عنوان مقاله:
ارایه روشی برای مقاوم سازی الگوریتم AES در برابر حملات کانال جانبی

محل انتشار:
کنفرانس بین المللی تحقیقات بنیادین در مهندسی برق (سال: 1396)

تعداد صفحات اصل مقاله: 7

نویسنده:
محمدعلی ناری ابیانه - *تهران، دانشگاه شاهد*

خلاصه مقاله:
حملات آنالیز توان تفاضلی یکی از روش های عملی به منظور حمله به پیاده سازی یک الگوریتم رمزنگاری می باشد. این روش به علت عدم نیاز به دانش تخصصی درباره دستگاه مورد حمله، یکی از محبوبترین روش های حمله به الگوریتم های رمزنگاری می باشد. به منظور ایمن کردن الگوریتم ها در برابر این حمله شایع و ارزان، روش های مقاوم سازی بسیاری از جمله [1.20] ارایه شده است. با توجه به استاندارد بودن و استفاده زیاد از الگوریتم AES[3]، مقاوم سازی این الگوریتم می تواند کمک بسیاری به ارایه ارتباطات دیجیتال امن کند. این مقاله به ارایه روشی برای ایمن سازی الگوریتم AES در برابر حملات تحلیل توان تفاضلی[3],می پردازد. این روش با درهم ریزی عملیات ها در مراحل مختلف الگوریتم AES توان مصرفی را از مقدار میانی واقعی مستقل می کند.

کلمات کلیدی:
رمزنگاری، مقاوم سازی، AES، کانال جانبی، DPA، تحلیل توان تفاضلی