عنوان مقاله:
پیرامون ANF و درجه جبری عمل دوران وابسته به داده

محل انتشار:
فصلنامه صنایع الکترونیک, دوره 1, شماره 1 (سال: 1389)

تعداد صفحات اصل مقاله: 8

نویسنده:
اکبر شاهسواران - *دانشگاه صنعتی شریف*

خلاصه مقاله:
در این مقاله عمل دوران وابسته به داده(DDR) را به عنوان کی تابع بولی برداری در نظرمی گیریم و نشان می دهیم که درجه جبری همه توابع مولفه ای آن k+۱ است که ۲K طول بیتیعملوندهاست.این موضوع به علاوه فرم نرمال جبری (ANF) توابع مولفه ای که ارایه می شود، علاوهبر اهمیت نظریهک و بینشی که نسبت به ماهیت جبری این عمل به ظاهر رام نشدنی و پیچیده بهدست میدهد، کاربردهایی در بررسی حمله تفاضلهای مراتب بالا بر الگوریتم های قالبی نظیر RC۵که از DDR به عنوان کی مولفه استفاده می کنند و نیز در بررسی حمله جبری Courtois دارد.

کلمات کلیدی:
دوران وابسته به داده, فرم نرمال جبری, درجه جبری, حمله تفاضل های مراتب بالا, حمله جبری