Relationship between Fibonacci and Lucas sequences and their application in Symmetric Cryptosystems

A. Luma and B. Raufi

***Abstract*—** Identification whether a certain number belongs to either Fibonacci or Lucas sequence is computationally intense task in the sense that the sequence itself need to be written from the beginning until the requested number. In this paper we present a method of detecting whether a certain number is of Lucas or Fibonacci sequence as well as introduce relationships between such sequences. This relationship is being used for creation of encryption/decryption methods by utilizing symmetrical key generated by elements of both Lucas and Fibonacci sequences. The strength of this symmetrical cryptosystem lies in the introduced mathematical operators called pentors and ultra pentors which are hard to generate and guess by brute force computation.

***Keywords*—** cryptography, key encryption. Fibonacci sequence, Lucas sequence

I. Introduction

Common problem in Fibonacci and Lucas sequences lies in the inability to detect whether a certain number x is of the above mentioned sequence. In traditional methods, this has been determined by writing the complete sequence from the beginning until the number itself.

A Fibonacci sequence represents a sequence of numbers where the current member is calculated as a sum of two previous consecutive numbers [4]. For example, the sequence:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, ...$$

Is a Fibonacci sequence, where $F_0 = 0$ and $F_1 = 1$ out of which the whole sequence can be generated using the equation:

$$F_n = F_{n-2} + F_{n-1}$$

Lucas sequence on the other hand represents a sequence of numbers where the current member is also calculated as a sum of two previous consecutive numbers where the initial number is 2. For example, the sequence:

$$2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, ...$$

Is a Lucas sequence, where $L_0 = 2$ and $L_1 = 1$ out of which the whole sequence can be generated using the equation:

$$L_n = L_{n-2} + L_{n-1}$$

For Fibonacci sequence, let us have the trinomial square:

$$W^2 \pm W - 1 = 0$$

From which three theorems can be derived [1].

Theorem 1: *For Fibonacci sequence $F_n, n \in N$, it holds that:*

$$F_{n-1} + F_n = F_{n+1}, n > 1$$

Theorem 2: *For odd numbers of Fibonacci sequence $F_n, n \in N$, it holds that:*

$$F_{2n-1} + F_{2n+1} = F_{2n}^2 + 1$$

Theorem 3: *For even numbers of Fibonacci sequence $F_n, n \in N$, it holds that:*

$$F_{2n} \cdot F_{2n+2} = F_{2n}^2 - 1$$

Based on Theorem 2 it can be written that:

$$F_{2n}^2 = (F_{2n+1} + F_{2n-1})^2 - 4 \cdot (F_{2n}^2 + 1)$$
$$F_{2n}^2 = (F_{2n+1} + F_{2n-1})^2 - 4 \cdot F_{2n}^2 - 4$$
$$5 \cdot F_{2n}^2 + 4 = (F_{2n+1} + F_{2n-1})^2$$
$$5 \cdot F_{2n}^2 + 4 = (F_{2n+1} + F_{2n-1})^2 = \Omega^2$$

Ω is the sum of two adjacent members of F_{2n}, Fibonacci sequences. We can prove in the same way that:

$$5 \cdot F_{2n+1}^2 - 4 = (F_{2n} + F_{2n+2})^2 = \Psi^2$$

where Ψ is the sum of two adjacent members of $F_{2 \cdot n+1}$.

Based on the above-mentioned equations, we can test wthether a given number x, belongs to Fibonacci's sequence. We can also use this to find a sequence of Fibonacci's numbers starting from any number x. If x, satisfies the relation $5 \cdot x^2 \pm 4 = \lambda^2$, we can say that it is Fibonacci's

Manuscript received June 30, 2010.

A. Luma is with the South East European University, Computer Science Department. Ilindenska, nn 1200, FYROM. Phone: +389 44 356 166; fax: +389 44 356 001; e-mail: a.luma@seeu.edu.mk).

B. Raufi is with the South East European University, Computer Science Department. Ilindenska, nn 1200, FYROM. Phone: +389 44 356 168; fax: +389 44 356 001; e-mail: b.raufi@seeu.edu.mk).

number and we mark it as $x = F_n$. Based on the pair (F_n, λ), we can find the preceeding F_{n-1} and the succeeding F_{n+1}, F_n through eqations.

$$F_{n-1} = \frac{\lambda - F_n}{2} \qquad and \qquad F_{n+1} = \frac{\lambda + F_n}{2}$$

Since we have found the elements of Fibonacci's series F_{n-1}, F_n, F_{n+1}, based on these three elements, we can construct the whole sequence of Fibonacci's numbers:

$$0, 1, 1, 2, 3, 5, \cdots, F_{n-3}, F_{n-2}, F_{n-1}, F_n, F_{n+1}, F_{n+2}, F_{n+3}, \cdots$$

Based on general form of Fibonacci sequence, elements of the Lucas sequence can be generated using the equation [2].

$$L_{n-m-1} = \frac{F_n \pm F_{n-2m}}{F_{n-m}}$$

From which three theorems can also be derived [2]:

Theorem 1: *For Lucas sequence $L_n, n \in N$, it holds that:*

$$L_{n-1} + L_n = L_{n+1}, n > 1$$

Theorem 2: *For odd numbers of Lucas sequence $L_n, n \in N$, it holds that:*

$$L_{2n-1} + L_{2n+1} = L_{2n}^2 + 5$$

Theorem 3: *For even numbers of Lucas sequence $L_n, n \in N$, it holds that:*

$$L_{2n} \cdot L_{2n+2} = L_{2n}^2 - 5$$

Based on Theorem 2 its can be stated that:

$$L_{2n}^2 = (L_{2n+1} + L_{2n-1})^2 - 4 \cdot (L_{2n}^2 + 5)$$
$$L_{2n}^2 = (L_{2n+1} + L_{2n-1})^2 - 4 \cdot L_{2n}^2 - 20$$
$$5 \cdot L_{2n}^2 + 20 = (L_{2n+1} + L_{2n-1})^2$$
$$5 \cdot L_{2n}^2 + 20 = (L_{2n+1} + L_{2n-1})^2 = \Omega^2$$

where Ω is the sum of two adjacent members of L_{2n}, Lucas sequence. We can prove in the same way that:

$$5 \cdot L_{2n+1}^2 - 20 = (L_{2n} + L_{2n+2})^2 = \Psi^2$$

where Ψ is the sum of two adjacent members of L_{2n+1}.

Based on the above-mentioned relations, we can test the same way, as in Fibonacci sequences, wthether a given number x, belongs to Lucas sequence. We can also use this to find Lucas sequence numbers starting from any given number x. If x, completes the relation $5 \cdot x^2 \pm 20 = \lambda^2$, we can say that it is Lucas number and we mark it as $x = L_n$. Based on the pair (L_n, λ), we can find the preceeding L_{n-1} and the succeeding L_{n+1} , L_n.

$$L_{n-1} = \frac{\lambda - L_n}{2} \qquad and \qquad L_{n+1} = \frac{\lambda + L_n}{2}$$

Since we have found the elements of Lucas sequence L_{n-1}, L_n, L_{n+1}, based on these three elements, we can construct the whole series of Lucas numbers as follows [5]:

$$2, 1, 3, 4, 7, 11, \cdots, L_{n-3}, L_{n-2}, L_{n-1}, L_n, L_{n+1}, L_{n+2}, L_{n+3}, \cdots$$

The rest of the paper is structured as follows: In section 2 we introduce the related work done regarding encryption/decryption algorithms using the above mentioned sequences. Section 3 introduces a novel approach on linking between Fibonacci and Lucas sequences. Section 4 introduces a case study with asymmetrical encryption using the above mentioned sequences and section 5 concludes this work and outlines some future directions.

II. RELATED WORK

Both, Fibonacci and Lucas sequences can be used for encryption/decryption purposes. The most important element of such a process is the creation of encryption/decryption key.

The encryption/decryption key is created based on level of the key itself. This key represents a vector, where the number of members in such vector is determined by the equation [1], [2]:

$$N = 2m + 1$$

Where m is the level of the key and N is the number of vector's elements. The overall scheme for key generation for both, Fibonacci and Lucas sequences is depicted as in fig 1.

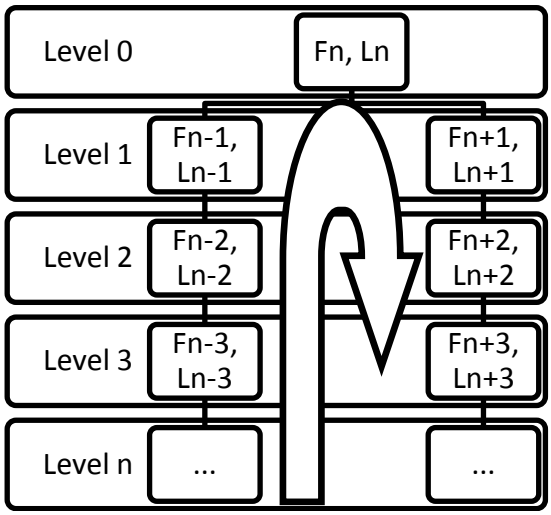

Fig. 1 Key generation based on levels

For example if we take $m = 2$, then its successive keys generated are:

$$F_{n-2}, F_{n-1}, F_n, F_{n+1}, F_{n+2}$$

and

$$F_{n-2}, F_{n-1}, F_n, F_{n+1}, F_{n+2}$$

for Fibonacci and Lucas sequences respectively.

III. LINK BETWEEN FIBONACCI AND LUCAS SEQUENCE

Based on Fibonacci and Lucas sequences, all geometrical angled forms and their respective constants can be derived. I.e. for every *n-angled* geometrical element there exist one and only one particular constant for every of the above mentioned sequence which are mutually linked.

For the case of Fibonacci sequence, such constants can be generated through the equation:

$$C = \frac{F_n \pm F_{n-2f}}{F_{n-f}} \quad (1)$$

Where $f > 0$ is the object's *form* which represents the value of n-angled element (*1-angle, 2-angle, …, n-angle*) and $n > 2f$. If the form f is odd the sign in the above mentioned formula is negative otherwise the sign is positive.

For example, let us consider three forms (*3-angle, 4-angle and 5-angle*), then for this we will have the following constants based on equation (1).

For *3-angle* we have $f = 3$ and because f is odd then the constant is:

$$C = \frac{F_n - F_{n-6}}{F_{n-3}}$$

For $n > 2f = 6$, if we consider $n = 7$ we will have:

$$C = \frac{F_7 - F_{7-6}}{F_{7-3}} = \frac{F_7 - F_1}{F_4} = \frac{8-0}{2} = 4$$

The same values applied for $f = 4$ and $f = 5$ for 4-angle and 5-angle can be derived as follows:

$$C = \frac{F_n - F_{n-8}}{F_{n-4}} = 7 \text{ and } C = \frac{F_n - F_{n-10}}{F_{n-5}} = 11$$

The graphical representation of Fibonacci sequence through a 3-angle is depicted as in fig 2.

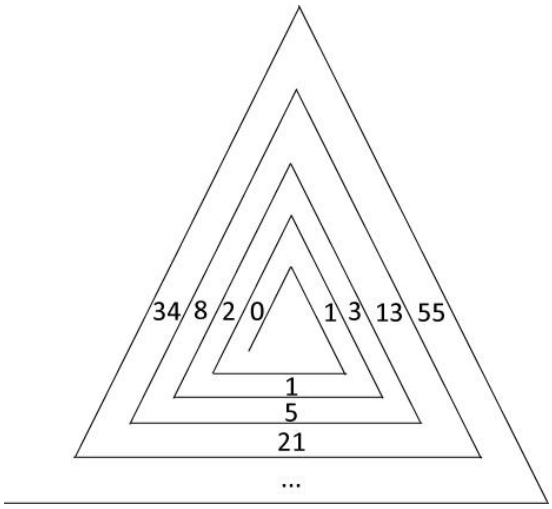

Fig. 2 Geometrical representation of a 3-angle with constant 4

For Lucas sequence, it can be shown identically that same such constants can be generated through equation:

$$C = \frac{L_n \pm L_{n-2f}}{L_{n-f}} \quad (2)$$

Where $f > 0$ is the object's *form* which represents the value of n-angled element and $n > 2f$. If the form f is odd the sign in the above mentioned formula is negative otherwise the sign is positive.

For the same example, considered for three forms (*3-angle, 4-angle and 5-angle*), then for this we will have the following constants based on equation (2).

For *3-angle* we have $f = 3$ and because f is odd then:

$$C = \frac{L_n - L_{n-6}}{L_{n-3}}$$

For $n > 2f = 6$, if we consider $n = 7$ we will have:

$$C = \frac{L_7 - L_{7-6}}{L_{7-3}} = \frac{L_7 - L_1}{L_4} = \frac{18-2}{4} = 4$$

The same values applied for $f = 4$ and $f = 5$ for 4-angle and 5-angle can be derived as follows:

$$C = \frac{L_n - L_{n-8}}{L_{n-4}} = 7 \text{ and } C = \frac{L_n - L_{n-10}}{L_{n-5}} = 11$$

The graphical representation of Lucas sequence through a 4-angle is depicted as in fig 3.

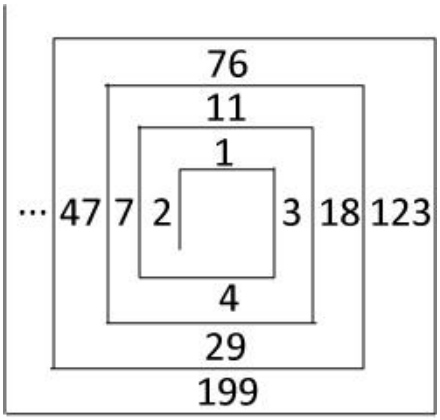

Fig. 3 Geometrical representation of a 4-angle with constant 7

Seen from equations (1) and (2), it can be seen that constant is the same for both sequences. If the above mentioned equations are treated further by equalizing both sides we will get:

$$\frac{F_n \pm F_{n-2f}}{F_{n-f}} = \frac{L_n \pm L_{n-2f}}{L_{n-f}} \quad (3)$$

From this equation it can be concluded for constant C that the expression of the same can be through elements of both Fibonacci and Lucas sequences. Another property of constant

C is that the numbers generated themselves are numbers from Lucas sequence. Considering that constant C represent a value from Lucas sequence, then every element from Lucas sequence it can be expressed through Fibonacci numbers with the equation:

$$L_{n-f} = \frac{F_n \pm F_{n-2f}}{F_{n-f}} \quad (4)$$

From equation (3) it can be seen clearly the link between Fibonacci and Lucas sequence. The benefit of such relation between Fibonacci and Lucas sequences can be used for encryption/decryption purposes.

IV. A CASE STUDY: SYMMETRICAL ENCRYPTION WITH LUCAS AND FIBONACCI SEQUENCES

A symmetrical key encryption represents a cryptosystem where the rules of communication are determined previously, in our case by mathematical operator called Pentor and Ultra Pentor [3] will be utilized.

Let person A choose (n, f) tuple and from equation (4) it can be found F_n, F_{n-2f}, F_{n-f} and L_{n-f}. By knowing that person A and B already know the value of f, person A sends a public encryption key to person B.

The public key is created as a product represented as:

$$K = F_n \cdot F_{n-2f} \cdot F_{n-f} \cdot L_{n-f} \cdot f \quad (5)$$

Person B after receiving the key K and by already knowing the value of f he can find the value of Pentor and Ultra Pentor. Based on the generated value for Ultra Pentor, person B performs a sequence division of public key K, where the size of divided sequences is determined by the value of Ultra Pentor itself. This operation is known as sequence attack with ultra pentor or *Ultra Pentoric "attack"*. After the division, the sum of divided sequences is performed resulting in another value. One aspect during division, as elaborated in [3] is that if the first digit on the left during division is 0, such a value is substituted with f. The division continues until the size of the divided sequence is smaller than the initial division value of the Ultra Pentor. Newly created sequence, the values of which can be shifted to the left or right by one place resulting in a non-repeated combination which finally is brought in a matrix of the size no greater than the value of the Ultra Pentor itself. We name this matrix as $M[UP(f), UP(f)]$.

The sole constraint that needs to be checked in this approach is that the length of the message should not exceed the value of Ultra Pentor. If this would be the case than the message is "chopped" into equivalent compatible sizes in order to perform the addition between the vector and the matrix. During the message sequence "chopping" process, if the last part is smaller in size than Ultra Pentor's value, such size is compensated by adding random values to the sequence, which latter during decryption can be removed.

According to the above mentioned the ciphertext created will be represented as:

$$C = M[UP(f), UP(f)] \cdot m_1[UP(f)] + M[UP(f), UP(f)] \cdot m_2[UP(f)] + \cdots + M[UP(f), UP(f)] \cdot m_i[UP(f)] \quad (6)$$

Now, person B sends the ciphertext to person A. This ciphertext is decrypted by person A by finding the inverse matrix of $M^{-1}[UP(f), UP(f)]$. The decrypted message respectively can be represented as:

$$m = M^{-1}[UP(f), UP(f)] \cdot C_1[UP(f)] + M^{-1}[UP(f), UP(f)] \cdot C_2[UP(f)] + \cdots + M^{-1}[UP(f), UP(f)] \cdot C_i[UP(f)] \quad (7)$$

All of the above elaborated can be illustrated with an example.

Let person A take certain form $f = 13$, $n = 28$ and initially agreed for Ultra Pentor, for example 6. By substituting values of n and f in equation (4) we will have:

$$L_{15} = \frac{F_{28} - F_2}{F_{15}}$$

From the Fibonacci sequences, the above mentioned values will be: $F_{28} = 196418, F_{15} = 377$ and $F_2 = 1$. If substituted above, the value of L_{15} is 521.

Having all these values, the generated key, according to equation (5) will be:

$$K = F_{28} \cdot F_2 \cdot F_{15} \cdot L_{15} \cdot f = 501537845978$$

Person A sends to person B only the key K.

On the other side of the line, person B, by knowing the value of Ultra Pentor, performs Ultra Pentoric "attack" [3] as shown below:

$$K = 501537 \mid 845978$$

$$\begin{array}{r} 845978 \\ +\ 501537 \\ \hline 1347515 \end{array}$$

Because the value has more digits than the value of Ultra Pentor, we continue with "Ultra Pentoric" attack as follows:

$$1 \mid 347515$$

$$\begin{array}{r} 347515 \\ +\quad 1 \\ \hline 347516 \end{array}$$

From the remainder of the Ultra pentoric attack, a matrix is generated by shifting its digits resulting in non-repeated combination represented as:

$$M[6,6] = \begin{pmatrix} 3 & 4 & 7 & 5 & 1 & 6 \\ 4 & 7 & 5 & 1 & 6 & 3 \\ 7 & 5 & 1 & 6 & 3 & 4 \\ 5 & 1 & 6 & 3 & 4 & 7 \\ 1 & 6 & 3 & 4 & 7 & 5 \\ 6 & 3 & 4 & 7 & 5 & 1 \end{pmatrix}$$

Person B takes a message $m = artanbujar$, the numerical values of which are generated by the position of the letter in English alphabet starting by $a = 1, b = 2, c = 3, \ldots$ The value of such a message represented numerically is:

$$m[10] = [1, 18, 20, 1, 14, 2, 21, 10, 1, 18]$$

Considering that the message is greater than matrix rank, the message should be divided into two sub messages with sizes not larger than the rank itself. The sub messages are:

$$m_1[6] = [1, 18, 20, 1, 14, 2]$$

and

$$m_2[6] = [21, 10, 1, 18, 1, 1]$$

Consequently, $m = m_1 \,||\, m_2$, where "||" sign represents the concatenation operator between two sub-messages.

From equation (6) for the ciphertext we will have:

$$C[12] = M[6,6] \cdot m_1[6] \,||\, M[6,6] \cdot m_2[6,6]$$

$$C[12] = [246, 321, 173, 216, 281, 219, 200, 177, 306, 175, 156, 286]$$

Person B sends the above mentioned ciphertext to person A. The accepted ciphertext from person A can be decrypted by knowing the key M from which the person A derives the inverse matrix with the equation:

$$M^{-1} = \frac{1}{\det(M)} adj(M)$$

After finding the inverse matrix, the cipher text can be decrypted based on equation (7):

$$m = M^{-1}[6,6] \cdot C_1[6] + M^{-1}[6,6] \cdot C_2[6]$$

The decrypted message will be:

$$m[12] = [1, 18, 20, 1, 14, 2, 21, 10, 1, 18, 1, 1]$$

If converted to text the message will be:

$$m = artanbujaraa$$

The last two letters, resulted in added values due to sequence division can now be removed resulting in original message $m = artanbujar$ given earlier.

V. Conclusion

In this paper we have presented the link between Fibonacci and Lucas sequence and the possibility of using the same for encryption/decryption purposes. The conclusive part of the paper is the possibility on utilizing the generated forms of both sequences as public keys for encryption and decryption purposes. The efficiency of the approach is seen in use case where both sequences are used for performing symmetrical key encryption. The strength of the symmetrical cryptosystem lies in the previously agreed Ultra Pentor value, necessary for Ultra Pentoric "attack" which is hard to find due to the nature of Ultra Pentor where different values can have the same Ultra Pentor and the process is not reversible.

The future work would also involve seeking the possibility of developing asymmetrical key encryption based on Lucas and Fibonacci sequences as well as Pentor and Ultra Pentor values.

References

[1] A. Luma, "Data encryption and Decryption using ANZF Algorithm" in *Proc. 31st Int. Conv. Information and Communication Technology, Electronics and Microelectronics*, Opatija, Croatia, 2008, pp. 90-94.

[2] A. Luma, N.Zeqiri, "Data encryption and Decryption using ANZL Algorithm" in *Proc. 31st Int. Conv. Information and Communication Technology, Electronics and Microelectronics*, Opatija, Croatia, 2008, pp. 219-223.

[3] A. Luma, B. Raufi. *New Data Encryption Algorithm and its Implementation for Online User Authentication*. In Proc. 2009 International Conference on Security and Management. CSREA Press, Las Vegas, Nevada. pp. 81-85.

[4] C. Brown, *The Fibonacci Analysis (Bloomberg Professional).* Bloomberg Press, 2008.

[5] S.Vajda, *Fibonacci and Lucas Numbers, and the Golden Section: Theory and Applications.* Dover Publications, 2007.