IRAQI Academic Scientific Journals
العراقية المجلات الاكاديمية العلمية
مجلة كلية الكوت الجامعة
ISSN (E): 2616 - 7808 II ISSN (P): 2414 - 7419
www.kutcollegejournal.alkutcollege.edu.iq
k.u.c.j.sci@alkutcollege.edu.iq
المجلد 9 ، العدد 2 ، كانون الاول 2024

توليد الأرقام العشوائية وتطبيقها

د. لجين محمد زكي شيت [1]

المستخلص

نعرف الأرقام العشوائية بأنها الأرقام الموزعة بالتساوي عبر مدة زمنية محدودة ولا يمكن معرفة القيم الآتية باعتماد القيم السابقة .

سابقا كان يتم إنشاء أرقام عشوائية باستخدام حجر النرد او بطريقة السحب للمحظوظ إي قابلية التنبؤ ولكن ألان وجدت طرق مختلفة لتوليد الرقم العشوائي وهذه الطرق أكيد اقل قابلية من التنبؤ. وهذه الطرق المكتشفة لها أساليب لتوليد الرقم العشوائي ولها الكثير من التطبيقات المختلفة مثل تشفير البيانات والمحاكاة للأنظمة المعقدة وأيضا البرامج الالكترونية.

في هذه الورقة يتم اعطاء مقدمة في هذه الطرق لتوليد الارقام العشوائية وكيف تولد وتطبيقاتها من أجل العمل والاداء.

الكلمات المفتاحية: الأرقام العشوائية، طرق لتوليد الأرقام، تطبيقات الاعداد العشوائية

انتساب الباحث
[1] كلية التربية الاساسية، جامعة الموصل، العراق، الموصل،41001

[1]lujaenalsufar@uomosul.edu.iq

[1] **المؤلف المراسل**

معلومات البحث
تأريخ النشر : كانون الاول 2024

Random Number Generation and Application

Lugen M. Zake Sheet [1]

Abstract

The Random numbers are numbers chosen from a set at a fixed time.

In the past, the random number was generated from primitive methods, namely prediction or luck. Now I have found many ways to generate the random number, and it certainly has many applications, such as simulations, electronic programs, and others.

In this paper, abbreviations of these methods and their application in terms of performance will be given.

Keywords: Random numbers, methods for generating numbers, random number applications

Affiliations of Author
[1] College Basic Education, University of Mosul, Mosul, Iraq, 41001

[1]lujaenalsufar@uomosul.edu.iq

[1] **Corresponding Author**

Paper Info.
Published: Dec. 2024

المقدمة

إنّ طرق توليد الأرقام العشوائية تستخدم لبناء او إنشاء الرقم العشوائي عن الرقم الذي تم بناءه أو إنشاءه سابقا. وهذه الطرق لها استخدامات عديدة في العلوم والفن والإحصاء والتشفير والألعاب والقمار ومجالات أخرى [1].

هذه الطرق المختلفة سواء القديمة منها والحديثة لتوليد الرقم العشوائي لها بعض الايجابيات والعيوب أيضا ولكل طريقة. هناك نوعان للأرقام العشوائية هي الأرقام العشوائية الحقيقية والأرقام العشوائية الزائفة.

ويميز الأرقام العشوائية الحقيقية بأنها لايمكن التنبؤ به بينما الأرقام العشوائية الزائفة يمكن التنبؤ بها بعد مدة محدودة وهذه المدة تكون كبيرة جدا [1]. وهذا البحث يقدم الطرق المولدة للأرقام العشوائية الزائفة (PRNG).

عرض طرق توليد الأرقام العشوائية الزائفة (PRNG)

هناك العديد من الأوراق البحثية المختلفة فضلا عن الباحثين أيضا الذين حاولوا تطوير خوارزميات مختلفة لتوليد عدد غير منتظم. فمثلا الخوارزمية الزائفة (PRNG) تستخدم لتوليد مجموعات من الأرقام تقترب من الخصائص المختلفة للأرقام العشوائية [1]. فان الأرقام العشوائية الزائفة مهمة في عمليات المحاكاة ومهمة في التشفير وهناك الكثير من الطرق لتوليد هذا الأرقام العشوائية الزائفة. ومن هذه الطرق التي تعتمد على خوارزمية التوليد الزائفة (PRNG) نذكر منها (طريقة Blum Blum Shub، طريقة الضرب التكميلي بالتحميل، طريقة المولد المتطابق

الانعكاسي، طريقة مولد Fibonacci، طريقة المولد التطابق الخطي، طريقة المولد بإزاحة التغذية الراجعية الخطية، طريقة المربع الأوسط، طريقة الضرب بالتحميل، طريقة المولد بالتحويل (Xorshift)، طريقة المولد القائم على العداد، طريقة مولد MIXMAX، طريقة مولد Yarrow، طريقة مولد Blum Micali).

فمثلا قدمت طريقة Blum Blum Shub في عام 1986 من قبل Lenore Blum و Manuel Blum و Michael Shub. إذ إن التسلسل الرقمي شبه العشوائي الذي يتم إنتاجه بواسطة المولد هو وقت متعدد الحدود عشوائي لكل مقطع أولي ثابت. في هذه الطريقة هناك نوعان من المولدات المختلفة التي تم تحديدها. هم مولد (1/P) الذي يمكن التنبؤ به ومولد (x^2 mod n) الذي لا يمكن التنبؤ به. تطبيق هذه الطريقة هي بناء حسب متواليات (de Bruijn) (1)، وتشفير المفتاح العام [2].

والطريقة الآتية هي طريقة الضرب التكميلي بالتحميل ، تستخدم في الطريقة الأعداد الأولية للصيغة الآتية ($ab_r + 1$). هذه الطريقة بسيطة وسريعة وذات جودة جيدة وتتطلب مدة قصيرة. هذه الطريقة تستخدم في تطوير الألعاب [1].

وطريقة المولد المتطابق الانعكاسي هو توليد العدد العشوائي الزائف بالتطابق غير الخطي [2]. يُعبر عن هذه الطريقة أو المولد بواسطة ICG.

وان طريقة مولد Fibonacci هذه الطريقة تمتلك المعادلة الآتية $[(x_n = x_nK + x_nL \pmod M)]$ ؛ حيث ان $K < L$ وان M = الوحدات النمطية وكذلك الأولية، و L = طول التسجيل ، و K = التأخر.

هذه الطريقة المستخدمة في أجهزة الكمبيوتر ويمكن أن توفر حسابًا معياريًا عن طريق اقتطاع جزء التخزين.

فالتحدث عن طريقة مولد التطابق الخطي هو أساس خوارزمية التوليد الزائفة (PRNG) [3]. وان معادلة الطريقة لتوليد الرقم العشوائي هي [$X_n + 1 = (ax_n + c) \bmod m$] " إذ X_n هي تسلسل القيم العشوائية الزائفة ، وان m هو المعامل ، وحيث ان كل من a هو المضاعف ، و c هي الزيادة ، و X_0 هي القيمة الأولية [3]. هذه الطريقة سريعة وتتطلب ذاكرة أقل. لكن هذه الطريقة التي يرمز لها باختصار LCG ليست مفيدة للتطبيق حيث تكون العشوائية المطلوبة عالية الجودة.

ان طريقة المولد بإزاحة التغذية الراجعية الخطية تستخدم لإنشاء سلسلة من نقط الثنائية. وتستخدم هذه الطريقة في العديد من تطبيقات الأجهزة. تقوم هذه الطريقة بإنشاء رقم عشوائي بطريقة سريعة. تُستخدم عملية الازاحة لتوليد رقم عشوائي. لتطبيق هذه الطريقة تستخدم في البث الرقمي والاتصالات[4] .

وطريقة المربع الأوسط هي ان الأرقام الوسطى من الرقم السابق تولد كل رقم متوال . فمثلا في بدء نأخذ قيمة أولية ونحسب مربعًها ثم بعد تربيعه ، نختار الخانات الوسطى لهذا الرقم ونأخذها كقيمة أولية لرقم عشوائي زائف تال [5]. بهذه الطريقة ، تعمل الأرقام الوسطى للأرقام السابقة كقيمة أولية للرقم الآتي [5].

طريقة الضرب بالتحميل هي طريقة تستخدم لتوليد تسلسل عدد صحيح عشوائي من مجموعة أولية مكونة من الاثنين إلى آلاف من القيم الأولية المختارة عشوائيًا [4]. هذه الطريقة تستدعي حسابًا بسيطًا للعدد الصحيح للكمبيوتر وتؤدي إلى توليد سريع جدًا لتسلسلات من الأرقام العشوائية بمدد كبيرة جدًا، تتراوح من 260 إلى 22000000، وهي تعدّ من مزايا هذه الطريقة [4].

طريقة مولد الأرقام العشوائية إزاحة التحويل (Xorshift) عبارة عن فئة من الطرق المولدة للأرقام العشوائية الزائفة (PRNG). عبر الجمع بين العديد من عمليات إزاحة تحويل (Xorshift) ، يمكن الجمع بين مجموعات مولد الارقام العشوائية البسيطة والأسرع. فإذا كان عدد المجموعات فرديًا ، فإن هذه المجموعة الأولية تكون معكوسة. يتطلب ازاحة تحول (Xorshift) رمزًا او كود أقل وحالة صغيرة. هذا هو أسرع مولدات الأرقام العشوائية غير المشفرة الآمنة [6] .

طريقة مولد الأرقام العشوائية المعتمد على العداد ويرمز لها بالرمز (CBRNG) يستخدم للحساب المتوازي. وتعدّ هذه الطريقة القائمة على العداد سريعة وتحتاج إلى حالة صغيرة أو بدون حالة وسهلة التهيئة. لديها مدد طويلة ووافقوها على مجموعة من الاختبارات الإحصائية. تستخدم خوارزميات تولد الأرقام العشوائية المعتمدة على العداد (CBRNG) لتشفير AES وThree fish الكاملة. يتم تضمين أسرع خوارزمية تولد الأرقام العشوائية الزائفة (PRNGs) في عائلات Philox و Three fry [6].

طريقة مولد MIXMAX عبارة عن طريقة مصفوفة N×N تم تطويرها كحل لمشكلة تحديد مولد المصفوفة الأحادية المعيارية ذات القيمة المتكاملة لطرق الأرقام العشوائية الزائفة (PRNs).

حيث ان طريقة مولد MIXMAX أسرع في دقة 24 بت و 48 بت و 32 بت Mersenne Twister.

وان طريقة مولد يارو Yarrow هو تحسين طرق تولد الارقام العشوائية الزائفة (PRNG). ويعيد Yarrow استخدام كتل البناء الموجودة [7]. تم تصميم طريقة Yarrow ليكون آمنًا للتعامل مع هجمات التحليلات، كما أن مولد Yarrow هو الأفضل في معارضة الهجمات [7]. بالنسبة لعدد محدود من بايتات الإخراج، ويعطي مولد yarrow حدودًا للهجوم التراجعي [8].

وطريقة خوارزمية مولد Blum Micali هي مولد آمن مشفر[9]. لنفترض أن x شرطًا فرديًا، وy هو مقياس الجذر البدائي x. و X_0 يكون بذرة أو نقطة البداية، ولنفترض ان ($X_i + 1 = y^{xi} \bmod$ x). إذا كانت (xi= p-1/2)، فإن الناتج i^{th} هو1، وإلا فسيكون 0. يعد حساب اللوغاريتمات المنفصلة modulo p مستحيلًا إذا كانت p كبيرة جدًا وبسبب هذه الخوارزمية أصبحت آمنة [9].

من المناقشة السابقة نستنتج أن لدينا العديد من الطرق لتوليد رقم عشوائي. كل هذه الطرق لها مزايا وعيوب. ولكن من المراجعة أعلاه يمكننا أن نقول بان طريقة الضرب التكميلي بالتحميل هي الطريقة الأفضل لإنشاء رقم عشوائي لبعض التطبيقات التي تعتمد كليًا على العشوائية، كما أن طريقة يارو (yarrow) هي الطريقة المفيدة للأغراض الأمنية.

التطبيق لطريقة الضرب التكميلي بالتحميل

عبر مراجعة كل هذه الطرق يمكننا القول بأن طريقة الضرب التكميلي بالتحميل هي الطريقة التي يمكن استخدامها لتوليد الكابتشا. والتطبيق هو لاستبدال كلمة التحقق لبوابات الويب إذ يتم القيام بذلك أولا نقوم بإنشاء رقم عشوائي ثم نحسب طول هذا الرقم العشوائي. ثم ثانيا نقسّم الرقم العشوائي على مصفوفة من رقمين. إذا كان هناك أي رمز مثلا LFHII للنماذج المكونة من رقمين ، فستقوم وظائف الإنشاء بتحويل هذا الرقم المكون من رقمين إلى الأبجدية ، وإلا احتفظ به كما هو. لذلك سيكون طول الرقم العشوائي المعدل 5- 10. سيتم استخدام هذا الرقم العشوائي بدلاً من رمز التحقق أثناء استخدام بوابات الويب. سيقلل هذا التطبيق من عبء استخدام قواعد البيانات في بوابات الويب لإنشاء كلمة التحقق. وسيتم ذلك عن طريق التحقق من صحة الأرقام العشوائية التي تم إنشاؤها بواسطة الخادم مع إدخال الرقم العشوائي من قبل المستخدم على جانب العميل. تُظهر الصورة الآتية عينة من اختبار الكابتشا (8G5F3).

الاستنتاجات

استعرضت هذه الورقة بإيجاز خوارزميات توليد الأرقام العشوائية. إذ إن الاختيار الصحيح لتقنيات توليد الأرقام العشوائية مهم لتوليد رقم عشوائي لأغراض أمنية. تقدم هذه الورقة لمحة عامة عن خوارزميات توليد الأرقام العشوائية.

المصادر

[1] Marsaglia, George, "Random number generators" Journal of Modern Applied Statistical Methods. (May 2003), 2 (1): 2–13. doi:10.22237/jmasm/1051747320.

[2] L. Blum, M. Blum, and M. Shub " A Simple Unpredictable Pseudo-Random Number Generator" SIAM Journal on Computer, Society for Industrial and Applied Mathematics 003, May 1986, Vol. 15, No. 2.

[3] I. Zelinka et al. " Do Evolutionary Algorithms Indeed Require Random Number " Springer International Publishing Switzerland, AISC 2013, pp. 61–75. doi: 10.1007/978-3-319-00542-3_8 .

[4] Goresky, Mark &Klapper, Andrew. "Efficient multiply-with-carry random number generators with maximal period" ACM Transactions on Modeling and Computer Simulation, (2003), 13 (4): 310–321.

[5] Benjamin Jun and Paul Kocher “The Intel® Random Number Generator” cryptography research, inc. white paper prepared for Intel corporation, 1999, April 22,.

[6] Marsaglia, George "Xorshift RNGs" Journal of Statistical Software, (4 July 2003), 8 (14): PP. 1– 6. doi:10.18637/jss.v008.i14.

[7] M. Santha and U.V. Vazirani, “Generating Quasi-Random Sequences from Slightly Random Sources” Journal of Computer and System Sciences, 1986, Vol. 33, pp. 75–87.

[8] G.B. Agnew, “Random Source for Cryptographic Systems” Advances in Cryptology-Eurocrypt ’87 Proceedings, Springer-Verlag, 1988, pp. 77–81.

[9] M. Blum. and S. Michali, "How to Generate Cryptographically Strong Sequences of Pseudo – Random Bits" Society for Industrial and Applied Mathematics SIAM J. Computer, 1984, Vol.13, No. 4, PP. 850- 864.