Balancing and Lucas-Balancing Numbers and Their Application to Cryptography

Sujata Swain, Chidananda Pratihary and Prasanta Kumar Ray

Department of Computer Science, DAV Unit-8, Bhubaneswar, India
Department of Mathematics, National Institute of Technology, Rourkela, India
Department of Mathematics, VSS University of Technology, Burla, India
sujataswn@gmail.com,
cnpratihary@gmail.com
rayprasanta2008@gmail.com

ABSTRACT

It is well known that, a recursive relation for the sequence $a_{0,}\ a_{1,}\ a_{2,}\ \cdots$ is an equation that relates a_n to certain of its preceding terms $a_{0,}\ a_{1,}\ a_{2,}\ \cdots a_{n-1}$. Initial conditions for the sequence $a_{0,}\ a_{1,}\ a_{2,}\ \cdots$ are explicitly given values for a finite number of the terms of the sequence. The recurrence relation is useful in certain counting problems like Fibonacci numbers, Lucas numbers, balancing numbers, Lucas-balancing numbers etc. In this study, we use the recurrence relations for both balancing and Lucas-balancing numbers and examine their application to cryptography.

Keywords*:* Recurrence relations, Balancing numbers, Lucas balancing numbers, Cryptography

1. 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. Multi-level ciphering can avoid all sorts of attack.

In mathematics, a Cryptosystem is a five tuple (P, C, K, E, D) where, P is a finite set of possible plaintext C is a finite set of possible cipher texts, K is a finite set of possible keys [1]. For each$k \in K$, there is an encryption mapping $e_K: P \to C$ and a corresponding decryption mapping $d_K: C \to P$ defined by $d_k(e_k(x)) = x$, where $e_k \in E$ and $d_k \in D$ where $e_k \in E$ and $d_k \in D$and for every plaintext elements $x \in P$.

In this paper, the objective is to develop new cryptographic schemes using recurrence relations and recurrence matrices. Many authors have studied the application of Fibonacci numbers and their related sequences in cryptography. In [2], Stakhov et.al. introduced a different kind of cryptography based on the golden ratio which is popularly known as golden cryptography. Luma et. al. have found a very interesting relationship between Fibonacci and Lucas numbers and applied it to symmetric cryptosystem [3]. The purpose of this paper is to study the possible application of balancing numbers and their related sequences in cryptography and serve as an alternating to the Fibonacci cryptography.

2. DEVELOPMENT OF CIPHER USING RECURRENCE MATRIX

It is well known that, a recursive relation for the sequence $a_{0,}\ a_{1,}\ a_{2,}\ \cdots$ is an equation that relates a_n to certain of its preceding terms $a_{0,}\ a_{1,}\ a_{2,}\ \cdots a_{n-1}$. Initial conditions for the sequence $a_{0,}\ a_{1,}\ a_{2,}\ \cdots$ are explicitly given values for a finite number of the terms of the sequence. The recurrence relation is useful in certain counting problems like Fibonacci numbers, Lucas numbers, balancing numbers, Lucas-balancing numbers etc. 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 $1+2+\cdots+(n-1)=(n+1)+(n+2)+\cdots+(n+r)$ [4]. It is well known that, the recurrence relation for balancing numbers is

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

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

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

with $C_1 = 3,\ C_2 = 17$ [5]. Liptai [6], showed that the only balancing number in the sequence of Fibonacci numbers is 1. In [7] and [8], Ray obtained nice product formulas for both balancing and Lucas-balancing numbers. Panda and Ray [9] 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 [4–20].

2.1. Balancing and Lucas-balancing matrices

In [10], Ray has introduced balancing Q-matrix of order 2 whose entries are nothing but the first three balancing numbers $0, 1$ and 6, that is

$$Q_B=\begin{pmatrix}6 & -1\\ 1 & 0\end{pmatrix}. \tag{3}$$

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

He also proved that for all integers n, the power of this matrix is

$$Q_B^n = \begin{pmatrix} B_{n+1} & -B_n \\ B_n & -B_{n-1} \end{pmatrix} \tag{4}$$

where B_n is the n^{th} balancing number [10]. Without loss of generality, we present the balancing matrix Q_B in a different way by interchanging the main diagonal elements as follows:

$$Q_{B_1} = \begin{pmatrix} 0 & -1 \\ 1 & 6 \end{pmatrix} \tag{5}$$

The general form of this balancing matrix is given by

$$Q_{B_1}^n = \begin{pmatrix} -B_{n-1} & -B_n \\ B_n & B_{n+1} \end{pmatrix}. \tag{6}$$

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

$$Q_{B_2} = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 6 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

which 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

$$Q_{B_3} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 6 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The same logic can be used to extend any order square matrix. Notice that, the usual product of $Q_{B_2} = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 6 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and its inverse $Q_{B_2}^{-1} = \begin{pmatrix} 6 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ gives the identity matrix $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Therefore generalization of this result yields

$$Q_{B_2}^n Q_{B_2}^{-n} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

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:

$$Q_C = \begin{pmatrix} 0 & -1 \\ 1 & 3 \end{pmatrix}. \tag{7}$$

The general form of this Lucas-balancing matrix is given by

$$Q_C^n = \begin{pmatrix} -C_{n-1} & -C_n \\ C_n & C_{n+1} \end{pmatrix} \tag{8}$$

where C_n is the n^{th} Lucas-balancing number. The extension of Lucas-balancing matrix Q_C can be similarly obtaind as

$$Q_{C_2} = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ Q_{C_3} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 3 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \text{ and so on.}$$

We also observe that, $Q_{C_2}^n Q_{C_2}^{-n} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, for all integers n .

2.2. Application of balancing and Lucas-balancing matrices 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 $a_1, a_2, a_3, a_4, a_5, \cdots$. We choose the first nine readings and form a 3×3 matrix of the form $A = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{pmatrix}$ 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 and the type of recursion used is R that is, $K = \{P_i, x, R\}$. Here $C(x)$ denote the cipher text matrix.

3. 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.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

Step 2: Define recurrence relation R and recurrence matrix Q_{R_n}. Choose the cryptographic key x.

Step 3: Define the cipher text. [Cipher text is equal to the plain text matrix$*$ (the recurrence matrix)^x]

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

The above steps can be written in a compact form as follows:

```
$If\ R = balancing\ numbers, then$
    $(C) \leftarrow (A)(Q_{B_2}^{x})$
  $End\ if$
$If\ R = Lucas - balancing\ numbers,\ then$
    $(C) \leftarrow (A)(Q_{C_2}^{x})$
  $End\ if$
```

3.1. Decryption

On receiving the secret key, cipher text and recurrence matrix decrypt the message using multiplicative inverse of the recurrence matrix and the secret key, to get the original information. The following is the algorithm for decryption

```
$If\ R = balancing\ numbers, then$
    $(A) \leftarrow (C)(Q_{B_2}^{-x})$
  $End\ if$
$If\ R = Lucas - balancing\ numbers, then$
    $(A) \leftarrow (C)(Q_{C_2}^{-x})$
  $End\ if$
```

4. EFFICACY OF THE PROPOSED ALGORITHM

4.1. Mathematical work

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

4.2. Strength of the key

It is very difficult to guess the secret key even if the recurrence relation is known.

4.3. Encryption and Decryption Time calculation

The encryption consists in calculation of the nine elements of the $C(x)$ which include three multiplications and two additions. If Δ_{t_m} is the time required for each multiplication and Δ_{t_a} is the time required for addition, then total encryption time is given as

$$T_e = 27\Delta_{t_m} + 18\Delta_{t_a}.$$

Similarly, the total decryption time is given by

$$T_d = 27\Delta_{t_m} + 18\Delta_{t_a}.$$

Hence, the time taken for encryption and decryption is less. So this method as an enhanced cryptography can prove to be a fast method for digital signals.

4.4. Security analysis

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

5. AN EXAMPLE TO EXPLAIN THE WHOLE APPLICATION

Example 5.1 Let the plaintext to be transmitted be $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$. Choosing $x = 1$ and the types of recursion as balancing numbers $Q_{B_2}^1 = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 6 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. The initial step to form the ciphertext matrix $C(x)$ as follows:

$$C(x) = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} 0 & -1 & 0 \\ 1 & 6 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 11 & 3 \\ 5 & 26 & 6 \\ 8 & 41 & 9 \end{pmatrix}.$$

The second step is to form enciphering matrix A from $C(x)$ with the inverse matrix $Q_{B_2}^{-1}$ as follows:

$$A=\begin{pmatrix}2&11&3\\5&26&6\\8&41&9\end{pmatrix}\begin{pmatrix}6&1&0\\-1&0&0\\0&0&1\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix}.$$

If the type of recursion used is Lucas-balancing for which $Q_{C_2}^1=\begin{pmatrix}0&-1&0\\1&3&0\\0&0&1\end{pmatrix}$, then the ciphertext matrix $C(x)$ be

$$C(x)=\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix}\begin{pmatrix}0&-1&0\\1&3&0\\0&0&1\end{pmatrix}$$

$$=\begin{pmatrix}2&5&3\\5&11&6\\8&17&9\end{pmatrix},$$

and the enciphering matrix A will be

$$A=\begin{pmatrix}2&5&3\\5&11&6\\8&17&9\end{pmatrix}\begin{pmatrix}3&1&0\\-1&0&0\\0&0&1\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix}.$$

6. 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 three parameters such as permutation, the power of the matrix 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, more information can be sent securely at a time.

ACKNOWLEDGEMENTS

The author wishes to thank the anonymous referees for their detailed comments and suggestions which have improved the presentation of the paper.

REFERENCES

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

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

[3] A. Luma and B. Raufi, Relationship between Fibonacci and Lucas Sequences and their Application in Symmetric Cryptosystems, Latest Trends on Circuits, Systems and Signals, 4th International Conference on Circuits, Systems and Signals, July 22-25, 2010, 146-150

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

[5] 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.

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

[7] 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.

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

[9] 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.

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

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

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

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

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

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

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

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

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

[19] 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.

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