ارزیابی روش‌های شناسایی تروآهای سخت‌افزاری

مؤلف:

علیرضا الطائی کامی

نیکان کتاب

بهار ۹۷

www.ketab.ir

سرشناسه	: لطفی تاکامی، علیرضا، ۱۳۷۲-
عنوان و نام‌پدیدآور	: ارزیابی روش‌های شناسایی تروآهای سخت‌افزاری / مولف: علیرضا لطفی‌تاکامی
مشخصات نشر	: زنجان: نیکان کتاب، ۱۳۹۷.
مشخصات ظاهری	: ۱۱۲ ص.: مصور، جدول، نمودار.
شابک	: ۹۷۸-۹۶۴-۱۹۶-۴۷۸-۰
وضعیت فهرست‌نویسی	: فیپا
یادداشت	: سخت‌افزار
یادداشت	: Computer input-output equipment
موضوع	: کامپیوترها — ایمنی اطلاعات
موضوع	: Computer security
موضوع	: مدارهای مجتمع — راستی‌آزمایی
موضوع	: Integrated circuits -- Verification
رده‌بندی کنگره	: ۱۳۹۷ ۴ الف۶ ل/۵/ TK ۷۸۸۷
رده‌بندی دیویی	: ۶۲۱/۳۹۱۶
شماره کتابشناسی ملی	: ۵۱۲۶۷۶۴

ارزیابی روش‌های شناسایی تروآهای سخت‌افزاری / علیرضا لطفی تاکامی

صفحه‌آرایی: سعید ناصحی بنی‌زاد

طراحی جلد: عرفان فرجی

چاپ و صحافی: فانوس

چاپ اول: بهار ۹۷

تیراژ: ۱۰۰۰ نسخه

قیمت: ۱۲/۰۰۰ تومان

شابک: ۰- ۴۷۸-۱۹۶-۹۶۴-۹۷۸

دفتر نشر:

زنجان، چهارراه سعدی، روبروی بانک پاسارگاد، کوچه باقری، ساختمان [illegible]، واحد ۴

تلفکس: ۲-۳۳۳۳۵۵۴۱-۰۲۴

Email:Nikanketab@yahoo.com

www.chaponashr.ir/nikanketab

www.ketab.ir

پیشگفتار

هر چه که فنّاوری ساخت مدارهای مجتمع[1] به سطوح با اندازه‌های خیلی کوچک نزدیک شد، پیچیدگی و هزینه ساخت مدارهای مجتمع به‌طور چشمگیری افزایش پیدا کرد؛ بنابراین فقط تعداد کمی از شرکت‌ها قادر به انجام تمام مراحل ایجاد یک مدار مجتمع از مرحله طراحی تا ساخت هستند. اکثر شرکت‌های طراح به‌منظور هزینه کمتر ساخت، محصول خود را به شرکت دیگری می‌سپارند که همین امر فرصت را به مهاجمان می‌دهد که تغییرات و خرابکاری‌های خود را در مدارهای مجتمع اعمال کنند. این تغییرات و خرابکاری‌ها به‌عنوان تروآهای سخت‌افزاری[2] شناخته می‌شود. تروآی سخت‌افزاری به مسئله مهمی برای برنامه‌های حیاتی امنیتی تبدیل‌شده است و دلیل این امر آن است که تروآی سخت‌افزاری باعث عملکرد اشتباه مدار مجتمع، قابلیت اعتماد کمتر به مدارهای مجتمع، نشت اطلاعات سری به بیرون و یا حتی نابود شدن سیستمی که تحت شرایط خاصی طراحی‌شده است، می‌شود. تروآ می‌تواند در هر مرحله‌ای (سطح انتقال ثبات تا ساخت) به مدار مجتمع اضافه شود.

هدف این پروژه، ارزیابی سه روش مختلف شناسایی تروآ، بر روی مداری که تروآ در آن گنجانده‌شده، است. درواقع ورودی‌های این پروژه مداری شامل تروآ و سه روش شناسایی تروآ است و خروجی آن مقایسه این سه روش ازنظر میزان توانایی در شناسایی تروآ و سربار واردشده، است. پس از پیاده‌سازی این سه روش بر روی مدار محک s1196 میزان توانایی

---

[1] Integrated Circuits

[2] Hardware Trojans

www.ketab.ir

هرکدام از این روش‌ها در شناسایی HTH مورد ارزیابی قرار گرفت و سرباری که هرکدام از این روش‌ها به مدار وارد می‌کردند محاسبه شد و سپس به مقایسه و ارزیابی آن‌ها پرداخته شد و نهایتاً بررسی شد که هرکدام از این روش‌ها برای چه نوع مداری مناسب‌ترین گزینه خواهد بود.

کلمات کلیدی: اسب تروآی سخت‌افزاری، مدار مجتمع، فلیپ‌فلاپ زائد، ثبات سایه، بردار معلق

www.ketab.ir

فهرست مطالب

پیشگفتار أ

مقدمه ۹

۱ مباحث اولیه درزمینه‌ی HTH ۱۲

۱-۱ تعاریف مفاهیم اولیه ۱۲

۱-۲ اهمیت و خطر HTHها ۱٤

۱-۲-۱ مدل HTH و اجزای آن ۱۵

۱-۲-۲ انواع HTHها ۱٦

۱-۲-۳ سایر مشخصه‌های HTHها ۱۸

۲ HTH طراحی‌شده ۲۲

۲-۱ مشخصه‌های جانبی ۲۲

۲-۲ میزان تأثیرگذاری در چینش تراشه ۲۳

۲-۳ نحوه‌ی برانگیزش ۲۳

۲-۴ نحوه‌ی توزیع ۲۳

www.ketab.ir

۲-۵ ماهیت دیجیتال یا آنالوگ ۲۵

۲-۶ دلیل انتخاب و طراحی این HTH ۲۵

۳ مروری بر برخی از روش‌های کشف HTH **۲۷**

۳-۱ شفاف‌سازی طرح ۲۷

۳-۲ تاریک‌سازی طرح ۲۸

۳-۳ [illegible]پ‌های زائد ۲۹

۳-۴ معکوس [illegible]ازی و [illegible]ز ۲۹

۳-۵ ساختارهایی برای بررسی مشخصه‌ی تأخیر ۳۰

۴ پیاده‌سازی روش فلیپ‌فلاپ زائد **۳۱**

۴-۱ معرفی روش ۳۱

۴-۲ مدار محک انتخابی ۳۲

۴-۳ نوع HTH تعبیه‌شده در مدار ۳۲

۴-۴ به دست آوردن احتمال فعالیت نت‌ها ۳۲

۴-۵ فلیپ‌فلاپ زائد ۳۳

۴-۵-۱ حالت $P_0 >> P_1$ ۳۴

www.ketab.ir

٤-٥-٢ حالت P۰<<P۱ ..... ٣٥

۴-۶ روال پیاده‌سازی ٣٦

نتایج پیاده‌سازی ٣٨

٤-٦-١ سربار واردشده ٤٠

۵ پیاده‌سازی روش ثبات سایه ۴۱

۵-۱ معرفی روش ٤١

۵-۲ مدار محک انتخابی ٤٢

۵-۳ نوع HTH تعبیه‌شده در مدار ٤٣

۵-۴ ثبات سایه ٤٣

۵-۵ روال پیاده‌سازی ٤٤

٥-٥-١ قسمت‌هایی از کد Verilog مدار محک ٤٦

٥-٥-٢ شبیه‌سازی در Model sim ٤٧

۵-۶ نتایج پیاده‌سازی ٥٠

٥-٦-١ سربار واردشده ٥١

www.ketab.ir

۶ پیاده‌سازی روش بردار معلق ۵۳

۶-۱ معرفی روش ۵۳

۶-۲ مدار محک انتخابی ۵۵

۶-۳ نوع HTH تعبیه‌شده در مدار ۵۵

۶-۴ روال پیاده‌سازی ۵۵

۶-۵ نتایج پیاده‌سازی ۵۶

۶-۱-۱ سربار واردشده ۵۸

۷ ارزیابی و مقایسه ۵۹

۷-۱ سربار واردشده به مدار ۵۹

۷-۱-۱ روش فلیپ‌فلاپ زائد ۵۹

۷-۱-۲ روش ثبات سایه ۶۰

۷-۱-۳ روش بردار معلق ۶۰

۷-۱-٤ مقایسه ۶۰

۷-۲ توانایی شناسایی HTH ۶۱

۷-۲-۱ روش فلیپ‌فلاپ زائد ۶۱

www.ketab.ir

۷-۲-۲ روش ثبات سایه ٦٢

۷-۲-۳ روش بردار معلق ٦٢

۷-۲-٤ مقایسه ٦٢

مقایسه‌ی روش‌ها در حالت کلی: ۶۲

مقایسه‌ی روش‌ها بر روی s1146: ۶۳

۸ مراجع ۶۶

پیوست ۶۷

(پ-۱) کد پیمانه‌ی شناسایی کننده ۰۱۰ به زبان verilog ٦٧

(پ-۲) کد پیمانه فلیپ‌فلاپ زائد ٦٨

(پ-۳) معرفی ابزار Design Compiler ٦٩

(پ-۳-۱) محیط کار در ابزار ٦٩

(پ-۳-۲) نحوه‌ی سنتز مدار در ابزار ۷۰

(پ-٤) محاسبه‌ی احتمال فعالیت نت‌ها به زبان جاوا ۷۷

(پ-٥) گزارش تحلیل توان پویا ۷۹

(پ-٥-۱) در حالت کارکرد معمول مدار ۷۹

www.ketab.ir

(پ-۵-۲) در حالت آزمون ۸۱

(پ-٦) گزارش مساحت ۸۱

(پ-٦-۱) گزارش مساحت فلیپ‌فلاپ زائد ۸۱

(پ-٦-۲) گزارش مساحت مدار محک ۸۲

(پ-۷) نحوه‌ی شبیه‌سازی در Model sim ۸۳

(پ-۸) نحوه‌ی کار با ابزار SOC-Encounter ۸۹

(پ-۹) گزارش تحلیل زمان توسط SOC-Encounter ۱۰۲

(پ-۹-۱) در حالت کارکرد معمول مدار ۱۰۲

(پ-۹-۲) در حالت آزمون ۱۰۵

www.ketab.ir