دانشکده مهندسی برق و کامپیوتر

پردیس دانشکده های فنی

بسمه تعالی

جلســه دفاعیه پایان نامه کارشناسی ارشد

گرایش: سیستم‌های الکترونیک دیجیتال

موضوع: مسئله‌ی صدق‌پذیری و کاربرد آن در حفاظت از مدارات مجتمع دیجیتال در برابر مهندسی معکوس

توسط: محمد مرادی شهمیری

استاد راهنما: دکتر بیژن علیزاده ملفه

روز ، ساعت ، تاریخ دفاع: ۱۴۰۲/۶/۵ ساعت ۸ صبح

مکان دفاع: اتاق جلسات ۸۱۴، ساختمان شماره ۲ دانشکده برق و کامپیوتر (ساختمان جدید)

چکیده:

طی دهه‌های اخیر، پیشرفت در ساخت تراشه‌های دیجیتال باعث شده هزینه‌ی تأسیس و بهره‌برداری از کارخانه‌های تولید آن‌ها افزایش چشمگیری پیدا کند. در نتیجه، بسیاری از طراحان به برون‌سپاری تولید محصولاتشان رو آورده‌اند. در این راستا، قفل منطقی به عنوان روشی برای جلوگیری از کپی طرح توسط پیمانکار غیر قابل اعتماد ارائه شده. بدین منظور، طراح تغییراتی در ساختار مدار ایجاد می‌کند که باعث می‌شود مدار تنها در صورتی کارکرد درستی داشته باشد که کلید مناسب در ورودی‌های کلید آن اعمال شود. در سال‌های اخیر حمله‌های مبنی بر یادگیری ماشین بسیاری از قفل‌های منطقی قدیمی را شکسته‌اند. از سوی دیگر، قفل‌هایی که در جواب به این حمله‌ها ارائه شده‌اند، عموما در برابر حمله‌های قدیمی‌تر و مبنی بر SAT آسیب‌پذیرند.

در پاسخ به دو چالش بالا، در این پایان‌نامه قفل منطقی جدیدی به اسم قفل ترکیبی معرفی می‌شود که هم امنیت بالایی در برابر حمله‌های مبنی بر یادگیری داشته و هم در برابر حمله‌های دیگر از طرح حفاظت می‌کند. بدین منظور از دو رویکرد جدید استفاده می‌شود: ۱) قفل‌کردن مدار با استفاده از مالتی‌پلکسر در قالب یک مسئله‌ی بهینه‌سازی با استفاده از صدق‌پذیری بیشینه تعریف می‌شود، به گونه‌ای که همبستگی بین کلید و ویژگی‌های مدار در پاسخ بهینه کم شود. ۲) روشی برای تغییر غیرقطعی در ساختار مدار ارائه می‌شود که امکان ترکیب قفل یادشده با قفل‌های دیگر را فراهم می‌کند. با این روش، امکان تأمین امنیت به شکل هم‌زمان در برابر حمله‌های مبنی بر یادگیری و SAT ایجاد می‌شود.

برای نشان‌دادن اثربخشی قفل ترکیبی، با استفاده از حمله‌های MuxLink، SCOPE و SAT امنیت آن را با قفل DMUX مقایسه کردیم. در مورد حمله‌ی MuxLink، تعداد بیت‌های کلید درست پیش‌بینی‌شده توسط مهاجم به طور متوسط ۴۶٫۰۷٪ کاهش داشت. در تمامی آزمایش‌های حمله‌ی SCOPE تعداد بیت کلید بازیابی‌شده توسط مهاجم کمتر از حدس رندوم بوده و تعداد بیت‌های غیرقابل پیش‌بینی نسبت به DMUX به طور میانگین ۴۵٫۲۸٪ افزایش داشت. با استفاده از حمله‌ی SAT، هیچ‌کدام از مدارهای قفل‌شده با قفل ترکیبی با طول کلید دستکم ۶۴ بیت شکسته نشدند، در حالی که در مورد DMUX بیش از ۵۰٪ کلیدهای ۱۲۸ بیتی هم بازیابی شدند. همچنین سربار ناشی از این دو قفل با معیار تعداد گیت پس از سنتز مقایسه و مشاهده شد که قفل ترکیبی به طور متوسط ۱۱٫۳۳٪ سربار کمتری به مدار اضافه می‌کند. در مجموع، مشاهده شد که قفل ترکیبی با وجود سربار کمتر، امنیت در برابر حمله‌های مختلف را به شکل چشمگیری افزایش می‌دهد.