ارائه مدار عملی برای تولید دنباله کاملاً تصادفی

عباس هاشمی، ابراهیم احمدی
دانشجویان کارشناسی مخابرات
دانشکدهٔ مخابرات
ahmadibent@yahoo.com

دکتر محمد دخیل علیان
استادیار دانشکدهٔ برق
دانشگاه صنعتی اصفهان
mdalian@yahoo.com

چکیده:

امروز با پیشرفت علوم و تکنولوژی ارتباط از طریق وسایل و امکانات مخابراتی به نحو چشمگیری افزایش یافته است. از این میان ارگانهایی نظیر سازمانهای نظامی، تجاری و دولتی بیشترین بهره‌وری را از این امکانات به عمل می‌آورند و بالطبع اطلاعات گرانبهایی از طریق شبکه‌های خود رد و بدل می‌نمایند. امّا همواره خطر استراق سمع، دستکاری و مغشوش کردن اطلاعات توسط افراد سودجو این اطلاعات را تهدید می‌کند. لذا لزوم استفاده از روش‌هایی که امنیت اطلاعات را تضمین کنند به خوبی احساس می‌شود. در این مقاله روشی عملی جهت تولید یک رشته کاملاً تصادفی با مشخصات آماری مطلوب جهت استفاده به عنوان دنباله کلید اجرایی، یا فایل کلید در عملیات رمزنگاری معرفی شده است.

کلمات کلیدی:

رمزنگاری ـ دنباله کلید اجرایی ـ نویز (noise) ـ چگالی طیف (spectral density) ـ مولد نویز (noise Gen) ـ کاملاً تصادفی

۱ـ مقدمه:

سیستمهای رمزنگاری شامل دو بخش رمزگذار و رمزگشا هستند. رمزگذار تبدیل اطلاعات موردنظر به یک متن رمز شده را به عهده دارد و رمزگشا تبدیل متن رمز شده به اطلاعات موردنظر را انجام می‌دهد. کارآیی یک سیستم رمزنگاری به کلید رمز وابسته است که نقش اساسی را در امنیت

سیستم به عهده دارد. چرا که ساختار سیستمهای رمز برای همگان مشخص است و تنها کلید، بخش محرمانه است. بنابراین امنیت و اعتبار پیام وابسته به کلید می‌باشد [1].

هرچه دنباله کلید تصادفی‌تر جلوه کند مناسب‌تر می‌باشد. بنابراین اگر آنتروپی کلید حداکثر باشد، برای حدس کلید با ابهام حداکثر مواجه می‌باشیم. آنتروپی کلید موقعی حداکثر می‌گردد که بیتهای دنباله تولید شده دارای توزیع یکنواخت و مستقل از هم باشند. برای این منظور و ارایهٔ یک روش عملی برای تولید چنین دنباله‌هایی در این مقاله چگونگی استخراج این دنباله‌ها از ادوات نیمه هادی تشریح شده است.

این مقاله در چهار بخش تهیه شده است. پس از مقدمه در بخش دوّم، نویز سفید مورد بررسی قرار گرفته است. در بخش سوّم در مورد تعدادی از منابع نویز موجود در المانهای اکتیو و پسیو به بحث پرداخته‌ایم و در پایان مولدهای نویز مورد استفاده در مدار عملی به همراه نتایج تستهای آماری روی دنبالهٔ تولید شده آورده شده است.

۲ـ نویز سفید و نویز فیلتر شده [7]:

بسیاری از انواع منابع نویز توزیع آماری گاوسی دارند و درگسترهٔ وسیعی از حوزهٔ فرکانس دارای چگالی طیفی تخت‌اند. تمام مؤلفه‌های فرکانسی در چنین طیفی مقدار یکسان دارند و از این رو در قیاس با نور سفید، نویز سفید نامیده می‌شود. چگالی طیفی نویز سفید عموماً بصورت زیر نوشته می‌شود:

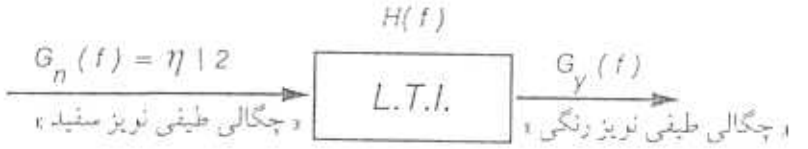
$$G(f) = \frac{\eta}{2} \qquad (1\text{-}1)$$

η چگالی توان فرکانس مثبت نامیده می‌شود و به نوع منبع نویز و چگالی طیفی مربوطه بستگی دارد. تابع خود همبستگی به صورت زیر است:

$$R_y(\tau) = \int_{-\infty}^{+\infty} \frac{\eta}{2} e^{j\omega\tau}\, df\delta(\tau) = \frac{\eta}{2} \qquad (1\text{-}2)$$

معادلهٔ بالا نشان می‌دهد که $R(\tau \neq 0) = 0$ و بنابراین هر دو نمونهٔ تصادف متفاوت از یک سیگنال نویز سفید ناهمبسته هستند و با توجه به اینکه فرآیند گوسی می‌باشد می‌توان نتیجه گرفت که نمونه‌های متفاوت مستقل نیز می‌باشند.

اگر نویز سفید به یک مدار L.T.I با تابع تبدیل H(f) مطابق شکل اعمال شود خروجی نویز سفید فیلتر خواهد بود که اصطلاحاً نویز رنگی نامیده می‌شود.



چگالی طیف نویز رنگی در خروجی مدار به صورت زیر است:

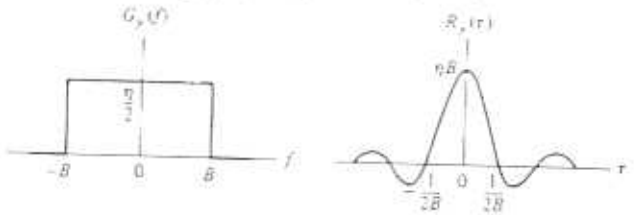
$$Gy(f) = |H(f)|^2 \cdot Gn(f) = \frac{\eta}{2}|H(f)|^2$$

با محاسبهٔ تابع خود همبستگی خروجی داریم:

$$Ry(\tau) = \frac{\eta}{2} \cdot F\left[|H(f)|^2\right]$$

بنابراین مشاهده می‌شود که تابع خود همبستگی دارای مقادیر غیرصفر می‌باشد. به عبارت دیگر نمونه‌های تصادفی استخراج شده از نویز رنگی وابسته می‌باشند. بدیهی است که با افزایش τ میزان همبستگی نمونه‌ها کاهش می‌یابد. بعنوان مثال اگر H(f) را یک فیلتر ایده‌آل پایین‌گذر با پهنای باند B در نظر بگیریم آن گاه تابع خود همبستگی به صورت زیر خواهد بود:

$$Ry(\tau) = \eta B \operatorname{sinc}(2B\tau)$$



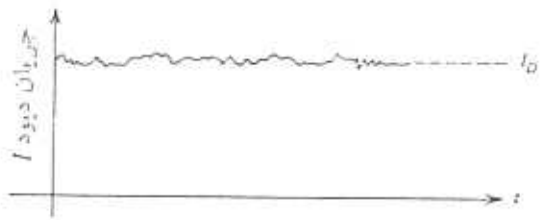
همانطور که در شکل دیده می‌شود با افزایش τ تابع خود همبستگی به سمت صفر میل می‌کند. اگر τ به اندازهٔ کافی بزرگ در نظر گرفته شود می‌توان با تقریب خوبی تابع خود همبستگی را صفر در نظر گرفت. در عمل با انتخاب τ برابر $\frac{10}{B}$ تقریب بسیار خوبی خواهیم داشت.

بنابراین جهت تولید نمونه‌های مستقل باید پهنای باند نویز مورد توجه قرار گیرد. اگر نویز سفید باشد نمونه‌برداری با هر فرکانسی نمونه‌های تصادفی مستقل بدست می‌دهد. در صورتی که جهت داشتن نمونه‌های مستقل از نویز رنگی باید فرکانس نمونه‌برداری مورد توجه قرار گیرد.

۳ـمنابع نویز:

الف ـ نویز ضربه‌ای: (shot noise)

نویز ضربه‌ای به علت طبیعت گسسته جریان حاملهای بار بوده و در اغلب المانهای فعال مانند ترانزیستورهای دو قطبی و دایودها مشاهده می‌شود. این نویز به علت عبور تصادفی حاملهای بار از یک شکاف انرژی تولید می‌شود. در یک دایود حاملهای بار به طور تصادفی از کاند تشعشع می‌شوند و تعداد این حاملها دارای تغییرات آماری از لحظه‌ای به لحظهٔ دیگر می‌باشد. عبور هر حامل از پیوند پدیده‌ای کاملاً تصادفی است و بستگی به این دارد که حامل انرژی کافی و سرعتی به سوی پیوند داشته باشد [6]. بنابراین جریان خارجی I که جریان ثابتی به نظر می‌رسد در واقع از تعداد فراوانی پالسهای جریان مستقل تشکیل شده است. اگر شکل جریان روی یک اسیلوسکوپ حساس مشاهده شود، شکلی مانند زیر خواهیم داشت که در آن I_D جریان میانگین است.



این نوسان در I نویز ضربه‌ای نام دارد و عموماً برحسب متوسط مجذور تغییرات حول مقدار میانگین مشخص می‌شود که با $\overline{i^2}$ نشان داده می‌شود. جهت محاسبهٔ $\overline{i^2}$ ابتدا جریان حاصل از عبور یک الکترون که با ماکزیمم سرعت V_{max} و در مدت t_f شکاف انرژی را طی می‌کند، محاسبه می‌گردد. اگر تعداد الکترونی که به صورت همزمان ساطع می‌گردند با n نمایش دهیم، n یک متغیر تصادفی با توزیع پواسن خواهد بود. بنابراین تابع خود همبستگی جریان‌های ضربه‌ای عبارت است از:

$$\Gamma_i = M\left[\ ni(t)\ ni(t+\tau)\ \right] \qquad (۱-۲)$$

با محاسبهٔ Γ_i و بدست آوردن طیف توان از روی آن به رابطهٔ زیر می‌رسیم:

$$S(\omega) = \frac{1}{2\pi}\ qI\left[\ 1 - \frac{(\omega t_0)^2}{18} + \ldots\right] \qquad (۲\text{-}۲)$$

مقدار متوسط مجذور جریان از روی رابطهٔ اخیر قابل محاسبه خواهد بود که برابر مقدار زیر می‌باشد:

$$\overline{i^2} = S(f)\,\Delta f = 2qI\left[\ 1 - \frac{(\omega t_0)^2}{18} + \ldots\ \right]\Delta f = 2qIF_{fp}^{\ 2}\ \Delta f \qquad (۳\text{-}۲)$$

که در آن $F_{fp} \leq 1$ می‌باشد و فاکتوری است که به ωt_0 وابسته است [2]. با بررسی رابطهٔ (۲-۲) به این نتیجه می‌رسیم که در فرکانس‌های پائین $S(\omega)$ ثابت است و به شکل پالس وابسته نیست. این بدان معناست که طیف نویز ضربه‌ای به صورت نویز سفید در رنج فرکانسی وسیعی ملاحظه می‌شود.

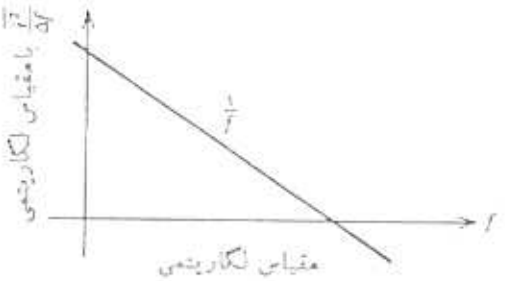
ب ـ فیلکر نویز: (Filker noise)

این نویز در تمام اجزاء فعال و نیز در برخی عناصر غیرفعال مثل مقاومتهای ذغالی یافت می‌شود. جهت دست‌یابی به دلیل فیزیکی این نویز آزمایشهای زیادی انجام گرفته است و مدلهای متعددی ایجاد گشته است. مهمترین آنها مدلهایی هستند که بر پایهٔ تغییرات دمایی و یا تغییر تحرک و یا فرض شرایط سطحی آرام بنا شده‌اند. به عنوان مثال در ترانزیستورهای دو قطبی این نویز عمدتاً بوسیلهٔ تله‌هایی ایجاد می‌شود که همراه ناخالصی‌ها و نقایص بلور در شکاف انرژی امیتر ـ بیس وجود دارند. این تله‌ها حامل را به صورت تصادفی می‌گیرند و رها می‌کنند و ثابتهای زمانی مربوطه به این فرآیند سبب می‌شود که یک سیگنال نویزدار با انرژی متمرکز در فرکانس‌های پایین حاصل شود. طیف توان این نویز به فرم زیر است: [2]

$$S(f) = \text{Const}\ .\ \frac{I^{\beta}}{f^{\alpha}}$$

که در آن I جریان Dc قطعه، f فرکانس اندازه‌گیری، β ثابتی در گسترهٔ 0/5 تا 2 و α نیز ثابتی در محدودهٔ 0/8 تا 1/3 می‌باشد. α معمولاً 1 در نظر گرفته می‌شود. بنابراین فیلکر نویز با فرکانس نسبت

معکوس دارد.



از مشخصات جالب فیلکر نویز می‌توان به موارد زیر اشاره کرد [2]:

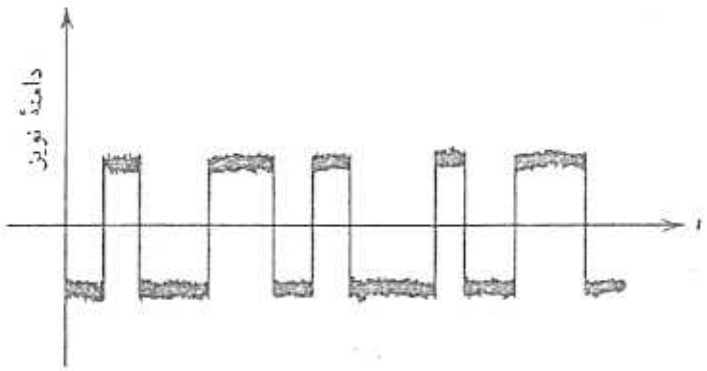
۱ـ توزیع دامنهٔ آن گوسی نیست.

۲ـ نمونه‌ها ناهمبسته نیستند.

۳ـ فرآیند ایستان نیست.

ج ـ برست نویز: (Burst noise)

یک نوع پالس نویزی برست نویز نامیده می‌شود که در مقاومتهای کربنی و یا اتصالات p-n بایاس شده همچنین در مدارهای فشرده یا گستردهٔ ترانزیستوری مشاهده می‌شود. این نویز مانند یک سیگنال مربعی با تغییرات تصادفی ظاهر می‌شود و به انواع دیگر نویز اضافه می‌گردد. [6]



گاهی ممکن است به جای دو سطح، سه یا چهار سطح متمایز وجود داشته باشد. می‌توان نشان داد میانگین مربع جریان برست نویز به فرم زیر است [6]:

$$\overline{i^2} = K \frac{I^c}{1 + (\frac{f}{f_c})^2} \Delta f$$

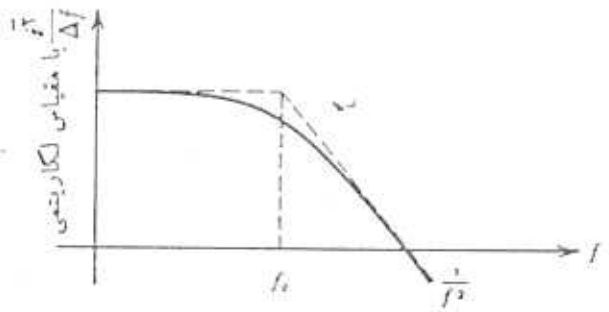
که در آن K ثابت مربوط به هر وسیلهٔ خاص است.

I جریان مستقیم است

c ثابتی بین ۰/۵ تا ۲ است

و f_c فرکانس مخصوص به هر نوع فرآیند نویز است.

چگالی طیف در شکل زیر رسم شده است. مشاهده می‌گردد که در فرکانس‌های بالا طیف نویز به صورت $\frac{1}{f^2}$ افت می‌کند.



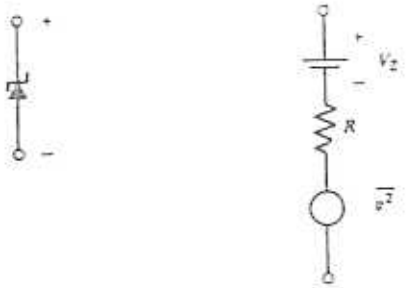
نویز بهمنی: (Avalanche noise)

این نویز در شکست زنری یا بهمنی یک پیوند p-n بوجود می‌آید. یک دایود بایاس معکوس دارای دو مکانیزم تولید نویز می‌باشد. آن مکانیزم‌ها زنر و بهمنی می‌باشند. در شکست بهمنی الکترونها و حفره‌ها در ناحیهٔ تخلیه پیوند p-n آنقدر شتاب می‌گیرند که انرژی آنها جهت تولید جفت‌های الکترون و حفره جدید کافی است. این جفت‌های جدید تحت میدان الکتریکی حاصل از ولتاژ بایاس معکوس شتاب می‌گیرند و جفت‌های الکترون ـ حفره بیشتری تولید می‌کنند. این فرآیند فزاینده است و منجر به تولید یک رشته تصادفی از جهشهای بزرگ نویز می‌شود. مقدار این نویز بسیار بزرگتر از نویز ضربه‌ای در همان جریان است. دلیل این امر این است که یک حامل در فرآیند بهمنی سبب تولید

حاملهای دیگری می‌شود و کل نویز برابر مجموع تعدادی تصادفی از این نوع حاملهاست. [2]

۴ـ مدار عملی و نتایج:

همانطور که قبلاً اشاره شد هدف از انجام این پروژه تولید یک رشتهٔ کاملاً تصادفی است. این طرح بر پایهٔ تولید رشتهٔ کاملاً تصادفی از یک مولد نویز بنا شده است. طبق مطالب بیان شده در بخش ۲ نمونه‌های استخراج شده از یک منبع نویز سفید مستقل می‌باشند. به دلیل پهنای باند محدود منابع نویز این کار در عمل ممکن نیست و ما بیشتر با نویز رنگی سر و کار داریم. در بخش ۲ بیان شد که نمونه‌های استخراج شده از یک منبع نویز رنگی وابسته می‌باشند و این وابستگی در صورتی که فیلتر ایده‌آل باشد بصورت تابع سینک بیان شد. با توجه به شکل تابع سینک در صورتی که نمونه‌برداری با فرکانسی کمتر از پهنای باند نویز رنگی انجام گیرد می‌توان مطمئن بود که نمونه‌ها مستقل می‌باشند، زیرا $\lim_{\tau \to \infty} R_y(\tau)$ منابع نویز مورد استفاده در این طرح می‌تواند دیودزنر و یا ترانزیستور دو قطبی باشد. همانطور که در بخش ۳ اشاره شد، دیودهای‌زنر به علت تولید نویز بهمنی می‌توانند به عنوان منبع نویز مورد توجه قرار گیرند. مدار معادل نویز یک دیودزنر به فرم زیر است:



که $\overline{v^2}$ مولد ولتاژ نویز می‌باشد، V_z ولتاژ شکست دیود و مقاومت R نوعاً ۱۰ تا ۱۰۰ اهم است. پیشگویی اندازهٔ $\overline{v^2}$ دشوار است زیرا به ساختمان دیود و یکنواختی بلور آن بستگی دارد ولی مقادیر نوعی اندازه‌گیری شده برابر $\frac{\overline{v^2}}{H_z}$ $\cong 10^{-14}$ $\frac{\overline{v^2}}{\Delta f}$ در جریان 0.5 mA dc می‌باشد [6].

نویز ایجاد شده در مقاومت R در مقایسه با نویز بهمنی بسیار ناچیز است و در آن محو می‌شود. همانطور که قبلاً اشاره شد چگالی طیف نویز بهمنی در گسترهٔ وسیعی بصورت یکنواخت می‌باشد.

پیوند بیس ـ امیتر در ترانزیستور دو قطبی هم می‌تواند به عنوان منبع نویز مورد توجه قرار گیرد. همانطور که در بخش ۳ اشاره شد طبق رابطهٔ (۲-۳) نویز ضربه‌ای با فلوی جریان در سد پتانسیل اسباب نیمه هادی رابطه دارد. این اتصال دارای دو جزء جریان می‌باشد که در اثر حاملهای اکثریت و اقلیت ایجاد می‌شوند. هر دوی این جریانها نویز ضربه‌ای ایجاد می‌کنند که با یکدیگر جمع می‌شوند. از طرف دیگر تجربه نشان داده است که برست نویز و فیلکر نویز موجود در یک ترانزیستور را می‌توان با مولدهای جریانی به موازات پیوند بیس ـ امیتر نشان داد. این مولدها به سادگی با نویز ضربه‌ای موجود در جریان بیس ترکیب می‌شوند. چون این منابع نویز از مکانیزمهای فیزیکی مستقل و جداگانه‌ای ناشی می‌شوند نسبت به یکدیگر مستقل هستند و مقدار متوسط مجذور آنها چنین است:

$$\overline{i_b^2} = 2qI_B\Delta f + K_1\frac{I_B^a}{f}\Delta f + K_2\frac{I_B^c}{1+(\frac{f}{f_c})^2}\Delta f$$

برست نویز — نویز ضربه‌ای — فیلکر نویز

بر این اساس، رشتهٔ کاملاً تصادفی با نمونه‌برداری از یک منبع نویز تولید گردید. بدین منظور پس از تقویت نویز عمل نمونه‌برداری توسط مدرا S&H انجام گرفت. نمونه‌ها پس از دیجیتال شدن از طریق پورت موازی کامپیوتر در یک فایل ذخیره شدند و فایل بدست آمده مورد تست قرارگرفت. جهت بررسی خواص آماری مطلوب یک رشتهٔ باینری تستهای آماریِ متعددی وجود دارد. هدف از این تستها بررسی سازگاری دنبالهٔ تولید شده توسط مولد تصادفی با یک مدل احتمال فرضی می‌باشد. آزمونهای آماری معمولاً بر روی زیر دنباله‌های دنبالهٔ اصلی اعمال می‌شوند. زیرا هر زیر دنباله از دنبالهٔ کلید

اجرائی نیز باید کاملاً تصادفی جلوه نماید. آزمونها معمولاً بر روی زیر دنباله‌های ۵۰۰ تا ۱۰۰۰ بیتی اعمال می‌شوند و در واقع تصادفی بودن آنها بصورت محلی مورد بررسی قرار می‌دهند. نتیجهٔ تستهای انجام شده بر روی دنباله‌های مختلف تولید شده توسط مدار موردنظر در پایان آورده شده است. جهت انجام تست‌ها نرم‌افزار آماری آرمان مورد استفاده قرار گرفته است.

۵ـ جمع‌بندی:

همانطورکه مشاهده شد نتایج برای آزمونهای آماری فرکانس، سریال، پوکر، گپها، و بلوک‌ها [۳] و تعداد رنها و مشتقات بایتری [۵] و سریال تعمیم یافته [۴] مطلوب بوده است در آزمونهای فوق طول زیر دنبالهٔ ۲۵۰ بیت گرفته شده است.

در صورتی که الگوریتمهای رمز ضعف داشته باشد سیستم ممکن است مورد حمله قرار گیرد. الگوریتمهای متعددی تاکنون ابداع شده‌اند که پس از گذشت اندک زمانی از کابرد آنها، تحلیل‌گران آنان را مورد ارزیابی قرار داده و نقاط ضعف الگوریتمها را یافته‌اند. طراحان نیز به ناچار گونه‌های جدیدتری از الگوریتمها را با نقطه ضعفهای کمتری، ارائه داده‌اند. این حقیقت باعث شده است تا طراحان و تحلیل‌گران پابه‌پای یکدیگر در عرصهٔ رمزنگاری رقابت نمایند و حاصل این رقابت رشد روز افزون این علم بوده است.

منابع:

۱ـ دکتر محمد دخیل علیان، «ارزیابی دنباله‌های شبه تصادفی و طراحی مولدهای آشوبی»، رسالهٔ دکتری، دانشگاه صنعتی اصفهان، آبان ۱۳۷۷

2- Ambrozy , Andras : "Electronic noise" : McGraw-Hill : 1982

3- Beker H. and Peper F. , Cipher System : "The Protection of Communications" , Northwood Book , London , 1982

4- Kimbrely M. , "Comparison of Two Statitical Test for Keystream Sequences" , Electronic letter, vol. 23 , No.8 , PP.365-366 , April 1987

5- Gustafson H. , Dawoson E. D. and Caell, B. , "Comparison of Black and stream Clipher" , Advances in Cryprologe , Springer - Verlag , AusCrypy , 90 , PP.208-219

6- Gray , Meyer ; "Analysis and Design of Analoy Integrated Circuits" , John wiley & Sons , 1984

7- A. B. Carlson , "Communication systems" , McGraw-Hill , 1986

Proportion Test:

Threshold: 3.8415

Test Name	Average	Chi2 Value	Result
Frequency	%92.00	1.8947	Pass
Serial	%92.00	1.8947	Pass
Number of Runs	%93.00	0.8421	Pass
Modified Serial	%95.00	0.0000	Pass
Gaps	%96.00	0.2105	Pass
Blocks	%95.00	0.0000	Pass
Binary Derivative	%100.00	5.2632	Pass
Poker	%97.00	0.8421	Pass
Autocorrelation	%93.00	0.8421	Pass
Linear Complexity Profile	%96.00	0.2105	Pass

Kolmogorov-Smirnov Test:

Threshold: 1.2072

Test Name	KN+	KN-	Result
Frequency	0.3000	1.0291	Pass
Serial	0.3716	0.7558	Pass
Number of Runs	0.7555	0.4758	Pass
Modified Serial	0.3736	0.7720	Pass
Gaps	0.9226	0.6299	Pass
Blocks	0.4851	0.5683	Pass
Poker	0.5304	1.1010	Pass
Autocorrelation	1.1102	0.7881	Pass
Linear Complexity Profile	1.1244	0.1350	Pass