در میان وسیله های رمزنگاری، ابزارهای کوچک مانند حسگرها، برچسب‌های شناسایی با بسامد رادیویی، کارت‌های هوشمند و ... دسته‌ای خاص از رمزنگاری را طلب می‌کنند. این وسیله‌ها دارای محدودیت سه‌گانه حافظه، توان مصرفی و توان محاسباتی هستند. از این رو به دسته‌ای از رمزها که رمزهای سبک نام دارند، نیازمندند. رمزهای سبک به علت ویژگی‌ها و محدودیت‌هایی که دارند در برابر حملات گوناگون از جمله روش‌های تحلیل توانی آسیب‌پذیرتر از الگوریتم¬های رمز متداول هستند. به همین دلیل مقاوم‌سازی آن‌ها در برابر این حملات توجه بیشتری می‌خواهد. تاکنون روش‌های گوناگونی برای مقاوم‌سازی پیاده‌سازی الگوریتم‌های رمزنگاری مختلف، در برابر روش‌های تحلیل توانی ارائه شده¬است. بیشتر این روش‌ها سعی در کاهش همبستگی میان مقادیر میانی و توان مصرفی، با تصادفی کردن مقادیر میانی را دارند. دسته دیگر اما این همبستگی را با ثابت نگاه‌داشتن توان مصرفی کاهش می‌دهند. از جمله ی این ر.ش ها می توان به روش مقاوم سازی با منطق دو ریلی با استفاده از فاز پیش شارژ اشاره کرد. این روش ها در بخش پیش شارژ خود دارای نشت اطلاعات توسط مدل توانی فاصله ی همینگ هستند. از جهت دیگر الگوریتم های رمز قالبی سبک در پیاده سازی بر روی بستر نرم افزار دارای مشکل سیگنال به نویز هستند. به این معنی که در پیاده سازی روش های امن سازی با استفاده از پوشش گذاری، نیازمند سطح سیگنال به نویز پایین می باشند. این در حالی است که غالباً این الگوریتم ها بر روی بستر نرم افزار دارای سطح بالای سیگنال به نویز هستند. لذا ابتدا با اعمال روش های پوشش گذاری تلاش به کاهش این آن می شوند. روش پیشنهادی، با در نظر گرفتن مدل‌های توان، توان مصرفی دستگاه را تا حد امکان ثابت نگاه می‌دارد. می‌دانیم هر الگوریتم رمز را می‌توان با دو عملگر AND و XOR به طور کامل پیاده‌سازی کرد. این روش با انتقال محاسبات به فضای جدید و استفاده از عملگرهای معادل در آن فضا، الگوریتم را به‌گونه‌ای پیاده‌سازی می‌کند که وزن همینگ و فاصله همینگ در هر لحظه از زمان مقادیر ثابتی داشته باشند. این عمل باعث کاهش تغییرات وابسته به داده‌ی پردازش‌شده در توان مصرفی می‌شود. سپس بعد از انجام محاسبات، خروجی کدگشایی می‌شود تا متن رمز شده به دست آید. در این پژوهش، با آماده سازی بستر سخت¬افزاری و نرم افزاری مناسب برای جمع آوری تعداد زیادی نمودارهای توان و اعمال حملات تحلیل توانی تفاضلی و با بررسی موردی الگوریتم رمز متقارن سبک وزن SIMON در حالت‌های امن و ناامن متناظرو پیاده‌سازی آن‌ها روی کارت هوشمند، میزان کارایی و مقاومت حاصله بررسی شده است. به کمک کدینگ پیشنهادی و سه روش برای عملگر-AND معادل و تعریف مقاومت به این صورت که با تعداد نمودار توان مشخص، در هیچ لحظه ای امکان شناسایی کلید وجود نداشته باشد و ضریب همبستگی کلید صحیح در تمام لحظات بیشتر از ضریب همبستگی دیگر کلیدهای فرضی نباشد، میزان مقاومت در برابر حملات تحلیل توانی همبستگی نسبت به حالت ناامن در حدود ۴۵۰ برابر افزایش داشته است.