Pseudorandom generators based on Lucas Sequences .

A. Di Porto - W. Wolfowicz
Fondazione Ugo Bordoni, Rome, Italy

Abstract: Pseudo-random sequence generators are the heart of stream-cipher systems. This work presents some design criteria for such generators, based on innovative methods. To this aim the Lucas Sequences, reduced modulo a prime p, are taken and suitably manipulated. Modular Exponentiation is the function used to attain the output sequences. The periodicity of the Lucas Sequences allows to define a lower bound for the period of the generated sequences; actually our purpose is to ensure that the sequences which are generated have a period greater than a prefixed value. Furthermore the cryptographic strength of these sequences relies on the one-wayness of the discrete logarithm problem.

1. INTRODUCTION

The pseudorandom sequence generators are the main part of stream-cipher cryptographic devices [1].

Several studies pertaining the definition of pseudo-randomness of a sequence, lead to a large number of works both theoretical and applicative [1,2,3,4,5] where tools belonging to different branches of mathematics are used.

We address to specific publications for the different definitions of pseudorandom sequence and we suppose that the reader is familiar with the meaning and implications of the cryptographic algorithms, and in particular of stream-ciphers.

The aim of this work is to define some non conventional pseudorandom sequence generator, based on mathematical and implementative hypotesis different from those of most generators proposed in the past.

In this work some generator based on modular exponentiation will be examined, utilizing the special sequences of the Lucas Numbers. In these generators the minimum period of the sequences can be taken as a design parameter. For this purpose some elements of Number Theory and the properties of the Lucas Sequences are recalled in section 2; the generators we propose are described and analyzed in section 3 and 4.

Work carried out in the framework of the agreement between the Italian PT Administration and the Fondazione "Ugo Bordoni".

2. FUNDAMENTALS OF NUMBER THEORY REQUIRED FOR THE GENERATOR DESIGN

In this section some definition and fundamental theorem of Number Theory which will be necessary in the generator design, are recalled. Notice that it is not our intention to give here a systematic treatment, which would need much more than only one section; we wish to give the reader a set of notions which are necessary to the following of this paper. We refer to the literature [6,7,8] for a deep insight of the subject.

Let us define *Generalized Lucas Sequence with parameter* s the sequence:

$$V_i(s) = sV_{i-1}(s) + V_{i-2}(s) \tag{1}$$

being s an integer and with the initial conditions

$$V_o(s) = 2 \quad , \quad V_1(s) = s \tag{2}$$

It is proved [6,9,10] that the sequence defined by (1) and (2), reduced modulo an integer n, is periodic, with period T.

Some interesting consideration can be made regarding such period. In particular:

- the sequence $V_i(s) \mod 2^k$, $k \geq 1$, has period $T = 3 \cdot 2^{k-1}$, when s is odd;
- the sequence $V_i(s) \mod 2$ has period $T = 1$, when s is even;
- the sequence $V_i(s) \mod 4$ or $\mod 8$ has period $T = 1$ or $T = 4$ respectively, when $s = 2(2t + 1)$;
- the sequence $V_i(s) \mod 2^k$ has:

  $T = 2^{k-2}$, when $s = 2(2t + 1)$, $k \geq 4$;
  $T = 2$, when $s = 2^v(2t + 1)$, $v \geq 2$, $2 \leq k \leq v$;
  $T = 2^{k-v}$, when $s = 2^v(2t + 1)$, $v \geq 2$, $k > v$;

- given a prime $p > 2$:
  - the period T of $V_i(s) \mod p$ is always an even number greater than 2;
  - if $s^2 + 4$ is a Quadratic Residue[1] (QR) mod p, then the period T of $V_i(s) \mod p$ is p -1 or a divisor of p-1;

[1] Given a prime p, the integer a is said to be a quadratic residue mod p , if the congruence $x^2 \equiv a \mod p$ has solutions.

- if $s^2 + 4$ is not a Quadratic Residue (NQR) mod p, then the period T of $V_i(s)$ mod p is $2(p+1)$ or a divisor of $2(p+1)$. Furthermore, if $p+1 = 2^{\alpha}(2k+1)$ with $\alpha \geq 1$, then $T \geq 2^{\alpha+1}$ always;
- let T the period of $V_i(s)$ mod p, then the period of $V_i(s)$ mod p^k, $k \geq 1$, is a divisor of $T \cdot p^{k-1}$.

3. Generators based on modular exponentiation of Lucas Sequences

The content of previous works [4,5] allows to design pseudorandom number generators, taking the period of the generated sequences as a design parameter. Actually the periodicity of the generalized Lucas Sequences when taken modulo a prime p, can be a very useful tool for our purposes. Moreover modular exponentiation of these sequences, as it will be considered in the sequel of this work, allows us to attain unpredictability of the generated sequences and their cryptographic strength, with respect to the previous defined parameter s of the eqns. (1) and (2), when it is considered as a part of the cryptographic key.

Let us consider the two following Lucas Sequences

$$V_h(m) = mV_{h-1}(m) + V_{h-2}(m)\,; \quad h=h_0, h_0+1, h_0+2, \ldots \text{ and } m \geq 1 \tag{3}$$

$$V_k(n) = nV_{k-1}(n) + V_{k-2}(n)\,; \quad k=k_0, k_0+1, k_0+2, \ldots \text{ and } n \geq 1\,. \tag{4}$$

Notice that the values $V_{h_0}(m)$ and $V_{k_0}(n)$ can be reached, for every h_0 and k_0 in a logarithmic number of steps, according to the results given in [11,12], instead of applying the recursion indicated by (3) and (4).

Let us consider the sequence given by the following formula

$$C_i = V_h(m)^{V_k(n)} \pmod p\,; \quad i=0, 1, 2, \ldots; \quad h=h_0+i\,; \quad k=k_0+i\,; \tag{5}$$

substituting in eqn. (5) the expressions (3), (4) we get

$$C_i = (mV_{h-1}(m)+V_{h-2}(m))^{nV_{k-1}(n)+V_{k-2}(n)} = \tag{6}$$

$$\sum_{t=0}^{nV_{k-1}(n)+V_{k-2}(n)} \binom{nV_{k-1}(n)+V_{k-2}(n)}{t} (m\,V_{h-1}(m))^{nV_{k-1}(n)+V_{k-2}(n)-t}(V_{h-2}(m))^t =$$

$$m^{nV_{k-1}(n)}(C_{i-1})^n \sum_{t=0}^{V_{k-2}(n)} \binom{nV_{k-1}(n)+V_{k-2}(n)}{t} (m\ V_{h-1}(m)\ )^{V_{k-2}(n)-t}\ (V_{h-2}(m))^t +$$

$$+ \sum_{t=V_{k-2}(n)+1}^{nV_{k-1}(n)+V_{k-2}(n)} \binom{nV_{k-1}(n)+V_{k-2}(n)}{t} (m\ V_{h-1}(m)\ )^{nV_{k-1}(n)+V_{k-2}(n)-t}\ (V_{h-2}(m)\ )^t .$$

From the above expression (6) we can see how the symbol C_i is a function of the previous generated symbol C_{i-1} and of the parameters m and n.

Notice that, if we take m and n as a part of the cryptographic key, the difficulty to find them, given C_i and C_{i-1}, is the same as solving the discrete logarithm problem.

Actually, further algebraic manipulation of (6) can lead to a general expression of (5) having the form

$$C_i \equiv f\,(C_{i-1},\, C_{i-2},\, m,\, n\,) \pmod p\ , \tag{7}$$

but it could be seen that finding m and n, given C_i ,C_{i-1} and C_{i-2}, implies always an inversion of several modular exponentiations.

The equation (5) can be rewritten by Fermat little theorem [6], as follows

$$C_i = <<V_h(m)>_p{}^{<V_k(n)>_{p-1}}>_p \tag{8}$$

where $< x >_p$ denotes the residue of x mod p.

In order to define the period of the sequence $\{C_i\}$, p must be chosen in an appropriate way; according to the choice of p, the parameters m and n play a fundamental role to allow a period long enough for cryptographic purposes.

In the sequel, different possibilities will be shown as far as the expression of p is concerned, and the period will be determined according to the quadratic residuosity of $m^2 + 4$ and $n^2 + 4$. To this regard it is important to notice that a good level of freedom on the choiche of m and n with respect to p, still remains. Actually, for a given p, it can be proven that the number of values of m, $0 \le m \le p - 1$, for which it results $m^2 + 4$ quadratic residue mod p, is $(p + 1) / 2$ or $(p - 1) / 2$ depending on p. The demonstration of this assertion is straightforward and we omit it for sake of brevity.

In the following two examples are given to show how the choiche of p, m and n can be utilized for the design of our generators based on the modular exponentiation of the Lucas Sequences, and how a lower bound for the period of the generated sequences can be attained.

3.1 Generator with $p = 2q + 1$

If $p = 2q + 1$, with q prime, the formula (8) takes the expression

$$C_i = <<V_h(m)>_{2q+1}{}^{<V_k(n)>_{2q}}>_{2q+1} . \tag{9}$$

The choice of the parameters m and n, makes possible the following four cases

Case 1:

$m^2 + 4$ QR mod $2q + 1$

$n^2 + 4$ QR mod q

In such a case the period of the sequence $V_i(m)$ mod $2q + 1$ is a divisor of $2q$, and, being q a prime, it is equal to $2q$.

For the period of $V_i(n)$ mod $2q$ the following considerations can be made: it is the least common multiple between the periods of $V_i(n)$ mod 2 and $V_i(n)$ mod q ; the first of such periods is 1 or 3 depending on the fact if n is even or odd respectively, while the second period is equal to q-1 or to one of its divisors, then it is greater than or equal to 4.

Hence the sequence defined by the eqn. (9) has a period T which equals the least common multiple between the periods of the Lucas sequences respectively base and exponent of the expression (9), and for the above considerations, it results that:

$$T \geq 4q \sim p \tag{10}$$

Case 2:

$m^2 + 4$ QR mod $2q + 1$

$n^2 + 4$ NQR mod q

Then, for the period of $V_i(m)$ mod $2q + 1$, all the considerations of case 1 hold again, while for the period of the sequence $V_i(n)$ mod $2q$ we have: the period of $V_i(n)$ mod 2, is 1 or 3 depending on the fact if n is even or odd; the period of the sequence $V_i(n)$ mod q is greater than or equal to $2^{\alpha+1}$, being $q + 1 = 2^{\alpha}(2k + 1)$, $\alpha \geq 1$. It is possible to conclude that the period T of the sequence defined by the (9) is

$$T \geq 2^{\alpha+1} q \geq 4q \sim p \tag{11}$$

Case 3:

$m^2 + 4$ NQR mod $2q + 1$

$n^2 + 4$ QR mod q

The period of the sequence $V_i(m)$ mod $2q + 1$ is greater than or equal to $2^{\alpha+2}$, being again $q + 1 = 2^{\alpha}(2k + 1)$, $\alpha \geq 1$; the period of the sequence $V_i(n)$ is ≥ 4. In this case it is possible only to say that the period T defined by eqn (9) is:

(12) $$T \geq 2^{\alpha+2} \geq 8$$

Case 4: $m^2 + 4$ NQR mod $2q + 1$
$n^2 + 4$ NQR mod q;

then, again under the hypotesis that $q + 1 = 2^{\alpha}\ (2k + 1)$, $\alpha \geq 1$, the period of the sequence $V_i(m)$ mod $2q + 1$ is $\geq 2^{\alpha+2}$ and the period of the sequence $V_i(n)$ mod q is $\geq 2^{\alpha+1}$.

Hence for the period T of the sequence defined by the (5) we have

(13) $$T \geq 2^{\alpha+2} \geq 8$$

3.2 Generator with $p = 2q - 1$

If $p = 2q - 1$ the equation (8) takes the expression

(14) $$C_i = <<V_h(m)>_{2q-1}{}^{<V_k(n)>_{2q-2}}>_{2q-1} .$$

In order to attain a long period of the sequence generated by eqn. (14) it is sufficient, in this case, to consider only the case $m^2 + 4$ NQR mod p. According to this choiche[10] the sequence $V_i(m)$ has a period equal to $4q$.
Hence the period T of the sequence generated by (14) is

(15) $$T \geq 4q \sim p .$$

From the above considerations it turns out that the generators based on modular exponentiation of Lucas Sequences, defined by equations (8), (1) and (2), generate sequences whith a period greater than or equal to a prefixed value, if the parameters m, n and p are properly chosen (as in the cases 1 and 2 of sec. 3.1 and in sec. 3.2)

To give an idea of the magnitude order of the acceptable values for cryptographic purposes, the sequence generated by the algorithm expressed by (8), has a period of the order 10^{100} if m , n and p are chosen around 10^{100}

4. PSEUDORANDOM GENERATOR

The above generators could be used for cryptographic purposes, because of the unpredictability of the generated sequences. Moreover the possibility of controlling their period is a highly desirable property. Nevertheless a good statistical balancement must be guaranteed. This can be easily obtained by a self-synchronizing scrambler[13], whose input-output equation is

$$y(k) = \sum_{i=1}^{L} c_i\, y(k-i) + u(k) \tag{16}$$

where $u(k)$ and $y(k)$ are the input and the output sequences respectively, c_i, $i=1,..,L$, are p-ary multipliers, and all the calculations are performed mod p.

Globally the final scheme of the pseudorandom generator is represented in fig. 1, where p, m and n are the cryptographic key and the scrambler is completely defined by its characteristic polynomial[14], which can also be considered as a part of the cryptographic key.

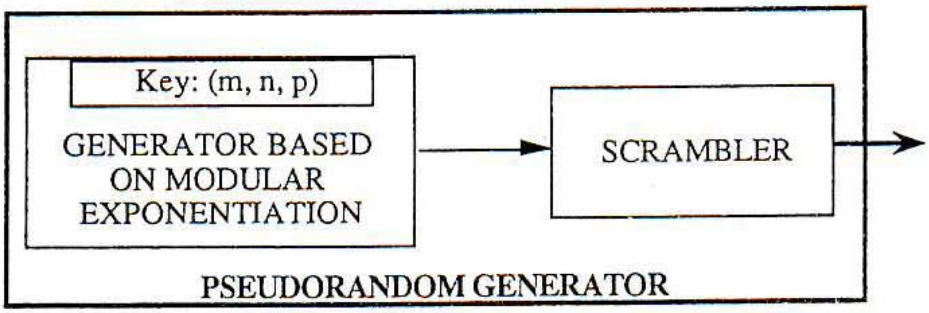

Fig. 1

5. CONCLUSIONS

By the results presented in this work it turns out that the use of the generalized Lucas Sequences allows to attain a pseudorandom number generator, having the period of the generated sequence greater than a prefixed value. This property can be used to generate sequences for cryptographic purposes. Nevertheless the difficulty of designing fast modular exponentiators on large numbers is still to be solved; a great amount of works in this area is being in progress, mainly for VLSI implementation of RSA co-decoders [15].

REFERENCES

[1] W.Diffie, M. E. Hellman : "*Privacy and Authentication: an Introduction to Cryptography.*" Proc. IEEE, Vol. 67, pp. 397-427, March. 1979.

[2] D. Knuth : "*The Art of Computer Programming.*" Vol. 2, *Seminumerical Algorithms*, Addison-Wesley, Reading, Mass., 1969.

[3] S. W. Golomb: "*Shift Register Sequences.*" Holden Day, S. Francisco, 1967.

[4] O. Goldreich, H. Krawczyk, M. Luby: "*On the Existence of Pseudorandom Generators.*", presented at Crypto '88, S. Barbara, Aug. 1988.

[5] S. Micali, C.P. Schnorr: "*Efficient, Perfect Random Number Generatoris*", presented at Crypto '88, S. Barbara, Aug. 1988.

[6] G. H. Hardy, E. M. Wright: "*An Introduction to the Theory of Numbers.*" Oxford at the Clarendon Press, 1945.

[7] I. M. Vinogradov: "*Elements of Number Theory.*" Dover Publications, inc. New York, 1954.

[8] A. Di Porto, P. Filipponi: "*A Probabilistic Primality Test Based on the Properties of Certain Generalized Lucas Numbers.*" Lecture Notes in Computer Science, Vol. 330, pp.211-223, Springer - Verlag 1988.

[9] Bro. A. Brousseau: "*An Introduction to Fibonacci Discovery.*" Santa Clara (CA): The Fibonacci Association, 1965.

[10] A. Di Porto: "*Periodo di Sequenze di Lucas ridotte modulo una potenza intera di 2; considerazioni sugli Pseudoprimi pari di Fibonacci*",FUB Internal Report 3B3490, nov. 1990.

[11] H. Riesel: "*Prime Numbers and Computer Methods for Factorization.*" Birkhäuser, 1985.

[12] A. Di Porto, P. Filipponi, E. Montolivo: "*An Efficient Algorithm for Finding Large Probable Primes*" Note Recensioni e Notizie, Vol.XXXVII, n. 3-4, July-December 1988, pp. 163-168.

[13] O. Brugia: Private communication.

[14] J. E. Savage: "*Some Simple Self-Synchronizing Digital Data Scramblers*", Bell System Tech .Journal, Vol. 46, n.2, feb. 1967, pp. 449-87.

[15] M. Bucci, A. Di Porto: "*Fast Serial-Parallel Multipliers* " Proc of 6th. International Conference, AAECC-6. Lecture Notes in Computer Science, Springer-Verlag, 1989, pp.111-121.