A Proposed Method for Arabic Text Random Number Generator using Secret Sharing

[1]Muna Ghazi Abdul Sahib
Computer Science Department, University of Technology, Iraq, 110096@uotechnology.edu.iq

Abstract

The Random Number Generators (RNG_s) are very important in a wide range of applications, the most popular one in security fields rely on the randomness of certain parameters and also in many other fields.

This paper proposed a new algorithm for generating a pseudo random number, based on using secret sharing method. The proposed method takes Arabic text as the seed which represents as the secret value of the secret sharing, then specify the length and range of RNG, after that generating several shares. These shares can be used as the random numbers. The test results show the proposed method has long period and proved the efficient using Arabic text as seed of the RNG.

Keywords: Random number generators, secret sharing, Arabic text.

الخلاصة

إن مولدات العدد العشوائي(RNG_s) مهمه جدا في تشكيلة واسعة من التطبيقات وخاصة في مجال الأمنية الذي يعتمد على العشوائية في بعض المتغيرات وأيضاً في العديد مِنْ المجالات الأخرى.

هذا البحث يقدم خوارزمية جديدة لتُوليّدُ عددَ عشوائيَ مزيّفَ، اساسها إستخدام طريقةِ المشاركة بالسريةِ.حيث تَأْخذُ الطريقةُ المُقتَرَحةُ نَصّاً عربياً كقيمة اولية التي تُمثّلُ القيمة السرية لطريقةِ المشاركة بالسريةِ ، ثمّ تُحدّدُ الطولَ والمدى لمولد العدد العشوائي و بَعْدَ ذلك تَولد عِدّة أسهم، ثمّ هذه الأسهمِ يُمْكِنُ أَنْ نستعملها كأعداد عشوائية.ان نتائج الاختبارات توضح ان الطريقة المقترحة لها فترة طويلة وكذلك اثبتت كفاءة استخدام النص العربي كقيمة اولية لمولد العدد العشوائي.

1. Introduction

Random Number Generators (RNG_s) have an important role in cryptography used for key generation and also have applications in many fields. The programmers recognized the need for a means of providing randomness into a computer program. However, it may seem it is difficult to get a computer to do something by chance. A computer follows the instructions blindly and is therefore completely predictable [1].The RNG is a process that provides random numbers; there are two main approaches to generating random numbers: Pseudo-Random Number Generators (PRNGs) and True Random Number Generators (TRNGs) [1].Secret sharing have been proposed as a solution to create Pseudo Random Number Generator. The idea of secret sharing is to start with a secret, divide it into pieces called shares, which are then distributed among participating individuals by the dealer. Only certain groups of participants can reconstruct the original secret.

The aim of this paper is to propose a new algorithm of Random Number Generator (RNG), based on using secret sharing method.

The rest of this paper are, random number generator in section 2, tests of randomness in section 3, secret sharing in section 4,the proposed method is in section 5, section 6 experiments results, while section 7 is conclusions.

2. Random Number Generator

The Random Number Generators (RNG_s) is a process that provides random numbers, which means the numbers in a sequence are random. The RNG_s have an important role in cryptography system used for generation of cryptographic keys for security and have applications in many fields such as games, roulette, lotteries and draws, statistics, simulation and modeling, computer algorithms , evolutionary algorithms, arts and other fields[2].

There are two types of random numbers [1, 3]:

- Pseudo random numbers are numbers that appear random but are obtained in deterministic ways that use mathematical formulae.
- True random numbers are obtained in non-deterministic ways but use physical phenomena.

2.1 Pseudo Random Number Generator (PRNG):

PRNGs are generators produced through algorithmic techniques that use mathematical formulae to produce sequences of numbers that look like they were really random but in reality, each value is determined based on system's state and is not truly random [3].

Properties of PRNGs [3,4]:

i. Serially uncorrelated:
The sequences of random numbers should be uncorrelated sequence

ii. Lengthy period:
The generator should be of *long period* which means the series of digits should not repeat only after the generation of a very large set of random numbers.

iii. Uniformity:
The sequence of random numbers should be uniform, and unbiased.

iv. Efficiency:
Mean they can produce many numbers in a short time (Fast).

v. Deterministic:
Mean that a given sequence of numbers can be reproduced when the start point of the sequence is known.

2.2 True Random Number Generator (TRNG)

TRNGs produce randomness by use a nondeterministic source referred to as an entropy source; the entropy source is come from the physical phenomenon and introduces it into a computer. The physical phenomenon can be very simple, like the little variations in somebody's mouse movements, the amount of time between keystrokes, the background noise from an office or laboratory and radioactive source also could be use as a physical phenomenon [3, 5].

The properties of TRNGs are not predictable, not a period that meaning the sequence does not repeat itself and inefficient because of it very slow that takes a long time to produce numbers [3, 5].

3. Tests of Randomness

The tests of random generators is used to check if the PRNG is random enough, or in the other word is used to check if the output of PRNG is independent and identically distributed[6, 7]. The following are an overview of some of these randomness tests [6]:

i. Frequency Test:
The frequency test is a simple type of test that could be considered as a first pass. This test uses to compare if the distribution of the set of numbers generated is equal distribution and not bias distribution. If PRNG passes in the frequency test that is not mean its random enough, but if PRNG fails in the frequency test then there is no need for further testing.

ii. Runs Test:
The runs test is used to determine the identical bits in the uninterrupted sequence, or in the other word testing if the actual number of runs of 0's and 1's is as expected for a random sequence.

iii. Poker Test:
The poker test is used to determine if the possible frequency of certain digits repeats in any sequence more than the other possibilities.
For example: 0.577, 0.909, 0.255, 0.414, 0.331

Note in this sequence there is a pair of like digits appear in each number generated.

4. Secret Sharing

A Secret Sharing (SS) is a technique that shows how to divide data D into n pieces, whereas the D can be easy reconstruct. In secret sharing the data D called secret and the pieces called shares [8]. There are two main types of secret sharing which are secret splitting and secret thresholding [9].

4.1 Secret Splitting

In secret splitting, the secret can be splitting into n shares and it requires all the shares to reconstruct the secret. The secret can be splitting either into two shares or into n shares, in both types all of shares will be used to reconstruct the secret. Therefore this type of secret sharing have a problem that is if any of the shares gets lost, then the secret cannot be reconstructed [9].

4.2 Secret Thresholding

In secret thresholding, the secret can be divided into n shares and it only requires specific number of the shares to reconstruct the secret without needs all of the shares [10, 11]. Therefore this type of secret sharing solves the problem of secret splitting because it is not requires all of the shares to reconstruct the secret but only t of shares [10]. The most common method of secret thresholding is Shamir's (*t, n*) threshold method which using interpolation polynomials. The Shamir's (*t, n*) threshold method is defined as the follow [11, 12]:

1. Choose a prime p larger than n (the number of shares) and the secret *S*.

2. Define S to be the constant term a_0 and choose $(t-1)$ random number of the coefficients

$a_1, \cdots, a_{t-1}$, $where\ 0 \le a_j \le p-1.$

3. Construct $f(x_i)$ by using $(t-1)$ degree polynomial, $where\ i = 1\ to\ n, x \in Z_p$

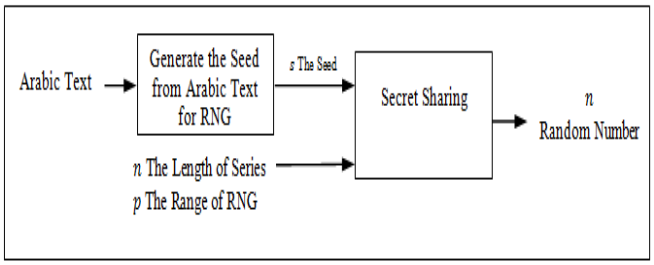
$f(x_i) = \sum_{j=0}^{t-1} a_j\ x^j$.

4. Compute the shares $s_i = f(x_i)\ mod\ p$, and distribute them to *n* users.

Some properties of $(t-1)$ threshold are [8]:
1- The size of each share does not exceed the size of the original data.
2- When t is fixed, the shares can be added, deleted or changed without affecting of the other existing shares.

5. Proposed Method

The proposed method is used the Arabic text as the seed of Random Number Generator (RNG) and using Shamir secret sharing to generate a random number. The process is performed by the following steps: The first step is entering the Arabic text and then taking the ASCII code of the Arabic text to generate the seed that will represent the secret value of the secret sharing. The second step is entering the desired length to generate random numbers with the specified length that will represent the number of shares in secret sharing. The next step will be select integer value to generate random numbers in a selected range. Finally is performing the concept of Shamir secret sharing to generate random numbers. as shown in figure (1).



Figure(1): Illustration RNG by using Arabic text and secret sharing.

Algorithm (1) describes the necessary steps to show how to generate a random number by using Arabic text as seed and Shamir secret sharing:

Algorithm(1): Arabic Text RNG using Shamir Secret Sharing

Input: Arabic text st the seed of RNG, The length of series n , The Range of RNG p .

Output: n Random Number .

Process:

Step 1: Read st , n , p .

Step 2: Split Arabic text string st into letters then computes its ASCII code and puts in array $s_1()$

Step 3: The Seed $s = sum\ s_1\ /\ length\ of\ s_1$

Step 4: Set $a_0 = s\ \ and\ a_1, \cdots, a_{t-1}\ \ random\ \ No.$

$where\ 0 \leq a_j\ \leq p-1\ \ \ , t \leq n$.

Step 5: For $x = 1\ to\ n$

Step 6: $rn_1(x) = \sum_{j=0}^{t-1} a_j\ x^j$.

Step 7: $rn(x) = rn_1(x)\ mod\ p$.

Step 8: End for x

Step 9: rn is array of n Random Number .

Step 10: End

6. Experiments Results

This section presents the results of the tests sets conducted on the established proposed method for generating random numbers with related discussion.

The test results of effects the different Arabic text with specific length and range to the results of random numbers as shown in the table (1).

Table (1): Random numbers of different Arabic text with specific length and Range.

Arabic Text	Length of	Range of	Random Numbers
الجامعة التكنولوجية	7	151	126,70,148,88,142,29,143
بلاد مابين النهرين	7	151	136,55,31,29,53,146,88
وادي الرافدين	7	151	125,87,140,81,56,107,21
بغداد السلام	7	151	63,11,16,73,45,116,36
ارض الحضارات	7	151	72,55,59,61,97,111,106

According to the table (1) when fixing the value of the length and the value of the range and using different Arabic text, the test shows that it is possible to prove each Arabic text that has different results of random numbers which means the efficient using Arabic text as seed of the RNG.

The test results of effects the specific Arabic text with different length and range to the results of random numbers as shown in the table (2).

Table (2): Random numbers of specific Arabic text with different length and Range.

Arabic Text	Length of series	Range of RNG	Random Numbers
الجامعة التكنولوجية	5	17	16,3,9,10,14
الجامعة التكنولوجية	10	37	11,5,24,12,21,26,36,20,18,30
الجامعة التكنولوجية	16	73	2,23,37,50,14,46,63,1,34,63,8,27,5,65,57,69
الجامعة التكنولوجية	21	131	19,59,98,54,122,119,8,29,44,61,103, 77,36,48,65,54,128,22,10,119,129
الجامعة التكنولوجية	27	211	119,168,190,123,6,190,72,205, 188,143,82,118,43,172,77,64,118, 114,28,148,19,131,20,167,99,77,41

According to the table (2) when fixing the Arabic text and using different value of the length and range, the test shows that the proposed method of the RNG has long period which means the efficient using Shamir secret sharing to generate random numbers.

In order to test the randomness of the proposed method, the three types of randomness tests (frequency test, runs test and poker test) have been tested to check if the RNG of the proposed method is random enough. This is done by using CrypTool software [6]. Table (3) shows the results of randomness tests of proposed RNG.

Table (3): Randomness Tests Results.

No.	Test Name	Test Result
1	FREQUENCY TEST	Frequency Test Passed
2	RUN TEST	Runs Test Passed , Long Runs Test Passed
3	POKER TEST	Poker Test Passed

7. Conclusions

The proposed method uses the technique of secret sharing to provide RNG, by taking the Arabic text seed as the secret value then generating several shares as the desired length of random numbers. The proposed method has good randomness performance that shows the effectiveness use of Arabic text based RNG. So that, when using the encryption will enhance the level of security.

REFERENCES

[1] W. Stallings, "Cryptography and Network Security: Principles and Practice", Fifth Edition, Prentice Hall, 2011.

[2] D. Biebighauser," Testing Random Number Generators", University of Minnesota - Twin Cities- REU Summer 2000.

[3] M. Haahr, "Introduction to Randomness and Random Numbers", Randomness and Integrity Services Ltd, Random .ORG, 2016, URL: http:// WWW.RANDOM.ORG

[4] V. Bhatnagar and C. Cheruvu , "Pseudo Random and Random Numbers", IISTE Journals
Malcolm Manly, 2014.

[5] D. DiCarlo, " Random Number Generation: Types and Techniques", Liberty University,
Spring 2012.

[6] C. Easttom, "Modern Cryptography: Applied Mathematics for Encryption and Informanion Security", 2016, WWW.CRYPTOOL.ORG

[7] C. Dutang and D. Wuertz," A note on random number generation", overview of random generation algoritms , September 2009.

[8] A. Shamir, "How to Share a Secret", Communications of the ACM, Vol. 22, No. 11, pp 612–613, 1979.

[9] L. Grant B. Fleming," Secret Sharing and Splitting", Notre Dame, IN – December16, 2002.

[10] C. Gidney," Rational Secret Sharing With and Without Synchronous Broadcast, Conspicuous Secrets, Malicious Players and Unbounded Opponents",Dalhousie University, March 2012.

[11] M. Mortensen, "Secret Sharing & Secure Multi Party Computation", Chalmers,December 2015.

[12] J. Leiwo, "Secret Sharing", Nanyang Technological University, 2004.