(2,1)-Lagged Fibonacci Generators Using Elliptic Curves over Finite Fields

Shankar B R[1] and Karuna Kamath K[2]
[1]Dept.of Mathematical And Computational Sciences,NITK,Surathkal,India-575 025
[2]Dept.of Computer Applications,NMAM Institute of Technology,Nitte,Karnataka, India-574 110

E mail:[1]brs@nitk.ac.in [2]karunapandit@rediffmail.com

Abstract

A novel pseudorandom sequence generator is presented in this paper. The genesis of this new generator is evolved from the concept of Lagged Fibonacci generator[1] *applied to points on elliptic curves over a finite field. It is observed that the generator has a long period. Also a successful statistical testing of the randomness attributes of the given generator, in accordance with the National Institute of Standards and Technology test suite, admits to a key stream source that is in conformance with the Advanced Encryption Standard for data encryption.*

1. Introduction:

Pseudorandom sequence generators are commonly used in cryptography for stream ciphers [2].The use of elliptic curves in cryptography (ECC) has been more popular since one may obtain the same level of security for much shorter key lengths compared to other crypto systems.

Lagged –Fibonacci generators may be described as follows:

Let X= $\{x_1, x_2, x_3$ --------, $x_r\}$ be a finite set of r elements, all from the some finite set S on which there is defined a binary operation *.The function f is defined by

$f(x_1, x_2, x_3$ ----, $x_r) = (x_1, x_2, x_3$ ---, $x_r\ x_1 * x_{r+1-s})$.

More explicitly, the sequence is described by a set of 'r' seed values followed by a rule for generating succeeding values, x_1, x_2, x_3 --------, x_r, x_{r+1} ------- with $x_n = x_{n-r} * x_{n-s}$. Such generators are denoted by F(r, s,*) and called (r, s)-lagged Fibonacci generator [1]. In this paper, we consider r = 2, s=1, the finite set S consists of all points on an elliptic curve over a finite field, the binary operation * being the usual law of addition of points on elliptic curves[4].

A cubic equation of the form $y^2 = x^3 + a\,x^2 + b\,x + c$ is called an Elliptic curve. Using suitable transformation of the coordinates this can be expressed as $y^2 = x^3 + a\,x + b$, called the Weierstrass normal form. a ,b ,x and y all vary over R or C or Q or a finite field Fq where q is a power of a prime. We add a special point to the curve ∞, called the point at infinity. The addition of points is defined as follows:

Let $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ be 2 points such that $P_1, P_2 \neq \infty$

1. If $x_1 \neq x_2$, $x_3 = m^2 - x_1 - x_2$, $y_3 = m(x_1 - x_3) - y_1$, where $m = (y_2 - y_1)/(x_2 - x_1)$.
2. $x_1 = x_2$ but $y_1 \neq y_2$, $P_1 + P_2 = \infty$.
3. If $P_1 = P_2$ and $y_1 \neq 0$, $x_3 = m^2 - 2x_1$ and $y_3 = m(x_1 - x_3) - y_1$, $m = (3x_1^2 + a)/2y_1$.
4. If $P_1 = P_2$ and $y_1 = 0$ then $P_1 + P_2 = \infty$

With this definition of addition the set of all points on the elliptic curve forms an abelian group, with ∞ as additive identity.

2. Proposed generator:

1. Select an Elliptic curve E over the Galois field GF (p).
2. Choose two points (x_1, y_1), (x_2, y_2) on E.
3. Apply Lagged Fibonacci F(2,1, *)generator.
4. If $x_1 = x_2$, the resulting point is point at infinity. Go to step 2.

The x coordinate or y coordinate or even XOR (after converting to binary) of these two can be taken as random sequence [5].

3. Properties

A good Pseudorandom sequence generator worthy of consideration for encryption purposes is characterized by the following properties. [6]

- Long period: The generator should have long enough period in order to avoid the repetition of the sequence after a short length of time.
- High linear complexity: Sequence with low linear complexity is easily predictable and susceptible to attack based on their linear structure.
- Reproducibility: identical output sequences are generated for a given seed.

978-0-7695-3521-0/09 $25.00 © 2009 IEEE
DOI 10.1109/ICCET.2009.103

❖ Statistical Properties: The generator must pass a battery of statistical tests to confirm its randomness attributes.[3]

The sequence produced by the proposed generator was analyzed and tested for conformance to the above characteristics. This analysis is important to check the quality of the sequence produced and thus establish confidence in its use for key stream generation.

A. The generated random number sequence has a long period as desired. The Table gives a sample list from a large set of primes p considered.
E: $y^2 = x^3 + x + 1$

p	Period
131	96
151	240
173	264
239	390
263	420
281	612
397	748
421	900

B. The linear complexity is an important concept in the analysis of stream ciphers. Any sequence produced over a finite field has a finite linear complexity[2]. The linear complexity of an infinite sequence s is
   - Zero if s is a zero sequence
   - ∞ if no LFSR generates s
   - Length of shortest LFSR that can generate s[7]

   The linear complexity was found to increase with the value of p.

C. Statistical Properties: The NIST test suite[3] was applied to pseudorandom sequence produced by the generator. This test suite is used as a bench mark by NIST in the evaluation of possible candidate generators for the AES. The suite conducts a comprehensive battery of Statistical tests in which there are 16 core test strategies. The results of the tests were found to be satisfactory.

4. Conclusion

The generator presented in this paper exhibits good randomness properties, in accordance with NIST statistical test suite. This may permit its usage to be considered for cryptographic applications.

5. REFERENCES

[1] George Marsagalia, The Mathematics of Random Number Generators, Proceedings of Symposia in Applied Mathematics, American Mathematical Society , Rhode Island, vol.46,1992.

[2] J. L. Massey, "Cryptography and System Theory", Proc. 24th Allerton Conf. Comm., Control, Computing, pp. 1-8, October, 1986.

[3] NIST, Special Publication: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,2001, available online http://csrc.nist.gov/rng/

[4] Neal Koblitz, " A Course in Number Theory and Cryptography" Springer-verlag,2nd Edition ,1994

[5] Shankar B R, Karuna Kamath K. Pseudorandom numbers using Elliptic curves and Linear Feed Back Shift Registers, Proceedings of National workshop on Cryptology, Hyderabad, India, August 2008.

[6] R. Mita et. al., "A Novel Pseudorandom Bit Generator for Cryptographic Applications", Electronics, Circuits and Systems. 9th International IEEE Conference 489-492 vol.2, 2002.

[7] A. J. Menezes et. al., Handbook of Applied Crytptography, CRC Press, 1996.