Application of Some Recurrence Relations to Cryptography using Finite State Machine

Prasanta Kumar Ray, Gopal Krishna Dila, and Bijan Kumar Patel

***Abstract*---**It is well known that, a recursive relation for the sequence $a_0, a_1, a_2, \ldots$ is an equation that relates a_n to certain of its preceding terms $a_0, a_1, a_2, \ldots, a_{n-1}$. Initial conditions for the sequence $a_0, a_1, a_2, \ldots$ are explicitly given values for a finite number of the terms of the sequence. In this study, we use the recurrence relations for both balancing and Lucas-balancing numbers and examine their application to cryptography using finite state machine.

***Keywords*-** Balancing numbers, Recurrence relation, Balancing matrix, Cryptography.

I. Introduction

CRYPTOGRAPHY is the study of methods of keeping communication secret and secure between a sender and a recipient in the presence of malevolent third parties. Security can only be as strong as the weakest link. In this world of Cryptography, it is now well established, that the weakest link lies in the implementation of cryptographic algorithms. The technological advancement in today's world have made the cryptographic algorithms more prone to attacks. Automata theory is the study of abstract machines and automata as well as the computational problems that can be solved using them. It is a theory in theoretical computer science under discrete mathematics. Thus, Automata Theory is the study of self-operating virtual machines to help in logical understanding of input and output process without or with intermediate stage or stages of computation or any function or process. So Multi-level ciphering which can avoid all sorts of attack is possible using finite state machine.

In this paper, the objective is to develop new cryptographic schemes using finite state machines, recurrence relations and recurrence matrices. The proposed method solves many problems that we are facing now a days to introduce a more secure cryptographic algorithm. The efficiency of the proposed method is analyzed, and the analysis shows an improved cryptographic protection in digital signals.

Prasanta Kumar Ray is with the International Institute of Information Technology, Bhubaneswar (phone: +91 6746636644; fax: +91 6746636600; e-mail: prasanta@iiit-bh.ac.in).

Gopal Krishna Dila was with National Institute of Technology, Rourkela-769008 ODISHA (e-mail: 410ma5087@nitrkl.ac.in).

Bijan Kumar Patel is with the International Institute of Information Technology, Bhubaneswar (e-mail:bijan.bijanpatel.patel@gmail.com).

II. Development Of Cipher Using Recurrence Matrix

In [18], Stakhov et.al. has introduced golden cryptography based on the golden ratio. In this study, we use the recurrence relations for both balancing and Lucas-balancing numbers and examine their application to cryptography.

Balancing numbers n and the balancers r are solutions of the Diophantine equation $1 + 2 + \ldots + (n-1) = (n+1) + (n+2) + \ldots + (n+r)$ [1]. It is well known that, the recurrence relation for balancing numbers is:

$$B_{n+1} = 6B_n - B_{n-1}, n \geq 2 \quad (1)$$

Where B_n is the n^{th} balancing number with $B_1 = 1, B_2 = 6$. Companion to balancing numbers is the sequence of Lucas-balancing numbers C_n defined by $C_n = 8B_n^2 + 1$ and their recurrence relation is same as that of balancing numbers, that is

$$C_{n+1} = 6C_n - C_{n-1}, n \geq 2 \quad (2)$$

Where C_n is the n^{th} Lucas-balancing number with $C_1 = 3$, $C_2 = 17$ [7].

Liptai [3], showed that the only balancing number in the sequence of Fibonacci numbers is 1. In [10] and [11], Ray has found two important product formulas for both balancing and Lucas-balancing numbers. Panda et.al. [8] linked balancing numbers with Pell and associated Pell numbers and shown that balancing numbers are indeed the product of Pell and associated Pell numbers. Many interesting properties for balancing numbers and their related sequences are available in the literature. One can go through ([1] − [17]).

2.1. Balancing and Lucas-balancing matrices

In [12], Ray introduced balancing Q-matrix of order 2 whose entries are the first three balancing numbers 0, 1 and 6 as follows:

$$Q_B = \begin{bmatrix} 6 & -1 \\ 1 & 0 \end{bmatrix}. \quad (3)$$

It is well known that, n^{th} power of the balancing Q-matrix is

$$Q_B^n = \begin{bmatrix} B_{n+1} & -B_n \\ B_n & -B_{n-1} \end{bmatrix}, \quad (4)$$

where $n = 0, \pm 1, \pm 2, \pm 3, \ldots$, and B_n is the n^{th} balancing number. Without loss of generality, we present the balancing matrix Q_B in a different way by interchanging the main diagonal elements as follows:

$$Q_{B_1} = \begin{bmatrix} 0 & -1 \\ 1 & 6 \end{bmatrix}. \quad (5)$$

The general form of this matrix will be

$$Q_{B_1}^n = \begin{bmatrix} -B_{n+1} & -B_n \\ B_n & B_{n+1} \end{bmatrix}, \quad (6)$$

We now extend the balancing matrix (5) to a 3x3 matrix of the form:

$$Q_{B_2} = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 6 & 0 \\ 0 & 0 & 1 \end{bmatrix}. \quad (7)$$

This matrix is so formed that its determinant is invariant without loss of generality to the Cassini Formula

$$B_n^2 - B_{n+1}\, B_{n-1} = 1$$

for balancing numbers. Similarly, extending it to 4^{th} order, we obtain:

$$Q_{B_3} = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 6 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \quad (8)$$

The same logic can be used for extending to any order square matrix. Notice that, the usual product of

$$Q_{B_2} = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 6 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ and } Q_{B_2}^{-1} = \begin{bmatrix} 6 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

gives the identity matrix $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Therefore generalization of this result yields:

$$Q_{B_2}^n Q_{B_2}^{-n} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad (11)$$

for all integers n.

The Lucas-balancing matrix whose entries are the first three Lucas-balancing numbers $0, 1$ and 3 can be similarly defined as follows:

$$Q_{C_1} = \begin{bmatrix} 0 & -1 \\ 1 & 3 \end{bmatrix}. \quad (12)$$

The general form of balancing matrix is:

$$Q_{C_1}^n = \begin{bmatrix} -C_{n-1} & -C_n \\ C_n & C_{n+1} \end{bmatrix}, \quad (13)$$

where $n = 0, \pm 1, \pm 2, \pm 3, \ldots$, and C_n is the n^{th} balancing number. The extensions of the Lucas-balancing matrix Q_C can be similarly obtained as:

$$Q_{C_2} = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 1 \end{bmatrix}, Q_{C_3} = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 3 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \text{ etc.}$$

The same logic can be used for extending to any order square matrix. And also,

$$Q_{C_2}^n Q_{C_2}^{-n} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad (16)$$

for all integers *n*.

2.2. Application of balancing and Lucas-balancing numbers to cryptography

In this section, we examine the application of recurrence relations to cryptography with a new dimensionality in the matrix. Let the initial message be a digital signal which is a sequence of separate real numbers $a_1, a_2, a_3, \ldots$ We choose the first nine readings and form a 3x3 matrixof the form

$$\begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{bmatrix},$$

which is to be considered as a plain text matrix. There can be 9! permutations to form the matrix A. Let P_i be the choice of i^{th} permutation. We choose the direct matrix as enciphering matrix, the inverse matrix as deciphering matrix and the variable *x* as cryptographic key. In general, the key *K* consists of the permutation P_i, the variable *x*, the Moore machine *M* and the type of recursion used is *R* that is, $K = \{M, P_i, x, R\}$.

III. Proposed Algorithm

3.1. Encryption

Step 1: Let the plain text A be a square matrix of order *n*; $n > 0$. Let P_i be the choice of i^{th} permutation.

Step 2: Define recurrence relation *R* and recurrence matrix Q_{R_n}. Choose the cryptographic key *x*. Define the Moore/Mealy machine.

Step 3: Define the cipher text.

$$Cipher\ text\ at\ q_{i+1}th\ state = (Cipher\ text\ q_i th\ state) * (Q_{R_n})^{(output\ at\ q_{i+1}th\ state)}$$

Step 4: Compute the cipher text and send it to the receiver.

3.2. Decryption

Step 1: On receiving the secret key, cipher text, the finite state machine and recurrence matrix decrypt the message using multiplicative inverse of the recurrence matrix and the secret key, to get the original information. For a finite state machine with *n* states, we need *n* multiplicative inverse matrix.

IV. Efficiency of the Proposed Algorithm

4.1. Mathematical work

Algorithm proposed is a simple application of the Hill cipher using recurrence matrix. It is very difficult to break the cipher text without proper key, finite state machine and choice of recurrence relation and permutation used.

4.2. Strength of the key

It is very difficult to guess the length of the secret key even if the recurrence relation and finite state machine are known.

4.3. Number of Rounds

The number of rounds for which the process continues also depend on the secret key and the finite state machine used. Even if we know the finite state machine it is very difficult to guess the number of rounds without an appropriate key.

4.4. Encryption and Decryption Time calculation

Let the sum of the outputs of the finite state machine for k bit secret key is s. Let t_m be the time required for each multiplication and t_a be the time required for each addition during the encryption process. Then the total time required for k bit secret key is: $s(n^3 t_m + n(n-1)t_a)$.

4.5. Security analysis

Extraction of the original information is difficult due to the matrix multiplication, chosen finite state machine, choice of permutation, recurrence relation and secret key. Brute force attack on key is also difficult due to the increase in secret key size.

V. Application

5.1. Example:

Let the plain-text to be transmitted be: A = $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$.

Choosing $n = 2$ and the types of recursion as balancing numbers,

$$Q_{B_2}^2 = \begin{bmatrix} -1 & -6 & 0 \\ 6 & 35 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Here we calculate the cipher text with respect to mod 47.

The secret key is 39 and the finite state machine is defined as Moore machine that calculates the residue mod 4 as given in the following table.

TABLE 1
EXAMPLE

SL. No.	Input	Previous State	Present State	Output	Cipher Text
1	1	q_0	q_1	1	$\begin{pmatrix} 11 & 17 & 3 \\ 26 & 10 & 6 \\ 41 & 3 & 9 \end{pmatrix}$
2	0	q_1	q_2	2	$\begin{pmatrix} 28 & 15 & 3 \\ 2 & 6 & 6 \\ 23 & 44 & 9 \end{pmatrix}$
3	0	q_2	q_0	0	$\begin{pmatrix} 28 & 15 & 3 \\ 2 & 6 & 6 \\ 23 & 44 & 9 \end{pmatrix}$
4	1	q_0	q_1	1	$\begin{pmatrix} 15 & 28 & 3 \\ 34 & 10 & 6 \\ 6 & 39 & 9 \end{pmatrix}$
5	1	q_1	q_3	3	$\begin{pmatrix} 2 & 1 & 3 \\ 16 & 30 & 6 \\ 30 & 12 & 9 \end{pmatrix}$
6	1	q_3	q_3	3	$\begin{pmatrix} 40 & 23 & 3 \\ 30 & 16 & 6 \\ 20 & 9 & 9 \end{pmatrix}$

Secret key = 39(100111).

So, from the table 1 we get the cipher text as $\begin{bmatrix} 40 & 23 & 3 \\ 30 & 16 & 6 \\ 20 & 9 & 9 \end{bmatrix}$

For decryption process we have to multiply the cipher text with the inverse of the recurrence matrix used. So, after getting the secret key, finite state machine and recurrence matrix we can decrypt the cipher text. For a finite state machine with n states, we need n multiplicative inverse matrix. So,

$$Decryption\ at\ q_i th\ state = (Cipher\ text) * (Q_{R_n})^{(output\ at\ q_i th\ state)}$$

For 1st round of decryption we multiply $\begin{bmatrix} 40 & 23 & 3 \\ 30 & 16 & 6 \\ 20 & 9 & 9 \end{bmatrix}$ with the inverse of $\begin{bmatrix} -1189 & -6930 & 0 \\ 6930 & 40391 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ to get $\begin{bmatrix} 2 & 1 & 3 \\ 16 & 30 & 6 \\ 30 & 12 & 9 \end{bmatrix}$, which is the cipher matrix at 5th round during encryption process. On continuing this process of multiplying the resulting cipher matrix with the inverse of recurrence matrix we can get the plain text after n rounds depending on the finite state machine. So, then on multiplying $\begin{bmatrix} 2 & 1 & 3 \\ 16 & 30 & 6 \\ 30 & 12 & 9 \end{bmatrix}$ with the inverse of $\begin{bmatrix} -1189 & -6930 & 0 \\ 6930 & 40391 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ to get $\begin{bmatrix} 15 & 28 & 3 \\ 34 & 10 & 6 \\ 6 & 39 & 9 \end{bmatrix}$.

Similarly by using the Finite state machine and the recurrence matrix, we multiply the resultant matrix with the inverse of $\begin{bmatrix} -1 & -6 & 0 \\ 6 & 35 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ to get $\begin{bmatrix} 28 & 15 & 3 \\ 2 & 6 & 6 \\ 23 & 44 & 9 \end{bmatrix}$.

On multiplying this matrix with the inverse of $\begin{bmatrix} -35 & -204 & 0 \\ 204 & 1189 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, we get $\begin{bmatrix} 11 & 17 & 3 \\ 26 & 10 & 6 \\ 41 & 3 & 9 \end{bmatrix}$.

Finally multiplying this resultant matrix with the inverse of $\begin{bmatrix} -1 & -6 & 0 \\ 6 & 35 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ to get $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$, which the plain text matrix. So, by knowing the finite state machine, the recurrence matrix and the secret key we can decipher the cipher text otherwise it is very difficult to decrypt the message.

VI. Conclusion

In the present study, two types of recurrences namely balancing and Lucas-balancing are discussed but in general can be extended to any recurrence relation. One can use any algorithm which are used in asymmetric cryptosystem to transmit the key. As compared to Fibonacci numbers, balancing and Lucas-balancing are large and therefore more secured. Also, the level of security is high since it involves four parameters such as permutation, the finite state machine, the secret key and type of recurrence used. The cryptographic protection of digital signals can be improved by multiple encryption and decryption algorithms. Also, with the increase

of the size of the matrix and number of rounds, more information can be sent securely at a time.

REFERENCES

[1] A. Behera and G.K. Panda, On the square roots of triangular numbers, The Fibonacci Quarterly, 37(2), 1999, 98-105.

[2] R. Keskin and O. Karaatly, Some new properties of balancing numbers and square triangular numbers, Journal of Integer Sequences,15(1), 2012.

[3] K. Liptai, Fibonacci balancing numbers, The Fibonacci Quarterly, 42(4), 2004, 330-340.

[4] K. Liptai, Lucas balancing numbers, Acta Math.Univ. Ostrav, 14(1), 2006, 43-47.

[5] K. Liptai, F. Luca, A. Pinter and L. Szalay, Generalized balancing numbers, Indagationes Math. N. S., 20, 2009, 87-100.

[6] P. Olajos, Properties of balancing, cobalancing and generalized balancing numbers, Annales Mathematicae et Informaticae, 37, 2010, 125-138.

[7] G.K. Panda, Some fascinating properties of balancing numbers, Proc. Eleventh Internat. Conference on Fibonacci Numbers and Their Applications, Cong. Numerantium, 194, 2009, 185-189.

[8] G.K. Panda and P.K. Ray, Some links of balancing and cobalancing numbers with Pell and associated Pell numbers, Bulletin of the Institute of Mathematics, Academia Sinica (New Series), 6(1), 2011, 41-72.

[9] G.K. Panda and P.K. Ray, Cobalancing numbers and cobalancers, International Journal of Mathematics and Mathematical Sciences, 2005(8), 2005, 1189-1200.

[10] P.K. Ray, Application of Chybeshev polynomials in factorization of balancing and Lucas-balancing numbers, Bol. Soc. Paran. Mat. 30 (2), 2012, 49-56.

[11] P.K. Ray, Factorization of negatively subscripted balancing and Lucas-balancing numbers, Bol.Soc.Paran.Mat., 31 (2), 2013, 161-173.

[12] P. K. Ray, Certain matrices associated with balancing and Lucas-balancing numbers, Matematika, 28 (1), 2012, 15-22.

[13] P.K. Ray, Curious congruences for balancing numbers, Int.J.Contemp.Sciences, 7 (18), 2012, 881-889.

[14] P.K Ray, New identities for the common factors of balancing and Lucas- balancing numbers, International Journal of Pure and Applied Mathematics, 85(3), 2013, 487-494.

[15] P.K. Ray, Some congruences for balancing and Lucas-balancing numbers and their applications, Integers, 14, 2014, A8.

[16] P.K. Ray, Balancing sequences of matrices with application to algebra of balancing numbers, Notes on Number Theory and Discrete Mathematics, 20(1), 2014, 49-58.

[17] P.K. Ray, On the properties of Lucas-balancing numbers by matrix method, Sigmae, Alfenas, 3(1), 2014, 1-6.

[18] A.P. Stakhov, The golden matrices and a new kind of cryptography, Chaos, Soltions and Fractals 32, 2007, 1138-1146.

[19] D.R. Stinson, Cryptography Theory and Practice, 3rd edition, Chapman and Hall/CRC, Taylor and Francis Group, Boca Raton, 2006.