عنوان مقاله:
روش جدید در امنیت سیستم های رمزنگاری توسط گیت های نامتوازن

محل انتشار:
فصلنامه سیستم های پردازشی و ارتباطی چندرسانه ای هوشمند, دوره 3, شماره 2 (سال: 1401)

تعداد صفحات اصل مقاله: 12

نویسندگان:
سید حمیدرضا موسوی - *استادیار دانشگاه آزاد زنجان*

مهدی صفائیان - *استادیار گروه برق و کامپی.تر دانشگاه ازاد اسلامی هیدج*

خلاصه مقاله:
امروزه اشتراک اطلاعات و انتقال ایمن آن بین سیستمهای مختلف الکترونیکی ضروری شدهاست. یکی از چالشهای مهم در این زمینه حملات کانال جانبی میباشد که با استفاده از تکنیکهای موجود سعی در بدست آوردن کلید رمزنگاری دارند. هدف از این پژوهش ارائه طرح جدیدی برای مقاوم سازی الگوریتم های رمزنگاری می باشد. در این طرح با به هم زدن توان مصرفی توسط دو عامل ارتقاء گیت های کلیدی و تزریق تصادفی تاخیر در اجرای بخش های مختلف از الگوریتم استاندارد رمزنگاری پیشرفتهAES ، میزان مقاومت این سامانه در مقابل حملات تفاضلی توان DPA افزایش یافته است. برای اصلاح گیت XOR از مدلی استفاده شده است که با وجود توان متغیر در زمانهای مختلف عملکردی ثابت و منطقی دارد. ترکیب گیت فوق با تاخیرهای تصادفی که توسط PLL در ناحیه گذرا ساخته می شود، مقاومت سیستم را بیشتر بهبود داده است. طرح فوق در تکنولوژی ۶۵nm پیاده شده و نتایج حاصل از شبیه سازی در مقابل حملات تفاضلی توان نتایج قابل قبولی را نشان داده است. این طرح تنها هزینه سربار ۳۳ درصد در فضای اشغالی و ۲۵ درصد در توان مصرفی را به دنبال داشته است، و تنها سرعت عملکرد ۳ درصد کم شده است در حالی که مقاومت تقریبا دو برابر شده است.

کلمات کلیدی:
استاندارد رمزنگاری پیشرفته, حملات تفاضلی توان, اندازه گیری توان, حلقه فاز قفل شده, گیت