عنوان مقاله:
طراحی یک سیستم رمز پی در پی مقاوم در برابر حمله همبستگی

محل انتشار:
دهمین کنفرانس دانشجویی مهندسی برق ایران (سال: 1386)

تعداد صفحات اصل مقاله: 5

نویسندگان:
معین احمدی - *پژوهشگاه مخابرات و الکترونیک نصر*

مبین احمدی
احسان سلیمانی

خلاصه مقاله:
در طراحی سیستمهای رمز پی در پی معمولا از چندین شیفت رجیستر با فیدبک خطی که با تابعی غیرخطی با هم ترکیب می شوند استفاده می شود دراین مقاله سعی شده است با ترکیب مناسب سیستمهای شناخته شده سیستمی مقاوم در برابر حملات انجام شده طراحی میگردد.

کلمات کلیدی:
جستجوی کامل، حمله همبستگی، شیفت رجیستر با فیدبک خطی، مالتی پلکسر، مولد شبه نویز

لینک ثابت مقاله در پایگاه سیویلیکا: