دانشکده مهندسی

گروه برق

پایان نامه کارشناسی

گرایش: الکترونیک

عنوان:

بررسی و ساخت دستگاه تولید کننده اعداد تصادفی

استاد راهنما: دکتر شهرام محمدی

نگارش: علیرضا کلانتری

شهریور ۹۵

چکیده

در این تحقیق به بررسی مفاهیم مربوط به اعداد تصادفی،کاربردها، روش‌ها و الگوریتم‌های تولید اعداد تصادفی با کامپیوترهای رقمی پرداخته می‌شود. در ابتدای امر الگوریتم‌ها را تعریف و ویژگی‌های آن‌ها را بیان می‌کنیم و نیز نتایج حاصل از آزمایش برخی از آن‌ها را که با کمک نرم‌افزار Excel انجام شده، بیان کرده و مشاهده می‌کنیم که در الگوریتم‌های میان‌ضربی و مضرب ثابت، معایبی مثل از هم پاشیده شدن وجود دارد به صورتی که در تولید دنباله اعداد، الگوریتم وارد حلقه تکرار صفر می‌شود که در نتیجه تعداد اعداد شبه تصادفی تولید شده بسیار کمتر از تعداد مورد نیاز ما می‌باشد. در ادامه مولدهای همنهشتی بررسی می‌شود و به دلیل مزایای آن، در بخش ساخت دستگاه مولد اعداد تصادفی، مورد استفاده قرار می‌دهیم. در نهایت گزارشی از ساخت دستگاه تولید کننده اعداد تصادفی، ارائه می‌شود.

فهرست مطالب

فصل اول

مقدمه

اعدادی که به صورت متغیرهایی تصادفی حاصل از اتفاقات تصادفی مانند ریختن تاس یا برداشتن گوی از کیسه، پرتاب سکه و . . . در زمان‌های قدیم صرفاً برای انجام بازی‌هایی، که البته اکنون نیز چنین بازی‌هایی انجام میابد، استفاده می‌شدند. با گسترش علم و فناوری و نیز علوم کامپیوتر، نیاز به استفاده‌ی تعداد زیادی از اعداد تصادفی در زمان کوتاه، به وجود آمده است.

دو روش اصلی برای تولید اعداد تصادفی[۱] استفاده می‌شود.یکی، پدیده‌های فیزیکی مثل نویز اتمسفری[۲]، نویز موجود در محیط یک اداره و ... را که انتظار می‌رود تصادفی باشند اندازه می‌گیرد و بایاس‌های موجود در فرایند اندازه‌گیری را خنثی می‌کند. روش دیگر از الگوریتم‌های[۳] ریاضی استفاده می‌کند که توالی‌های طولانی از اعدادی که ظاهراً تصادفی هستند را تولید می‌کند، که در حقیقت توسط یک مقدار اولیه، که به عنوان هسته[۴] شناخته می‌شود، برآورد می‌شوند. اولی به عنوان مولد اعداد تصادفی واقعی[۵] شناخته می‌شود.

اغلب سیستم‌های واقعی دارای یک یا چند فرایند تصادفی می‌باشند که رفتارشان بستگی کامل به این فرایندها دارد. ساختن اغلب مدل‌های شبیه‌سازی کامپیوتری مستلزم تولید رفتار تصادفی و احتمالی اشیاء یا مشخصه‌هایی از سیستم در این مدل‌ها می‌باشد.این گونه رفتارها در اغلب موارد به وسیله متغیرهای تصادفی که دارای قوانین معین احتمالی هستند بیان و شبیه‌سازی می‌گردند[۱].

با توجه به کاربرد روزافزون کامپیوتر، حفظ امنیت و تأیید صحت اطلاعات، روز به روز اهمیت بیشتری پیدا می‌کند.اطلاعات نظامی، دولتی و حتی پزشکی قبل از مخابره در شبکه باید در قالب‌های امن قرار بگیرند تا از دسترسی بون اجازه دیگران در امان باشند.این قالب‌های امن از طریق الگوریتم‌های رمزنگاری[۶]

---

۱ Random Number
۲ Atmospheric noise
۳ Algorithms
۴ Seed
۵ True Random Number Generator
۶ Cryptography

فراهم می‌شود که از متداول‌ترین این روش ها می‌توان به رمزنگاری بر اساس RSA و DES اشاره کرد.عملکرد مناسب تابع رمز در این روش‌ها ارتباط مستقیمی با کیفیت تولید کلید روز دارد که اساس تولید آن بر پایه اعداد تصافی است[۲].

۱-۱ اعداد تصادفی در شبیه‌سازی‌ها

یکی از ویژگی‌های هر مدل شبیه‌سازی تغییرات تصادفی است. برای اجراپذیر شدن مدل به وسیله کامپیوتر، نیازمند روش‌هایی هستیم که از طریق نوشتن برنامه برای آن‌ها بتوانیم رفتار تصادفی مورد بحث را تولید کنیم که در ادامه آن را توضیح خواهیم داد. در آغاز، واژه «رفتار» را به منزله توالی تصمیم‌هایی که با جلو رفتن ساعت شبیه‌سازی بر اساس مقادیر جدید ویژگی‌های نهادها اتخاذ می‌شود، تعبیر می‌کنیم. اگر دنباله‌ی مقادیر پذیرفته شده توسط هر ویژگی از توزیع احتمال معینی پیروی کند، آن دنباله‌ی مقادیر تصادفی است، تصمیم‌های مبتنی بر مقادیر موجود در دنباله تصادفی شمرده می‌شود و در نتیجه شبیه‌سازی برخوردار از رفتار تصادفی خواهد بود. از لحاظ عملی، پذیرش عامل تصادفی بودن ناظر به تعیین توزیع احتمال برای هر یک از دنباله‌های مورد بحث است تا بر اساس آن بتوان به«نمونه‌گیری» اقدام کرد.

به منظور تولید مقادیر تصادفی برای هر ویژگی، باید به نمونه‌گیری از توزیع احتمال نظیر آن پرداخت. روش‌های گوناگون برای نمونه‌گیری از طریق کامپیوتر وجود دارد. تمام این روش‌ها یکوجه مشترک دارند: اینکه تمام آن‌ها از برنامه‌های (کامپیوتری) مولد دنباله اعداد استفاده می‌کنند به طوری که «از لحاظ نظری»، اعداد مزبور در فاصله (۱و۰) توزیع یکنواخت دارند و از لحاظ آماری نیز هر عدد از سایر اعداد موجود در دنباله مستقل است.

با گذر از نظریه به کاربرد، به مطالبی برخورد می‌کنیم که مؤید محدود بودن امکان تولید مقادیر تصادفی مستقل و یکنواخت به روشی معین است. به طور مشخص، عواملی چون طراحی فیزیکی کامپیوتر (سخت افزار)، خصوصیات زبان انتخاب شده برای برنامه نویسی (نرم افزار) و الگوریتم منتخب (روش تولید مقدار) ممکن است به نحو بارزی بر قابل حصول بودن خواص پیش‌بینی شده در نظریه تأثیر بگذارد. از لحاظ طراحی فیزیکی، طول کلمه تمامی کامپیوترها محدود است به طوری که اعداد تنها در فواصل مشخصی قابل ذخیره و پردازش است. مثلا، کامپیوترهای آی‌بی‌ام از رده ۳۶۰/۳۷۰ کلماتی متشکل از ۳۲ بیت دارد اولین بیت سمت چپ، معرف علامت عدد است و از ۳۱ بیت سمت راست می‌توان به منظور ذخیره‌سازی اعدادی به بزرگی۲/۱۴۷ بیلیون استفاده کرد (b ۲/۱۴۷=۱−$۲^{۳۱}$). عدم امکان ذخیره هر

مقدار دلخواه در حافظه‌ی کامپیوتر، بر توزیع یکنواخت (پیوسته) اعداد تولید شده در فاصله صفر تا یک تأثیر می‌گذارد.

پس از ظهور کامپیوترهای رقمی الکترونیک به منزله ابزاری اصلی در زمینه پژوهش‌های علمی، از ابزار دیگری به طرق متفاوت برای تولید اعداد تصادفی استفاده می‌شد. طرق مورد بحث، از جمله ناظر به ریختن تاس، استفاده از جدول‌های اعداد تصادفی و استفاده از ابزار فیزیکی مولد بود. دسترسی فزاینده به کامپیوترهای رقمی، منجر به ارائه‌ی روش‌های محاسباتی متنوع در زمینه تولید اعداد تصادفی شد. تمام روش‌های محاسباتی که تا کنون منسوخ نشده، مبتنی بر الگوریتم‌های خطی تکرار پذیر است. این روش‌ها شامل مولدهای همنهشتی خطی[۱] و مولدهای خطی تکرار پذیر در پایه عددی دو است. پارامترهای هر یک از مولدهای رده اول (همنهشتی خطی) از یک نوع کامپیوتر به نوع دیگر تغییر می‌کند. مولدهای رده دوم، به تولید بیت‌های تصادفی برای کامپیوترهایی که پایه عددی ۲ دارد می‌پردازد و اعداد تصادفی را در قالب رشته‌هایی از این بیت‌ها تولید می‌کند. مولدهای اخیر این مزیت‌ها را دارد که پارامترهای آن‌ها به کامپیوتر بستگی ندارد و برای تمام کامپیوترهایی که برخوردار از پایه عدد ۲ است به صورتی یگانه تعریف می‌شود.

۱-۲ اعداد تصادفی در رمزنگاری

- **مفاهیم**

روش‌های مختلفی در رمزگذاری اطلاعت مطرح است که بطور کلی به دو دسته رمزگذاری جویباری[۲] و بلوکی[۳] تقسیم می‌شوند.که در نوع اول، در هر لحظه، رمزگذاری بیت به بیت یا کاراکتر به کاراکتر انجام می‌گیرد ولی در نوع دوم تمام رشته پیغام به یکباره رمز شده و ارسال می‌گردد.به طور کلی برای هر دو روش رمزگذاری از کلیدهایی استفاده می‌گردد که از اعداد شبه‌تصادفی[۴] ایجاد شده‌اند. برای تولید اعداد تصادفی روش‌های مختلفی وجود داردکه از آن‌جمله می‌توان به مولدهای همنهشتی خطی و غیر خطی،ثباتهای بازگشتی خطی[۵] و غیرخطی و . . . اشاره کرد.

---

۱ Linear Congruentional Generators

۲ Stream Ciphering

۳ Block Ciphering

۴ Pseudo Random Number

۵ Linear Feedback Registers

ثباتهای بازگشتی خطی به دلیل سادگی سخت افزار و قابلیت ایجاد دنباله طولانی از اعداد تصادفی بسیار مورد استفاده قرار می‌گیرند اما در اینگونه روش‌ها رمزگذاری به صورت جویباری انجام می‌گیرد و برای رمز کردن n بیت اطلاعات نیاز به n کلاک می‌باشد.همچنین مجموعه مقادیر تولید شده توسط این روش مرتباً طبق یک الگوی مشخص تکرار می‌شوند[۳].

رمزهای رشته‌ای، نسخه‌ای عملی از الگوی متعالی رمزنگاری یعنی رمز ورنام موسوم به (OPT) می باشند.استحکام رمز ورنام متکی بر حذف کامل ویژگی های آماری متن آشکار از طریق xor نمودن آن با یک کلید تصادفی واقعی از دوره تناوب بینهایت است(نام OPT برای این رمز از همینجا ناشی می شود). از آنجایی که در سایر رمزهای رشته ای بخاطر کلید با طول محدود، این قابلیت وجود ندارد، تولید رشته های شبه تصادفی متمایل به تصادفی و با قابلیت بازتولید توسط کلید و مقدار اولیه، در طراحی رمزهای رشته‌ای محوریت دارد.

در رمزهای رشته‌ای مبتنی بر شیفت رجیسترهای با فیدبک خطی، سعی می‌شود بکمک یک کلید رمز با طول محدود، رشته‌ای شبه تصادفی با طول دلخواه در خروجی رمزنگار تولید شود.

رمزهای رشته‌ای یک مرحله تزریق کلید و مقدار اولیه(شمارنده) به شیفت رجیسترها را دارند که کاملاً خطی و بصورت معادلات جبری-بازگشتی قابل بیان است. خروجی این مرحله را حالت اولیه می‌نامیم، تعداد کلاک‌های شیفت رجیسترها از ابتدای حالت اولیه تا رسیدن به بیت مورد نظر در رشته شبه تصادفی خروجی لحاظ می‌شود[۴].

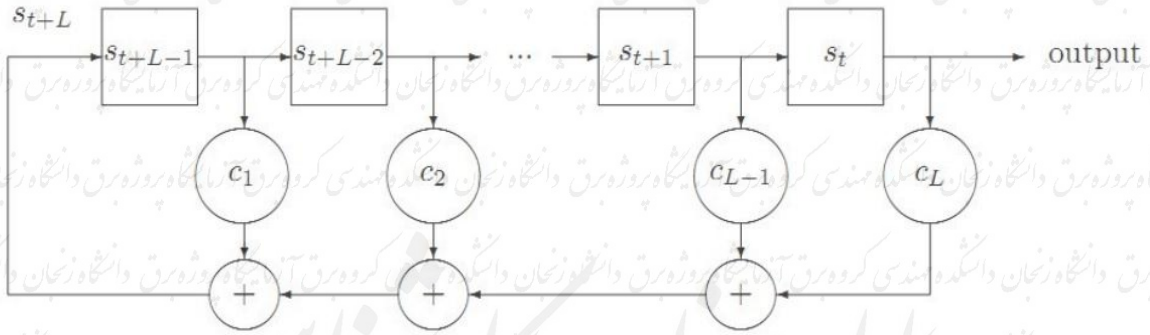
نحوه تولید دنباله $(S_t)_{t\geq 0}$ یا همان دنباله کلید، توسط ثبات انتقال خطی با پسخورد، به صورت :

$$\mathbf{s_{t+L} = c_1 s_{t+L-1} + c_2 s_{t+L-2} + \cdots + c_L s_t \qquad t \geq 0} \qquad (۱\text{-}۱)$$

می‌باشد.

نحوه تولید دنباله S_t توسطه ثبات انتقال خطی با پسخورد در شکل (۱-۱) نمایش داده شده است.که L طول ثبات است[۵].

این ثبات، حالت اولیه را با استفاده از رابطه بازگشتی (۱-۱) به یک دنباله با طول نامتناهی (که دنباله خروجی نامیده می‌شود) تبدیل می‌کند.



شکل(۱-۱) شمای کلی انتقال خطی با پسخورد یا (LFSR) که دارای L مرحله می‌باشد.

دانشجویان محترم:

جهت دسترسی به متن کامل پایان نامه‌ها به کتابخانه دانشکده مهندسی و یا آزمایشگاه پروژه گروه برق مراجعه فرمایید.

مراجع

[۱] حسن صالحی فتح‌آبادی، شبیه سازی سیستم‌ها بوسیله کامپیوترهای رقمی چاپ اول، واحد فوق برنامه بخش فرهنگی دفتر مرکزی جهاددانشگاهی، ۱۳۶۵.

[۲] رشیدی، رحیم، محمدعلی، "ارائه الگوریتمی برای تولید اعداد شبه تصادفی با کارآیی بالا و استفاده از آن در مدلسازی و ارزیابی سیستم‌های کامپیوتری"، همایش ملی مهندسی کامپیوتر، برق وفناوری اطلاعات، دوم، ۳۳۲-۳۳۵، همدان،۱۳۸۸.

[۳] وفائی جهان، مجید؛ سعید ستایشی و محمدرضا اکبرزاده توتونچی، ۱۳۸۶، رمزنگاری اطلاعات بر اساس عوامل محیطی با استفاده از اتوماتای سلولی، چهارمین کنفرانس انجمن رمز ایران، تهران، دانشگاه علم و صنعت ایران، انجمن رمز ایران.http://www.civilica.com/Paper-ISCC04-ISCC04_011.html

[۴] عرب پاریزی، مهدی و علیرضا کشاورزحداد، ۱۳۹۰، ارائه یک مدل جبری احتمالی برای تحلیل رمزهای رشته ای مبتنی بر شیفت رجیسترهای با فیدبک خطی، نوزدهمین کنفرانس مهندسی برق ایران، تهران، دانشگاه صنعتی امیرکبیر، http://www.civilica.com/Paper-ICEE19-ICEE19_194.html

[۵] ذاکری، زهرا؛ عزیزاله جمشیدی و محمود فرهنگ، ۱۳۹۴، تشخیص کور پارامترهای اسکرمبلرهای مبتنی بر LFSR، هفتمین کنفرانس ملی مهندسی برق و الکترونیک ایران، گناباد، دانشگاه آزاد اسلامی گناباد، http://www.civilica.com/Paper-ICEEE07-ICEEE07_296.html

[۶] هاشم محلوجی، شبیه‌سازی سیستمهای گسسته-پیشامد،چاپ نهم، تهران، مؤسسه انتشارات علمی دانشگاه صنعتی شریف، ۱۳۸۹.

[۷] آقائی، عبداله، زاهدی شولمی، مهدی، "نقش اعداد تصادفی در شبیه سازی و بررسی تحلیلی الگوریتم-های تولید اعداد تصادفی و ارائه روش تلفیقی جدید"، نشریه بین المللی مهندسی صنایع و مدیریت تولید ، دانشگاه علم و صنعت ایران،شماره ۴، جلد ۱۹، صفحه ۲۷-۱۷، زمستان ۱۳۸۷.