Cryptographic Scheme for Digital Signals using Finite State Machines

B.Krishna Gandhi
Vice Chancellor
J.N.T. University
Anantapur, A.P, India

Dr.A.Chandra Sekhar
Professor
Department of Engineering Mathematics
GITAM University
Visakhapatnam, India

S.Srilakshmi
Lecturer
J.N.T. U.C.E(A)
Anantapur, A.P, India

ABSTRACT:
Cryptography is the science of transmission and reception of secret messages. Recently electronic communication has become an essential part of every aspect of human life. Message encryption has become very essential to avoid the threat against possible attacks by hackers during transmission process of the message. In the present paper, new cryptographic schemes are proposed using finite state machine and recurrence matrix.

General terms
Cryptography
Keywords
Moore Machine, key, recurrence relation, cryptography

1. INTRODUCTION:
The fundamental objective of cryptography is to enable two people to communicate over an insecure channel in such a way that any opponent cannot understand what is being said. Communications security is gaining importance as a result of the use of electronic communications in more and more business activities. Cryptography is the only practical means to provide security services and is becoming a powerful tool in many applications for information security. Encryption is the process of obscuring information to make it unreadable without special knowledge. This is usually done for secrecy and typically for confidential communications.

A cipher is an algorithm for performing encryption and decryption. The original information is known as plain text and the encrypted form as cipher text. The cipher text message contains all the information of the plain text message, but is not in a format readable by a human or computer without the proper mechanism to decrypt it. It should resemble random gibberish to those not intended to read it. Ciphers are usually parameterized by a piece of auxiliary information, called a key. The encrypting procedure is varied depending on the key, which changes the detailed operation of the algorithm. Without the apt key the decryption is highly impossible[7].

Automata theory is a key to software for verifying systems of all types that have a finite number of distinct states, such as communication protocols or protocol for secure exchange of information. In Moore Machine every state of finite state machine has fixed output. Mathematically Moore machine is a six- tuple machine and is defined as $M= (Q, \sum, \Delta, \delta, \lambda, q_0)$

Q : A nonempty finite set of state in Moore machine

$\sum$: A nonempty finite set of inputs.

Δ : A nonempty finite set of outputs.

δ : It is a transition function which takes two arguments one is input state and another is input symbol. The out put of this function is a single state.

λ : Is a mapping function which maps $Q\times\sum$ to Δ, giving the output associated with each transition.

q_0 : is the initial state of Q.

Moore machine can also be represented by transition table, as well as transition diagram[6][10].

A recurrence relation relates the nth element of a sequence to its predecessors. Recurrence relations are useful in certain counting problems like Fibonacci number. A recursive relation for the sequence $a_0, a_1, a_2, ……..a_{n-1}$. Initial conditions for the sequence $a_0, a_1, a_2,……..$ are explicitly given values for a finite number of the terms of the sequence. Example The Fibonacci numbers F_n are the terms of the sequence 0,1,1,2,3,5,…… wherein each term is the sum of the two preceding terms, and we get things started with 0 and 1 as F_0 and F_1. A k-th order linear recurrence relation for the sequence $a_0, a_1, a_2,……..$ has the form $a_n = c_1a_{n-1}+ c_2a_{n-2}+…….+c_ka_{n-k}+f_n$ for $n>k$ where $c_1, c_2,…….c_k$ are constants and f_n is given some sequence. If $f_n=0$, then the linear recurrence relation is called homogeneous.

1.1 Recurrence matrix
Recurrence matrix is a matrix whose elements are taken from recurrence relation.

For example

$$Q=\begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$ where n=0,±1, ±2,…..

F_n's the Fibonacci numbers.

1.1.1 Theorem: The recurrence matrix is a secret key if and only if it is nonsingular.

Proof:
Suppose Q is a recurrence matrix which is a secret key and let A be the plain text. Then AQ = C is the cipher text. To decrypt the encrypted message $A= CQ^{-1}$. Therefore Q^{-1} must exit. Therefore Q must be non singular and vice versa.

1.2 Applications to cryptography
Let the initial message be a digital signal which is a sequence of separate real numbers $a_0, a_1, a_2,……..$ Let us choose nine

readings and form a 2x2 matrix P which is considered as plain text matrix $P=\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$.

There can be 4! Permutations to form the matrix, if P_i be the choice of i^{th} permutation. Choosing the direct matrix enciphering matrix and inverse as deciphering matrix. The variable x is chosen as cryptographic key. In general the key K consists of the Moore Machine M, the variable x the permutation P_i and the type of recurrence relation used is R[1][2][3][4].

K = {M, x, P_i, R}

2. ALGORITHM USING RECURRENCE RELATION OF ORDER 2

2.1 Algorithm :

Step 1
Let P be plain text
Step 2
Define Moor machine through public channel.
Step 3
Send key in binary form to the receiver.
Step 4
Let R (n) be the recurrence matrix of the defined recurrence relation for fixed n. define cipher text at q (i+1)th state .
Step 3
And the cipher text to the receiver.
Decryption
Decrypt the message using the inverse operation and key to get the original message.

2.2 Examples

2.2.1Example 1

Let the plain text be $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ and $R(n)=\begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$ of Fibonacci sequence**.**

Let the input key be 10110 and recurrence matrix key $=\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$

And finite state machine is defined as a machine which calculates the residue mod 4 of the given value

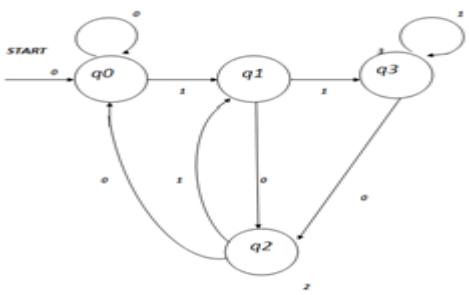

Fig 1 Moore Machine to calculate residue Mod 4

Example 1

Let the cipher text at q(i+1) state is equal to the cipher text at q(i) th state multiplied by $R(n)^{.\text{output of the Moore machine at q(i+1)sate}}$

Then cipher text will be

Table 1 Cipher text for the given secret key

S.No	Input	Previous state	Present state	Out put	Cipher text
1	1	q_0	q_1	1	$\begin{pmatrix} 4 & 1 \\ 10 & 3 \end{pmatrix}$
2	0	q_1	q_2	2	$\begin{pmatrix} 22 & 9 \\ 56 & 23 \end{pmatrix}$
3	1	q_2	q_1	1	$\begin{pmatrix} 53 & 22 \\ 135 & 56 \end{pmatrix}$
4	1	q_1	q_3	3	$\begin{pmatrix} 746 & 309 \\ 1900 & 787 \end{pmatrix}$
5	0	q_3	q_2	0	$\begin{pmatrix} 24348 & 1801 \\ 110746 & 4587 \end{pmatrix}$

For the easy of computations take mod 41 then the cipher text will be $\begin{pmatrix} 2 & 38 \\ 4 & 36 \end{pmatrix}$

2.2.2 Example- 2

Let the plain text be $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ and $R(n)=\begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$ of Fibonacci sequence

Let the input key be 10110
Let the cipher text at q(i+1) state is equal to the cipher text at q(i) th state multiplied by $R(n)^{\text{output of the Moore machine}}$ at q(i+1)th state , where n is the bit number

Then cipher text will be

Table 2 Cipher text for the given secret key

S. No	Input	Previous state	Present state	Out put	Key matrix	Cipher text
1	1	q_0	q_1	1	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 3 & 1 \\ 7 & 3 \end{pmatrix}$
2	0	q_1	q_2	2	$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 18 & 11 \\ 44 & 27 \end{pmatrix}$
3	1	q_2	q_1	1	$\begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 76 & 47 \\ 63 & 33 \end{pmatrix}$
4	1	q_1	q_3	3	$\begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}$	$\begin{pmatrix} 29 & 39 \\ 4 & 9 \end{pmatrix}$
5	0	q_3	q_2	2	$\begin{pmatrix} 8 & 3 \\ 3 & 2 \end{pmatrix}$	$\begin{pmatrix} 9 & 34 \\ 18 & 30 \end{pmatrix}$

Then the cipher text will be $\begin{pmatrix} 9 & 34 \\ 18 & 30 \end{pmatrix}$

3. PERFORMANCE ANALYSIS

3.1 Calculation of encryption and decryption time:

Let t_a be the time required for each multiplication. Let t_b be the time required for each addition. Then the total time required for n key bit matrix multiplication is
n[8(sum of output times) t_a + 4(sum of output)t_b].

Table 3 Encryption time calculations

Example	Mathematical computations	Total encryption time
1	less	8 (sum of output times) t_a+4(sum of output)t_b
2	less	8 (sum of output times) t_a+4(sum of output)t_b

3.2 Security analysis

To extract the original information is highly impossible due the mathematical calculations. Due the secret key , output at each sate and the recurrence relations are the three stage attacks are at a time impossible even the finite state machine is known.
Brute force attack on key is also not possible due to the increase in key size.

Table 4 Security analysis

S.No	Name of the attack	Possibility of the attack	remarks
1	A cipher text attack	Very difficult	Very difficult due to the different cipher texts at different states
2	A known plain text attack	Very difficult	Very difficult due to the different states in chosen finite state machine and recurrence matrix
3	A chosen plain text attack	Very difficult	Very difficult due to the matrix multiplication propagation errors.
4	An adaptive chosen plain text attack	Very difficult	Very difficult due to the chosen finite state machine and the recurrence matrix
5	A chosen cipher text attack	Very difficult	Very difficult due to the inverse recurrence matrix multiplication without knowing apt key
6	An adaptive chosen cipher text attack	Very difficult	Very difficult due to the mathematical calculations

4. CONCLUSIONS

Algorithm proposed, is based on finite state machine (Moore machine) and matrix multiplication. In this algorithm linear recurrence relation of order 2 is used. Secrecy is maintained at two levels, one is key and other is key matrix obtained using recurrence relation. The obtained cipher text becomes quite difficult to break or to extract the original information even if the algorithm is known.

5. ACKNOWLEDGMENTS

Our thanks to Dr.K.R.Sudha Chandra Sekhar who have contributed her valuable ideas in presenting the paper.

6. REFERENCE

[1] A.P. Stakhov, ”The ‘‘golden’’ matrices and a new kind of cryptography”, Chaos, Soltions and Fractals 32((2007) pp1138–1146

[2] A.P. Stakhov. “The golden section and modern harmony mathematics. Applications of Fibonacci numbers,”7,Kluwer Academic Publishers; (1998). pp393–99.

[3] A.P. Stakhov. “The golden section in the measurement theory”. Compute Math Appl; 17(1989):pp613–638.

[4] K.R.Sudha , A.chandra Sekhar ,Prasad Reddy P.V.G.D. “ Cryptography protection of Digital Signals using some recurrence relations” International Journal of Computer Science and Network security, Vol (7) no 5 m may 2007 ,203-207.

[5] D.Sravan Kumar.Ch.Suneetha A.Chandra Sekhar “ Encryption of Data streams using Paul’s spin ½ matrices”, International Journal of Engineering science and Technology. Vol2(6), 2010, 2024 -2028.

[6] Adesh K.Pandey. reprint 2009, “An introduction to automata theory and formal languages ‘S.K.Kararia & sons. New Delhi.

[7] A.Menezed, P.Van Oorschot and S.Vanstone Hand book of Applied Cryptography e-Book

[8] W. Y. YE Yongwei and YANG [4]Qinghua, (2003) “Magic cube encryption for digital image using chaotic sequence”, Journal of Zhejiang University of Technology, 31(2):173–176.

[9] Z. L. Z. X. feng and FAN Jiu-lun, (2007) “A digital image encryption algorithm based onchaotic sequences”, Microelectronics & Computer, 2.

[10] John E.Hopcroft, Rajeev Motwain, Jeffrey D.Ulman. “ Introduction to automata theory,language,and computation” Vanstone3rd impression,2007 CRC Press.,Dorling Kindersley (India) Pvt.Ltd