عنوان مقاله:

بهبود آماری رمز جریانی همزمان بومی (NJ۲)، جهت امنیت در تبادل اطلاعات محرمانه

محل انتشار:

مجله پدافند غیر عامل, دوره 3, شماره 1 (سال: 1391)

تعداد صفحات اصل مقاله: 7

نویسندگان:

عبدالرضا روستا

بهروز خادم

خلاصه مقاله:

پیشرفت های روزافزون در حوزه های ارتباطات، مخابرات، سامانه های شناسایی و جمع آوری اطلاعات، تغییرات قابل توجهی را در چالش های نظامی به وجود آورده است. امنیت در تبادل اطلاعات، یک معیار مهم پدافند غیرعامل بوده و علم رمزنگاری نقش انکارناپذیری در این سناریو ایفا می کند. به همین منظور، به بهبود آماری یک سامانه رمز جریانی بومی، با استفاده از گسسته سازی و جایگشت آشوبی پرداخته ایم که می تواند جهت افزایش امنیت، در تبادل اطلاعات محرمانه و در راستای پدافند غیرعامل استفاده شود. از جمله مزیت این سامانه رمزنگار نسبت به نسخه قبلی، برطرف نمودن ضعف قسمت غیر خطی می باشد. این عمل باعث افزایش قدرت و کارایی رمزنگار شده است.

کلمات کلیدی:

نگاشت آشوب, گسسته سازی, رمز جریانی همزمان

لینک ثابت مقاله در پایگاه سیویلیکا: