عنوان مقاله:
بررسی مدل ها و روش های اندازه گیری در حملات تحلیل توان

محل انتشار:
اولین کنفرانس سراسری توسعه محوری مهندسی عمران، معماری،برق و مکانیک ایران (سال: 1393)

تعداد صفحات اصل مقاله: 11

نویسندگان:
محمدمهدی غفارنسب - *دانشجوی مهندسی مخابرات رمز دانشکده و پژوهشکده مهندسی فناوری اطلاعات وارتباطات گروه رمزوامنیت دانشگاه جامع امام حسین (ع)*

پویا حبیبی ارباستان - *دانشجوی مهندسی مخابرات رمز دانشکده و پژوهشکده مهندسی فناوری اطلاعات وارتباطات گروه رمزوامنیت دانشگاه جامع امام حسین (ع)*

خلاصه مقاله:
یکی ازروشهای نوین دررمزگشایی استفاده ازحملات کانال جانبی است کانال جانبی منبعی ازاطلاعات مرتبط با پیاده سازی فیزیکی توابع رمزنگاری است که استفاده ازحملات کانال جانبی یک راه میان بردرامررمزگشایی است این حملات ازنشت اطلاعات همانند اطلاعات مصرف توان تشعشعات الکترومغناطیسی یازمان محاسبات عملیات رمزنگاری استفاده می کنند تا کلید مخفی رابدست آورند حملات کانال جانبی به علت پیچیدگی کمتر وموثربودن اهمیت زیادی دررمزنگاری پیداکرده اند و تحقیقات درمورد آنها درحال رشد است دراین مقاله مدلهای همینگ را بیان خواهیم کرد و درادامه تنظیمات و موارد موردنیاز جهت حملات تحلیل توان بررسی و نکات مرتبط با این موضوع بیان خواهد شد

کلمات کلیدی:
رمزگشایی ، حملات کانال جانبی ، مدل همینگ ، حملات تحلیل توان