عنوان مقاله:
یک تولید کننده رشته کلید شبه تصادفی جدید با استفاده از تئوری آشوب و جعبه جایگشت AES

محل انتشار:
دومین کنفرانس ملی توسعه کاربردهای صنعتی اطلاعات، ارتباطات و محاسبات (سال: 1392)

تعداد صفحات اصل مقاله: 6

نویسندگان:
اسماعیل بشارتی فرد - *دانشگاه گیلان*

رضا ابراهیمی آتانی - *دانشگاه گیلان*

خلاصه مقاله:
هسته اصلی رمزهای جریانی، تولید کننده رشته کلید شبه تصادفی می باشد. در مقالات مختلف، تولید کننده های متفاوتی برای این کارطراحی شده اند. در این مقاله، با توجه به خواص غیرقابل پیش بینی بودن رفتار نگاشت های آشوبی و حساسیت شدید آنها به شرایط اولیه و پارامتر های آشوبی، با استفاده از نگاشت آشوبی و جعبه جایگشتAESبه ارائه یک تولید کننده رشته کلید شبه تصادفی پرداخته می شود. با استفاده از آزمون های خود همبستگی، پیچیدگی خطی، توزیع صفر و یک ها و آزمون های آماریNISTکارایی روش پیشنهادی مورد بررسی قرارگرفته و نتایج نشان از مناسب بودن این روش می باشد

کلمات کلیدی:
رمز جریانی، رشته کلید شبه تصادفی، آشوب، جعبه جایگشت