

عنوان مقاله:

خواص جبری جمع مدولی به پیمانه t_2 با r عملوند

محل انتشار:

فصلنامه علوم و فناوری های پدافند نوین، دوره 1، شماره 2 (سال: 1389)

تعداد صفحات اصل مقاله: 8

نویسندگان:

مهدی علائیان - دانشکده ریاضی

علیرضا رحیمی پور - دانشکده ریاضی

سیدمجتبی دهنوی - دانشکده ریاضی

خلاصه مقاله:

یکی از پرکاربردترین عملگرها در رمزنگاری متقارن، جمع مدولی به پیمانه است. بنابراین بررسی خواص این عملگر نقش مهمی در طراحی و تحلیل رمزهای متقارن دارد. خواص جبری این عملگر در t_2 با دو عملوند مورد مطالعه قرار گرفته است. ما در این مقاله به منظور رسیدن به نتایج بهتر و بیشتر در این زمینه، برخی از خواص جبری را برای عملوندهایی با تعمیم داده ایم. به عبارت دقیق تر درجه جبری مولفه ای توابع بولی از جمع مدولی را به عنوان یک تابع بولی برداری در نظر گرفته ایم و تعداد عبارت ها و متغیرها در این توابع بولی را تعیین نموده و پس از تجزیه و تحلیل نظری در حالت های خاص، یک الگوریتم کارا برای یافتن درجه مولفه ای توابع بولی در حالت کلی پیشنهاد کرده ایم. با استفاده از این الگوریتم، درجه جبری مولفه ای توابع بولی برای جمع مدولی به پیمانه t_2 با سه تا هشت عملوند قابل محاسبه است.

کلمات کلیدی:

جمع مدولی به پیمانه t_2 ، تابع بولی، شکل نرمال جبری، درجه جبری

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/934900>

