدست می‌آید، منجر به آشکارسازی تروجان‌های سخت‌افزاری گردد [۱۷].

---

[7] process variations
[8] Process Monitor Control

از جمله کانال‌های جانبی، اندازه‌گیری تاخیر مسیرها در تراشه می‌باشد که اگر با دقت کافی انجام شود، می‌تواند به آشکارسازی تروجان‌ها منجر شود. یکی از ویژگی‌های اصلی این کانال جانبی آن است که به صورت خاص برروی گیت‌هایی که در یک مسیر خاص هستند، تمرکز می‌کند و می‌تواند در مشخص کردن مکان تروجان نیز کارا باشد. چالش عمده‌ای که این کانال جانبی با آن مواجه است، تغییرات تاخیر مسیرها بر اساس تغییر ناشی از فرآیند ساخت است که باید به دقت از تغییرات مربوط به وجود تروجان‌ها تفکیک گردد. برای رفع این مشکل تکنیک‌های مختلفی ارائه شده است که از جمله‌ی آنها می‌توان به مدلسازی تغییر ناشی از فرآیند ساخت و دخالت مدل موردنظر در محاسبات اندازه‌گیری تاخیر مسیرها و کشف میزان تاثیر تغییر ناشی از فرآیند ساخت برروی تاخیر گیت‌ها در بخش‌های مختلف مدار با قراردادن نوسان‌سازهای حلقه‌ای (RO) و نمایشگرهای کنترل فرآیند (PCM) در جاهای مختلف سطح تراشه اشاره کرد[۱۸-۱۹].

۳-۲- آشکارسازی با استفاده از مهندسی معکوس

مهندسی معکوس تراشه‌های دیجیتال عبارت از تحلیل ساختار داخلی آن برای استخراج شماتیک و یا دستیابی به اطلاعات داخلی ذخیره شده است. مراحل مختلف فرآیند مهندسی معکوس که معمولا به صورت خودکار انجام می‌گیرد، عبارت است از [۲۰]:

- کپسول برداری: در این مرحله تراشه‌ی سیلیکونی از پکیج که دورتا دور آن قرار گرفته می‌شود، جدا می‌گردد.
- لایه‌برداری: در این مرحله با استفاده از فرآیند شیمیایی خاصی، لایه‌های مختلف تراشه جدا می‌شوند.
- عکسبرداری: در این مرحله با استفاده از دوربین‌های ESM[۹] عکس‌هایی با قدرت تفکیک بسیار بالا از لایه‌ی موردنظر گرفته می‌شود. هر عکس به بخش کوچکی از لایه اختصاص دارد که در آخر عکس‌ها با دقت بالایی در کنار هم قرار می‌گیرند تا عکس یک لایه کامل شود. هنگامی که عکس‌های همه‌ی لایه‌ها تهیه شد، با قرارگیری آنها روی‌هم می‌توان به اتصالات بین لایه‌ای مانند Via ها دسترسی پیدا کرد.
- حاشیه نویسی: مکان، اندازه و نوع اجزاء تشکیل دهنده‌ی تراشه در لایه‌های مختلف به صورت دستی و یا خودکار برروی فایل‌های مربوطه ثبت می‌گردند.

[9]Electrochemical Strain Microscopy

- تولید شماتیک: در مرحله آخر با استفاده از خروجی مرحله حاشیه نویسی و سایر اطلاعات، شماتیک کل تراشه تولید و جهت بازتولید و یا استخراج اطلاعات مختلف مورد استفاده قرار می‌گیرد.

استفاده از مهندسی معکوس جهت آشکارسازی تروجان‌های سخت‌افزاری با اعمال پنج مرحله بالا بر روی تراشه و سپس مقایسه شماتیک استخراج شده با شماتیک تراشه‌ی طلایی انجام می‌گیرد. بدلیل وقت‌گیر بودن و مخرب بودن این روش، استفاده از این روش به موارد خاصی از جمله استخراج شماتیک تراشه‌ی طلایی محدود می‌شود. در بعضی از روش‌های مبنی بر مهندسی معکوس، سه مرحله‌ی اول برای استخراج عکس‌های لایه‌های مختلف تراشه اعمال می‌شود و دو مرحله‌ی آخر حذف می‌شود که منجر به صرفه‌جویی در هزینه و زمان خواهد شد. از عکس‌های استخراج‌شده، برای آموزش Classifier هایی مانند SVM[10] استفاده می‌شود. از جمله مزایای روش آشکارسازی بر مبنای مهندسی معکوس را عدم نیاز به تراشه‌ی طلایی و توانایی آن در آشکارسازی تروجان‌های کوچک و پارامتری که معمولا به وسیله‌ی روش‌های دیگر قابل آشکارسازی نمی‌باشند اشاره کرد [۲۰].

۳-طراحی برای امنیت

در این بخش به بررسی رویکردهای اصلی برای بالا بردن امنیت تراشه‌های دیجیتال در برابر حملات تروجان سخت‌افزاری می‌پردازیم. روش‌های مذکور معمولا در مرحله‌ی طراحی به کاربرده می‌شوند و مانند سپری، تراشه را در برابر حملات امنیتی در مراحل مختلف محافظت می‌کنند.

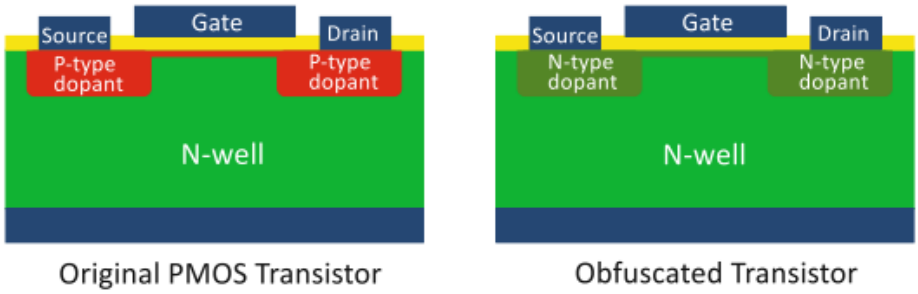
۳-۱ ایجاد ابهام در سخت افزار

ایجاد ابهام در ساختار داخلی یک سیستم به معنای ایجاد تغییراتی در اجزاء آن سیستم است به‌گونه‌ای که تشخیص آسان نحوه‌ی عملکرد آن برای فرد مهاجم را مختل کند. تکنیک‌های متعددی در ابهام سازی نرم‌افزارها مورد استفاده قرار گرفته است که از جمله‌ی آن‌ها می‌توان به تولید معادل ASCII کدهای برنامه مورد نظر اشاره کرد[۲۱]. در مدارهای سخت‌افزاری اخیرا به ابهام سازی جهت مقابله با تروجان‌های سخت‌افزاری توجه بسیاری شده است[۲۱]. هرگونه ابهام سازی در ساختار مدار باید دو شاخصه‌ی زیر را پشتیبانی کند: ۱- مدار دارای ابهام باید عملکرد مدار اصلی را با هزینه صرف زمان بیشتر از مرتبه چندجمله‌ای، داشته باشد. ۲- مدار دارای ابهام فقط باید اجازه نشت اطلاعات در حد استفاده از ورودی-خروجی‌های تراشه را بدهد یا به عبارت دیگر در حد یک جعبه‌ی سیاه باشد.

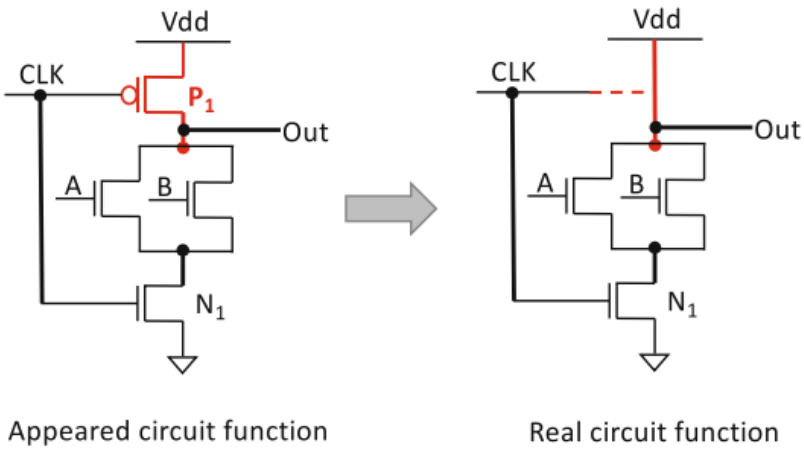
[10] Support Vector Machine

ایجاد ابهام در یک سیستم الکترونیکی در سطوح مختلفی قابل اجرا است که هرکدام نقش بازدارندگی در مقابل قراردادن تروجان‌های سخت‌افزاری با ساختارهای متفاوت را ایفا می‌کنند. با توجه به موضوع کار ما، در ادامه روش‌های مختلف ابهام‌سازی در سطح تراشه خواهیم پرداخت.

در روش‌های مبتنی بر ایجاد ابهام در سطح device (ترانزیستور)، به‌طور کلی ابهام سازی با تغییر ظاهر دادن ترانزیستورها با اعمال نقص‌های کنترل‌شده انجام می‌شود. چنین تغییر ظاهری می‌تواند فرد مهاجم را که از تکنیک‌های مهندسی معکوس جهت پی بردن به عملکرد اجزاء مدار را دارد، فریب دهد. به عنوان مثال در شکل ۸ یک روش ایجاد ابهام با معکوس کردن نوع ناخالصی در ناحیه‌ی درین و سورس یک ترانزیستور PMOS نشان داده شده است. فرد مهاجم با نگاه کردن به تصویر استخراج شده از این ترانزیستور به اشتباه آن را PMOS تشخیص می‌دهد در حالی‌که این قطعه در واقع نقش یک سیم را برای اتصال پایه درین به سورس ایفا می‌کند[۲۲].



شکل ۸- نمونه‌ای از ابهام‌سازی در سطح ترانزیستور [۲۲]



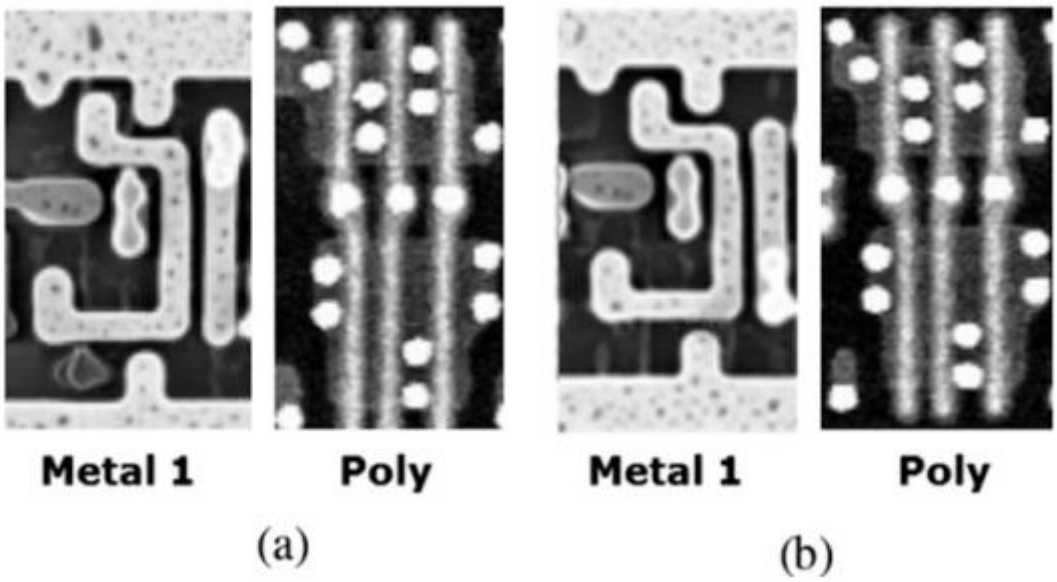
شکل ۹- مثالی از کاربرد ابهام سطح ترانزیستور در یک گیت منطقی [۲۲]

در شکل ۹، یک نمونه از کاربرد این قطعه ابهام دار در ساختار یک گیت نشان داده شده است. فرد مهاجم با دیدن ساختار سمت چپ به این نتیجه می‌رسد که در محل موردنظر یک گیت NAND دینامیک قرارگرفته

است و این در حالی‌ست که ما همواره منطق ۱ را در گره خروجی خواهیم داشت. علاوه بر روش معکوس کردن دوپینگ، از ناحیه‌کانال ترانزیستور، اتصال بین ترانزیستورهای مجاور و ناحیه دی‌الکتریک بین لایه‌های بخش مسیردهی می‌توان برای ایجاد ابهام در سطح قطعه استفاده کرد[۲۳].

ایجاد ابهام در سطح مدار خود به دوصورت انجام می‌گردد: روش استتار لی‌اوت و روش قفل ترانزیستورها. در روش استتار، لی‌اوت مدار به‌گونه‌ای تغییر داده می‌شود که فرد مهاجم با استفاده از عکس‌های SEM گرفته شده از طریق مهندسی معکوس به عملکرد اصلی مدار پی نبرد. اصول اساسی استتار عبارت از آن است که گره‌های متصل به هم به نظر منفک به نظر برسند و گرهای منفک از هم به صورت متصل نشان داده شوند. در این صورت فرد مهاجم به آسانی عملکرد گیت منطقی را اشتباه حدس می‌زند و لذا در ایجاد تریگر مناسب و یا ترکیب گیت‌ها برای ایجاد بارمفید، رویه‌ی اشتباهی را پیش خواهد گرفت.

برای ایجاد ابهام بیشتر معمولا از سلول‌های کتابخانه‌ای که اندازه‌ی مشابه دارند و در همه‌ی آنها استتار اعمال شده است، استفاده می‌شود. این امر به‌کارگیری روش‌های تشخیص ماهیت را برای افراد مهاجم سخت می‌کند. نمونه‌ای از استتار در لی‌اوت یک گیت NAND در شکل ۱۰ نشان داده شده است.



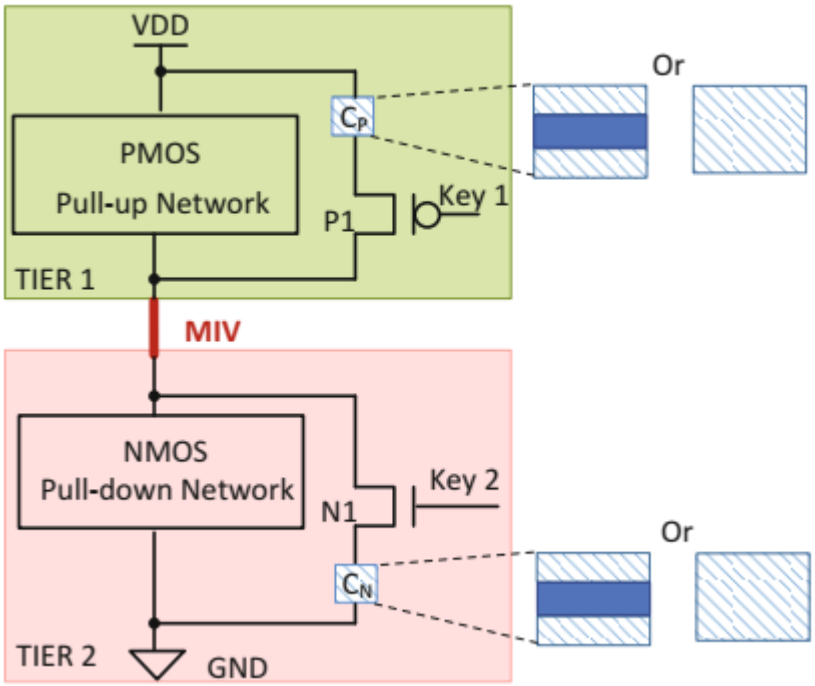
شکل ۱۰- نمونه‌ای از کاربرد استتار برای ابهام‌سازی [۲۲]

در روش قفل ترانزیستورها، از دو کلید متقارن و یا غیر متقارن برای میانبر زدن[11] بخش PUN و PDN در مدار داخلی گیت ها استفاده می شود. تا زمانی که کلید ها به درستی به گیت مورد نظر اعمال نگردد، گیت به

[11] bypass

درستی کار نمی کند و امکان شناسایی آن توسط فرد مهاجم امکان پذیر نمی باشد. نمونه ای از قفل ترانزیستورها در شکل ۱۱ نشان داده شده است[۲۴].

ایجاد ابهام در سطح گیت های منطقی معمولا با استفاده از تکنیک قفل منطقی انجام می شود و می توان آن را مکملی برای فرآیند ایجاد ابهام در سطح مدار معرفی کرد. در این روش ایجاد ابهام، انتقال حالت در مدار به گونه‌ای اصلاح می‌شود که فرد مهاجم نتواند به آسانی به حالتی که موجب تریگر شدن تروجان می شود، دسترسی پیدا کند. فعال سازی تروجان تنها در صورتی انجام خواهد شد که فرد مهاجم بتواند کلیدهایی که با آن فرایند قفل منطقی انجام شده است را درست حدس بزند که با توجه به اعمال الگوریتم های رمزنگاری کارا، امکان کشف کلید به مراتب پیچیده تر از حالت های اعمال شده در سطح مدار است.

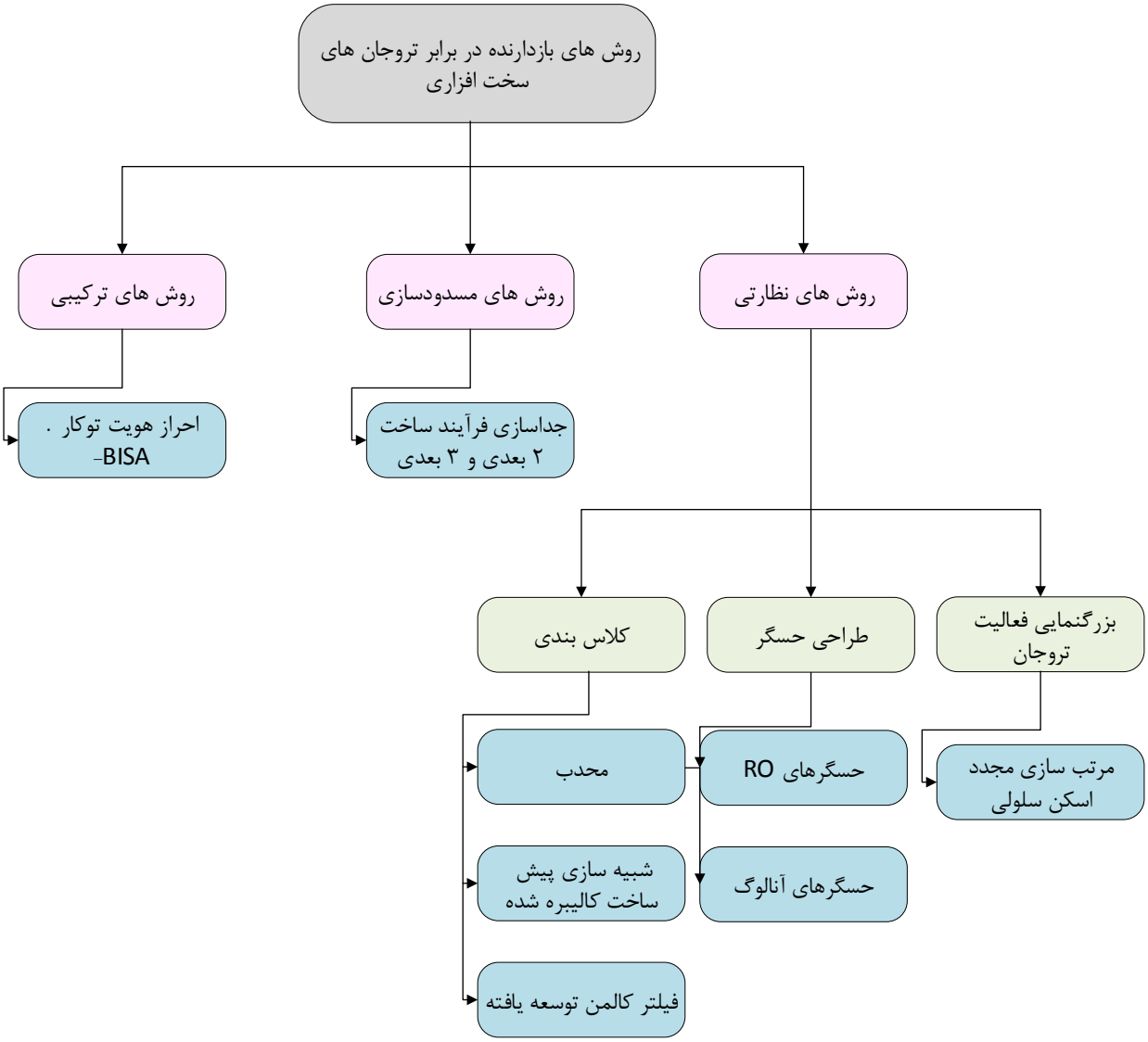


شکل ۱۱- روش قفل ترانزیستورها برای ابهام سازی [۲۴]

۲-۳- روش های بازدارنده برای جلوگیری از قرارگیری تروجان در تراشه ی دیجیتال

روش های بازدارنده به آن دسته از تکنیک هایی اشاره می کند که یا از قراردادن تروجان در تراشه جلوگیری می‌کنند و یا به فرد مهاجم می فهماند که در صورت قراردادن تروجان در سطح تراشه، آن تروجان به آسانی قابل آشکارسازی می‌باشد. روش‌های متعدد بازدارنده‌ای تا به‌حال پیشنهاد شده است که خلاصه‌ی آن را در شکل ۱۲ ملاحظه می‌فرمایید[۲۵].

مشهورترین روش بازدارنده روش نظارتی می‌باشد که از حسگرهای کارگذاشته شده در تراشه برای مشاهده‌ی تغییرات کانال های جانبی (دما و توان مصرفی) -که ناشی از فعالیت گره های مختلف مدار هستند- استفاده می‌کند. داده‌های جمع آوری شده از این حسگرها جهت اعمال به ابزارهای کلاس بندی و آشکارکردن وجود تروجان به کار برده می‌شوند. برای آنکه عملکرد ابزارهای کلاس‌بندی بهبود یابد، باید تغییرات کانال جانبی ناشی از فعالیت تروجان های سخت افزاری نسبت به بقیه مدار اختلاف واضحی داشته باشد. از این رو بهتر است که فعالیت گره‌های اصلی مدار بسیار پایین نگه داشته شود تا آشکارسازی فعالیت تروجان‌ها دقیق‌تر و آسان‌تر انجام گیرد. این عملیات با استفاده از روش "مرتب سازی دوباره مدار اسکن" انجام می‌شود که در آن با استفاده از روش بهینه سازی، فلیپ فلاپ های مناسب برای زنجیره‌ی اسکن به گونه‌ای انتخاب می‌شوند که فعالیت گره های مدار را در یک محدوده پایین نگه دارند[۲۶].



شکل ۱۲- مشخصه‌های فیزیکی تروجان های سخت افزاری

در مقابل روش‌های نظارتی، دسته‌ی دیگری از روش های بازدارنده وجود دارند که امکان قراردادن تروجان های سخت افزاری در سطح تراشه را از بین می برند. یکی از معروفترین روش های مسدودسازی[۱۲] روش جداسازی فرآیند ساخت است که در آن مانع از دستیابی شخص مهاجم یا شرکت مضنون به لی‌اوت کامل تراشه می شوند. دسته‌ی سوم از روش‌های بازدارنده، روش ترکیبی است که از مزایای هر دو روش نظارتی و مسدودسازی بهره می‌برد. در روش BISA تمام فضاهای خالی موجود در سطح تراشه با استفاده از گیت‌های عضو سیستم پر می شوند به گونه‌ای که به فرد مهاجم فضای خالی جهت قراردادن تروجان سخت افزاری را نمی‌دهد. از سوی دیگر در BISA با استفاده از روش‌های نظارتی مانع از برداشتن این گیت ها وخالی کردن فضا برای قرار دادن تروجان می شوند[۲۷].

هرکدام از این روش‌های بازدارنده مزایا و معایب خود را دارند و می توانند برای جلوگیری یا آشکارسازی دسته‌ی خاصی از تروجان‌های سخت افزاری مورد استفاده قرارگیرند. روش نظارتی معمولا نیازمند تراشه‌ی طلایی است تا عملکرد تراشه‌ی تحت آزمایش را با آن مقایسه کند. همان طور که پیشتر بیان شد وجود این تراشه‌های طلایی گاهی غیرممکن و گاهی با صرف وقت و هزینه‌ی بسیار ممکن می‌شود. هرچند روش مسدودسازی این نیازمندی را ندارد، اما نسبت به حملات تروجانی که احتیاج به اطلاعات مربوط به ساختار مدار ندارند، خطرپذیر است. روش ترکیبی نیز نسبت به تروجان‌های سخت افزاری که از سد عامل محافظ آن‌ها عبور می کنند خطرپذیر است.

[12] Obstructive

نتیجه‌گیری و رویکردهای آینده

در این نوشتار سعی شده است که تروجان‌های سخت افزاری و نحوه‌ی عملکرد آن‌ها به صورت دقیق تشریح شود. خطرات ناشی از تروجان‌های سخت‌افزاری مانند ایجاد شکست در عملکرد سیستم، ایجاد خطا در خروجی-های تولید شده توسط تراشه، مصرف توان بیشتر و نشت اطلاعات از طریق کانال‌های جانبی، در زنجیره خطرپذیر تولید تراشه‌های دیجیتال باید مورد توجه قرارگیرند. روش‌های گوناگونی برای آشکارسازی وجود تروجان‌های سخت‌افزاری در تراشه‌ها توسعه داده شده است که ازجمله‌ی آن‌ها می‌توان به روش‌های مبتنی بر آزمون مدارهای دیجیتال، استفاده از کانال‌های جانبی (مانند توان مصرفی و یا جریان فعال مدار) و مهندسی معکوس اشاره کرد. همچنین طراحان تراشه‌های دیجیتال سعی می‌کنند با استفاده از روش‌های طراحی مبنی بر امنیت، میزان خطرپذیری این قطعات را نسبت به حملات تروجانی کاهش دهند. از جمله‌ی این روش‌ها می‌توان به ابهام سازی در سطوح مختلف (از قطعات ترانزیستوری تا مدارهای پیاده‌سازی شده) و استتار اشاره کرد.

با پیچیده‌تر شدن معماری تراشه‌های دیجیتال و همچنین تکامل روش‌های تولید و قراردادن تروجان‌های سخت‌افزاری در این نوع تراشه‌ها، پژوهشگران در سال‌های پیش رو با چالش‌های جدی در زمینه آشکارسازی تروجان‌های سخت‌افزاری مواجه خواهند شد. یکی از رویکردهای موثر برای رفع این چالش‌ها توسعه‌ی الگوریتم-های مبتنی بر یادگیری ماشین است که در سال‌های اخیر مورد توجه بسیار قرارگرفته است. این ابزارها قادر به یادگیری رفتار تراشه‌های دیجیتال حاوی تروجان می‌باشند و در نتیجه قادر هستند که در صورت مشاهده لی‌اوت مدار مجتمع به آشکارسازی تروجان اقدام کنند. از سوی دیگر بحث تولید ابزارهای طراحی مدار با رویکرد درنظرگرفتن جنبه‌های امنیتی یکی از زمینه‌های پژوهشی در آینده خواهد بود. این ابزارها باید مجهز به روش‌های آشکارسازی و جلوگیری از قراردادن تروجان‌ها در مراحل مختلف باشند. همچنین توسعه‌ی این ابزارها باید به‌گونه‌ای باشد که خود در برابر حملات مهاجمین مقاوم باشند. به طور خلاصه طراحان وسازندگان تراشه‌های دیجیتال در آینده باید به جنبه‌ی امنیت مانند سایر معیارهای مهم توجه کنند.

منابع

[1] Hassan, R., Meng, X., Basu, K. and Dinakarrao, S.M.P., 2023. Circuit Topology-aware Vaccination-based Hardware Trojan Detection. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Jan 6 (2023).

[2] Chen, K., Arias, O., Guo, X., Deng, Q. and Jin, Y., 2022. IP-Tag: Tag-Based Runtime 3PIP Hardware Trojan Detection in SoC Platforms. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *42*(1), pp.68-81.

[3] S. Bhunia, M.S. Hsiao, M. Banga, S. Narasimhan, Hardware Trojan attacks: threat analysis and countermeasures. Proc. IEEE 102(8), 1229–1247 (2014).

[4] Guazzelli, R. A., Trindade, M. G., Guimarães, L. A., de Paiva Leite, T. F., Fesquet, L., & Bastos, R. P. (2020). Trojan Detection Test for Clockless Circuits. Journal of Electronic Testing, 1-9.

[5] J. Roy, F. Koushanfar, I. Markov, EPIC: ending piracy of integrated circuits. IEEE Comput. 43(10), 30–38 (2010).

[6] M. Tehranipoor, C. Wang, Introduction to Hardware Security and Trust (Springer, New York, 2012).

[7] M. Tehranipoor, U. Guin, D. Forte, Counterfeit Integrated Circuits: Detection and Avoidance (Springer, Cham, 2015).

[8] R. Torrance, D. James, The state-of-the-art in semiconductor reverse engineering, in IEEE/ACM Design Automation Conference (2011), pp. 333–338.

[9] Y. Zheng, S. Yang, S. Bhunia, SeMIA: self-similarity-based IC integrity analysis. IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 35(1), 37–48 (2016).

[10] X. Wang, M. Tehranipoor, J. Plusquellic, Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions, IEEE International Workshop on Hardware Oriented Security and Trust, 2008, pp. 15–22.

[11] Hasegawa, K., Seira H., Kohei N., Shinsaku K., and Nozomu T.. "R-HTDetector: Robust hardware-Trojan detection based on adversarial training." *IEEE Transactions on Computers* 72, no. 2 (2023): 333-345.

[12] Kok, Chee Hoo, Chia Yee Ooi, Mehrdad Moghbel, Nordinah Ismail, Hau Sim Choo, and Michiko Inoue. "Classification of Trojan nets based on SCOAP values using supervised learning." In 2019 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1-5. IEEE, 2019.

[13] Kurihara, Tatsuki, Kento Hasegawa, and Nozomu Togawa. "Evaluation on hardware-trojan detection at gate-level ip cores utilizing machine learning methods." In 2020 IEEE 26th International Symposium on On-Line Testing and Robust System Design (IOLTS), pp. 1-4. IEEE, 2020.

[14] Khalid, Faiq, Imran Hafeez Abbassi, Semeen Rehman, Awais Mehmood Kamboh, Osman Hasan, and Muhammad Shafique. "ForASec: Formal Analysis of Hardware Trojan-Based

Security Vulnerabilities in Sequential Circuits." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 41, no. 4 (2021): 1167-1180.

[15] S. Kelly, X. Zhang, M. Tehranipoor, A. Ferraiuolo, Detecting hardware trojans using on-chip sensors in an ASIC design. J. Electron. Test. 31(1), 11–26 (2015).

[16] M. Li, A. Davoodi, M. Tehranipoor, A sensor-assisted self-authentication framework for hardware Trojan detection, in Design, Automation & Test in Europe Conference (2012), pp. 1331–1336.

[17] J. Aarestad, D. Acharyya, R. Rad, J. Plusquellic, Detecting Trojans though leakage current analysis using multiple supply pad IDDQs. Trans. Inf. Forensics Secur. 5(4), 893–904 (2010).

[18] D. Rai, J. Lach, Performance of delay-based Trojan detection techniques under parameter variations, in International Workshop Hardware-Oriented Security and Trust, 2009, pp. 58– 65.

[19] X. Zhang, M. Tehranipoor, RON: An on-chip ring oscillator network for hardware Trojan detection, in Design and Test in Europe, 2011.

[20] R. Torrance, D. James, The state-of-the-art in semiconductor reverse engineering, in Proceedings of the 48th Design Automation Conference (ACM, 2011), pp. 333–338.

[21] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, K. Yang, On the (im)possibility of obfuscating programs, in Annual International Cryptology Conference (Springer,2001), pp. 1–18

[22] A. Vijayakumar, V.C. Patil, D.E. Holcomb, C. Paar, S. Kundu, Physical design obfuscation of hardware: a comprehensive investigation of device and logic-level techniques. IEEE Trans. Inf. Forensics Secur. 12, 64–77 (2017).

[23] R.P. Cocchi, J.P. Baukus, L.W. Chow, B.J. Wang, Circuit camouflage integration for hardware IP protection, in Proceedings of Design Automation Conference (DAC), June 2014, pp. 1–5.

[24] J. Dofe, C. Yan, S. Kontak, E. Salman, Q. Yu, Transistor-level camouflaged logic locking method for monolithic 3D IC security, in 2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST), Dec 2016, pp. 1–6.

[25] Y. Liu, K. Huang, Y. Makris, Hardware Trojan detection through golden chip-free statistical side-channel fingerprinting, in Proceedings of the 51st Annual Design Automation Conference, DAC'14 (ACM, New York, 2014), pp. 155:1–155:6.

[26] C. Bao, D. Forte, A. Srivastava, Temperature tracking: toward robust run-time detection of hardware Trojans. IEEE Trans. Comput. Aided Des. Integr. Circuits Syst. 34(10), 1577–1585 (2015).

[27] H. Salmani, M. Tehranipoor, Layout-aware switching activity localization to enhance hardware trojan detection. IEEE Trans. Inf. Forensics Secur. 7(1), 76–87 (2012).