عنوان مقاله:
تحریک فرکانسی، روشی جدید برای فعال سازی تراوژان های سخت افزاری

محل انتشار:
نهمین کنفرانس بین‌المللی انجمن رمز ایران (سال: 1391)

تعداد صفحات اصل مقاله: 6

نویسندگان:
سیدمحمدرضا میرصفای مقدم - *دانشجوی کارشناسی ارشد برق و الکترونیک، دانشکده برق و رایانه و فناوری اطلاعات، دانشگاه آزاد اسلامی، واحد قزوین*

سمیه میرزایی الموتی - *دانشجوی کارشناسی ارشد برق و الکترونیک، دانشکده فنی، دانشگاه گیلان، رشت*

رضا ابراهیمی آتانی - *استادیار گروه مهندسی کامپیوتر، دانشگاه گیلان، رشت، ایران*

خلاصه مقاله:
با توجه به کاربردهای روزافزون تراشه ها برای پردازش و کنترل سیگنال های الکترونیکی مباحث مربوط به امنیت سخت افزاری از اهمیت ویژه ای برخوردار شده است. تروژان های سخت افزاری در حقیقت بلوک ها و یا حتی پردازنده های جاسوسی یا تخریب کننده در داخل تراشه ها می باشند که با امکان فعال سازی از خارج کارکرد درست مدار را تحت تاثیر قرار می دهند. در این مقاله روشی جدید با نام تحریک فرکانسی برای طراحی تروژان رمزنگاری AES_128 قرار داده شده و از برد آزمایشگاهی NSK114 با هسته مرکزی SPARTAN3(XC3S400PQ2008) برای پیاده سازی این الگوریتم استفاده شده است. همچنین با استفاده از نتایج شبیه سازی و پیاده سازی به بررسی و ارزشیابی امنیتی این نوع تروژان از نظر عملکردی، مقاومت در مقابل آزمون های آشکار سازی تابعی، سطح تراشه مصرفی پرداخته شده است. نتایج بدست آمده حاکی از صحت عملکرد این نوع تروژان، مقاومت در مقابل آزمون های آشکار سازی تابعی و همچنین سطح اشغالی پایین آن در FPGA می باشد.

کلمات کلیدی:
تروژان سخت افزاری، امنیت سخت افزاری، رمزنگاری، تراشه های رمزنگاری، تست های تابعی، تحریک فرکانسی