عنوان مقاله:
تابع کپی ناپذیر فیزیکی؛ بررسی ساختار داخلی و حملات به آنها

محل انتشار:
نخستین همایش منطقه ای فناوری اطلاعات (سال: 1392)

تعداد صفحات اصل مقاله: 13

نویسندگان:
فرهاد فرخ پناه - *کارشناسی ارشد گروه علمی مهندسی کامپیوتر*

رضا ابراهیمی آتانی - *دانشکده فنی و مهندسی دانشگاه گیلان*

خلاصه مقاله:
در رمزنگاری سنتی یکروشحفاظت داده، استفاده از حافظه غیر فرار مانندEEPROM و fuseبرای قرار دادن کلید رمز و استفاده از توابع اولیه رمزنگاری مانند امضای دیجیتال است. عیبعمده روشهای معمول برای رمزنگاری این استکه حفاظتایمن از رمزها در یکحافظه دشوار و هزینهبر است.طراحیهایFPGAعمدتا به صورترشته بیتهای قابل ذخیره در حافظههای خارجی مثلPROMیا Flashوجود دارند. وقتیFPGAروشن میشود، یکرشته بیتداخل آن بارگذاری میشود و آن را پیکربندی میکند. در زمان بارگذاری، یکمهاجم میتواند به آسانی این رشته بیترا بردارد و یککپی از آن را تهیه کند و توسط این کپی یکFPGA دیگر را برنامهریزی نماید.PUFs1 توابع جدیدی هستند که برای گرفتن رمزها از مشخصههای فیزیکی پیچیده مداراتمجتمع و ذخیره اطلاعات در حافظه دیجیتال به کار میروند. به عنوان مثال یکرمز فرار میتواند از مشخصههای تاخیر تصادفی سیمها و ترانزیستورها ایجاد شود

کلمات کلیدی:
تابع کپی ناپذیر فیزیکی/PUF؛/حملات مخرب ؛ حملات غیر مخرب

لینک ثابت مقاله در پایگاه سیویلیکا: