دومین کنفرانس انجمن رمز ایران
دانشگاه صنعتی شریف
۳۰-۲۹ مهر ماه ۱۳۸۲

اصلاح آزمون رنها وارائه آزمون رنهابرای زیر قالبها

بهروز پی زری(دانشجوی کارشناسی ارشدمخابرات دانشگاه صنعتی اصفهان)
b_peyzari@hotmail.com

محمد دخیل علیان(استادیار دانشگاه صنعتی اصفهان)
mdalian@cc.iut.ac.ir

چکیده:تولید و بررسی دنباله های شبه تصادفی یکی از مباحث مهم در علم رمزنگاری می باشد.جهت بررسی خواص تصادفی دنباله های شبه تصادفی از تئوری آزمونهای آماری استفاده می شود.در آزمونهای آماری هدف ارائه ملاک عملی برای سنجش خواص دنباله مورد آزمون ومیزان نزدیکی آن به دنباله ایده ال یعنی دنباله های با توزیع یکنواخت که اعضای آن تؤاما مستقل هستند،می باشد.در این مقاله با نگرشی دقیق به خاصیت رنها در یک دنباله مدل احتمال دقیق آن را بدست می آوریم و به ارائه آزمونی دقیق برای بررسی تعداد رنها در یک دنباله شبه تصادفی می پردازیم .در ادامه نیز با بررسی مدل رنها برای زیر قالبها ی یک دنباله آزمون رنها برای زیر قالبها را ارائه خواهیم داد.

واژگان کلیدی:توزیع رنها[1] ،دنباله های شبه تصادفی،آزمونهای آماری[2]

۱.مقدمه

در بررسی و تجزیه و تحلیل الگوریتمهای رمز قالبی و سیستمهای رمز پی در پی دو مساله از اهمیت خاصی بر خوردار هستند.یکی از این مسایل بررسی تحلیلی این گونه سیستمها مانند مقاومت در برابر حمله تفاضلی ،حمله خطی و... می باشد. دیدگاه دیگر که از اهمیت و جایگاه خاصی در رمزنگاری و دیگر شاخه های علوم برخور دار است بررسی آماری قالبها و دنباله های تولید شده در این گونه سیستمها می باشد.در آزمونهای آماری میزان نزدیکی این دنباله های شبه تصادفی با حالت ایده ال مورد بررسی قرار می گیرد. در آزمونهای آماری با بدست آوردن مدل احتمال برای ویژگیهایی چون تعداد یکها،تعداد رنها،تعداد بلوکهاو گپها،میزان پیچیدگی ،میزان فشرده شدن دنباله و... میزان نزدیکی دنباله تولیدشده را با حالت ایده ال مورد

[1] Runs
[2] Statistical Testing