عنوان مقاله:
ردیابی بدافزارهای سخت افزاری تعبیه شده در یک تراشه FPGA از طریق تحلیل سیگنال تشعشعات الکترومغناطیس تراشه

محل انتشار:
ششمین کنگره ملی تازه های مهندسی برق و کامپیوتر ایران با نگاه کاربردی بر انرژی های نو (سال: 1398)

تعداد صفحات اصل مقاله: 12

نویسندگان:
مهدی نیک آرا - *کارشناس ارشد الکترونیک، دانشگاه آزاد اسلامی واحد تهران شرق*

مجتبی بهرامی - *دانشجوی دکتری مخابرات سیستم، دانشگاه صنعتی شیراز*

خلاصه مقاله:
تروجان سخت افزاری یک مدار اضافی مخرب است که به همراه مدار اصلی و با هدف خاصی پیاده سازی می شود و می تواند عملکرد سخت افزار اصلی را تحت تاثیر قرار دهد. مهاجم می تواند با درج تروجان در مدار، باعث ایجاد اثرات مخربی مانند تغییر کارکرد مدار، نشت اطلاعات محرمانه و کاهش کارآیی مدار شود. دراین مقاله ابتدا به بررسی مفهوم تروجان های سخت افزاری، نحوه دسته بندی و روش های آشکارسازی آنها پرداخته می شود و در ادامه یک تروجان که در حقیقت یک شمارنده 16 بیتی می باشد، با استفاده از زبان توصیف سخت افزاری Verilog طراحی و جهت همگام سازی درون هسته الگوریتم AES قرار داده شد. سپس با بکارگیری روش پیشنهادی که شامل ناحیه بندی سطح تراشه و نمونه گیری از توان مصرفی و تشعشعات الکترومغناطیس تراشه حین عملیات رمزنگاری می باشد، داده های مورد نیاز احصاء و در نهایت با استفاده از روش آزمون T و تحلیل در محیط نرم افزار متلب، تروجان سخت افزاری تعبیه شده ردیابی ومحل فیزیکی آن درتراشه کشف گردید

کلمات کلیدی:
حملات کانال جانبی، تروجان سخت افزاری، آزمون T، الگوریتم رمزنگاری، زبان توصیف سخت افزار