عنوان مقاله:
پیاده سازی مقاوم الگوریتم RSA در مقابل حمله کانال جانبی تحلیل توان با استفاده از محاسبات نامتعارف

محل انتشار:
سیزدهمین کنفرانس بین المللی انجمن رمز ایران (سال: 1395)

تعداد صفحات اصل مقاله: 6

نویسندگان:
سعید گرگین - *پژوهشکده برق و فناوری اطلاعات، سازمان پژوهش های علمی و صنعتی ایران، تهران*

حسین کریمی خوشرو - *دانشکده علوم و مهندسی کامپیوتر، دانشگاه شهید بهشتی، تهران*

خلاصه مقاله:
حمله های کانال جانبی از جمله مهمترین تهدیدها، علیه پیاده سازی های رمزنگاری مدرن، نظیر AES و RSA به شمار می روند. الگوریتم RSA از جمله الگوریتم های رمزنگاری نامتقارن و متداولی است که با استفاده از عملیات به توان رساندن و ضرب کار می کند و در عمل اختلاف توان مصرفی و تاخیر این دوعملگر موجب گردیده تا این الگوریتم در مقابل حمله کانال جانبی تحلیل توان، آسیب پذیر گردد. یکی از روش های مقابله با این حمله، از بین بردن رابطه توان مصرفی با کلید به کار رفته در الگوریتم است. در این مقاله، برای رسیدن به این مقصود از محاسبات نامتعارف ترکیبی مبنای دو و سه (HBT) استفاده گردیده است. در این روش با استفاده از تقسیم های متوالی، مبنای کلید از عدد دو به دو و سه تغییر می یابد. این عمل از یک سو موجب عدم کشف کلید با استفاده از تحلیل توان مصرفی می شود و از سوی دیگر به دلیل کوتاه شدن کلید در نمایش ترکیبی مبنای دو و سه، در الگوریتمی همانند RSA که از حجم محاسباتی بالایی برخوردار است، افزایش سرعت محاسبات را در پی خواهد داشت.

کلمات کلیدی:
کانال جانبی، حمله های آنالیز توان مصرفی، محاسبات نامتعارف مبنای دو و سه ترکیبی (HBT)، الگوریتم رمزنگاری RSA