عنوان مقاله:
ارزیابی فازی مولدهای شبه تصادفی

محل انتشار:
سومین کنفرانس انجمن رمز ایران (سال: 1384)

تعداد صفحات اصل مقاله: 8

نویسندگان:
حمید ملا - *دانشگاه صنعتی اصفهان*

محمد دخیل علیان - *دانشگاه صنعتی اصفهان*

خلاصه مقاله:
مولدهای شبه تصادفی از اهمیت ویژه ای در رمزنگاری به خصوص جهت تولید دنباله کلید اجرایی در سیستمهای رمز پی در پی برخوردارند. در دهه های اخیر آزمونهای آماری متعددی به منظور ارزیابی این گونه مدلها ارائه شده است. در روش متداول ارزیابی یک مولد شبه تصادفی، ابتدا دنباله های متعدد تولید شده توسط مولد تحت آزمونهای آماری نظیر آزمون فرکانس، آزمون رنها، آزمون پوکر و .. قرار می گیرند. سپس نتایج این آزمونها خود تحت آزمونهای کلی تر همچون آزمون KS، آزمون یکنواختی مقادیر احتمال و یاآزمون سازگاری رفتار مولد بامدل فرض شده، قرار میگیرند و در نهایت نتیجه چنین آزمونی به صورت رد یا قبول مولد به عنوان یک مولد شبه تصادفی می باشد. در این مقاله با در اختیار داشتن نتایج حاصل از اعمال آزمون آماری T بر روی دنباله های تولید شده توسط مولد، فرضیه شبه تصادفی بودن به صورت یک فرضیه فازی مدل می شود و سپس آزمون سازگاری جهت بررسی این فرضیه فازی مورد استفاده قرار می گیرد. نتیجه این روش بیان میزان شبه تصادفی بودن مولد به صورت یک تابع عضویت می باشد.

کلمات کلیدی:
مولد شبه تصادفی ، آزمون آمای ، آزمون فرض فازی ، آزمون سازگاری فازی

لینک ثابت مقاله در پایگاه سیویلیکا: