

Designing a Cryptosystem by Implementing Reversible Sequential Switching M/C – A Symmetric Key Approach.

Rati R. Sahoo¹, Girija S. Rath²

¹Department of Computer Science & Engg.
Krupajal Engineering College
Bhubaneswar, Orissa, India

²Department of Electronics & Communication Engg.
National Institute of Technology
Rourkela, Orissa

¹rati_mtech@yahoo.com

²qs Rath@nitrkl.ac.in

Abstract-This paper introduces an abstract model of reversible sequential machine in designing the cryptosystem based on the symmetric key approach. A reversible sequential machine is a one-to-one mapping old state and input to new state and output. Reversible computing machine is the mapping of old computational state to new computational state is one-to-one. The abstract model of the reversible sequential machine developed here for a cryptosystem is presented as a 4-tuple $M(\text{state, input, output, mapping-function})$ machine. In this machine, the mapping of present state and input to next state and output by residue number system.

I. INTRODUCTION

Since the cryptosystem developed in this paper is based on the principle of the reversible sequential machine, the principle of the reversible sequential machine is represented in brief. Block cipher matrix mostly based on the private key. It uses the principle of block codes. Reversible sequential machine as we suggest is a new concept arising out from these papers[9][10].

1.1 A General Model of Sequential Machine

- A general model of sequential machine, described by 6-tuple machine described as a set $M = \{Q, X, Z, f, g, q_0\}$.
- where $x = \{x_1, x_2, \dots, x_l\}$ represents the l -inputs vector,

- $z = \{z_1, z_2, \dots, z_m\}$ represents m -output vectors,
- $Q = \{q_0, q_1, q_2, \dots, q_n\}$ are the n -internal states of the machine
- $Q = f(x, Q)$, where f is a transition function
- $z = g(x, Q)$, where g is output function
- q_0 initial state

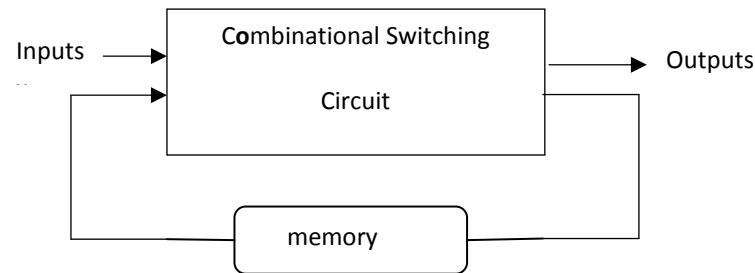


Fig. 1.1 Sequential Switching Circuit

The sequential machine defined by the above model is not reversible in general as the mapping of input space to output space is not necessarily onto mapping [2], and moreover in general the [6]combinational logic formed by AND, OR, NOT gates does not give the onto mapping from input to output.

II. The Abstract Model Of A Reversible Sequential Machine M

The abstract model of a reversible sequential machine M is a 4-tuple represent by the equations $M = (Q, X, Z, f)$, Where X is a finite set of input symbols.

Z is a finite set of output symbols.
Q is the finite set of internal states
f is a function that maps the present state q_i and input x_i to next state q_j and output z_j .
The machine will be reversible if f^{-1} exists.
This is presented in Fig.1.2

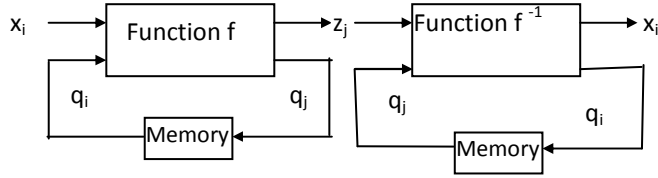


Fig.1.2 Reversible sequential machine

A model of “A reversible sequential machine based on modular arithmetic function” is proposed^[7]. This Mathematically is presented by equations (1.1) and (1.2). All the symbols used in these equations are based on residue number system.

$$\begin{bmatrix} z_j \\ q_j \end{bmatrix} = [f] \begin{bmatrix} x_i \\ q_i \end{bmatrix} \quad (1.1)$$

$$\text{And } \begin{bmatrix} x_i \\ q_i \end{bmatrix} = [f]^{-1} \begin{bmatrix} z_j \\ q_j \end{bmatrix} \quad (1.2)$$

Since the model is based on matrices with elements are of residue number system, then existence of the inverse of a square matrix is explained in the next section.

III. MODULAR ARITHMETIC

Let A be a 2×2 matrix with element of residue numbers of modulus M ^[8]. Then

$$A^{-1} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}^{-1} = \frac{1}{\Delta a} \begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix} \quad (1.3)$$

where Δa is the determinant of A mod. M. So the inverse will exist iff $\Delta a \text{ Mod } M \neq 0$ and the inverse of the determinant $\Delta a \text{ mod. } M$ exists

IV. SYMMETRIC KEY DISTRIBUTION

Symmetric-key cryptography is more efficient than asymmetric-key cryptography for enciphering large messages^[3]. Symmetric key cryptography, however, needs a shared secret key between two parties. The message that is sent through the channel is called the

ciphertext. To create the ciphertext from the plaintext, an encryption algorithm is used with the shared secret key. To create the plaintext from ciphertext, a decryption algorithm is used and use the same secrete key. The resistance of the cipher to attack should be based only on the secrecy of the key.

V. A SUGGESTED MODEL OF CRYPTOSYSTEM

In order to make the cryptosystem a practical robust system, this proposed model for the encryption uses 7-bit ASCII characters x and one 7-bit state vector q . Residue number system of mod 127 (the highest 7-bit prime number) is used for encryption as well as. In this model the cipher- texts are transmitted but not the states. Since the states are not transmitted, it is not possible to decipher the input text, unless another quantity is known at the receiving end. This quantity may be a state or an input texts that is to be known at the receiving end. In this paper, it is assumed that the initial state q_0 is known at the receiving end. Then using the following equation, one can obtain all the input texts from the set cipher texts. Thus if encryption algorithm can be explained mathematically as

$$\begin{bmatrix} z_i \\ q_{i+1} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} x_i \\ q_i \end{bmatrix} \text{ mod } M \quad (1.4)$$

where x_i , z_i and q_i are the i^{th} input plain text, output cipher text and state respectively. The plain texts x_i are ciphered sequentially from initial text x_0 to final text x_n assuming an initial state q_0 . At the receiving end, only cipher texts z_i are received. These cipher texts are deciphered sequentially by the following equation (1.5).

$$\begin{bmatrix} x_i \\ q_{i+1} \end{bmatrix} = \frac{1}{a_{11}} \begin{bmatrix} 1 & -a_{12} \\ a_{21} & a_1 a_{22} - a_{12} a_{21} \end{bmatrix} \begin{bmatrix} z_i \\ q_i \end{bmatrix} \text{ mod } M \quad (1.5)$$

Eqn.(1.5) detects that mod inverse of a_{11} must exists. If one takes a prime number as modulus, then the mod inverse of a_{11} will exist if it does not equal to zero. By knowing the initial state (q_0) and ciphered value Z_0 we can find the character value x_0 and next state.

VI. EXPERIMENT AND RESULT

For experimentation and verification of above algorithm, the encryption and decryption matrices are taken as $\begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$ and $\begin{bmatrix} 64 & 62 \\ 2 & 126 \end{bmatrix} \pmod{127}$ respectively.

PLAIN TEXT

Julius Caesar used a cryptosystem in his wars, which is now referred to as Caesar cipher. It is an additive cipher with the key set to three. Each character in the plaintext is shifted three characters to create cipher text.

CIPHER TEXT

```
BMIQkCHyJH-,g
;1$!q-----V
c(p'uk-c8M-02D{<@VIH je-   ^rWgRN-!P\C)y

y,ISM- 5&t{
      ^*!AqM?e&]XH}OOGqAb#c0"ngB^
-----
O+ds-----CyF
%d38K}f!tS;;1e&h%o`

Fx^v^{a 1>mb!l/

SYubwEl,e
-----
=-
MQ@li1~(zuzl{XnGC`?
-----
```

DECIPHER TEXT

Julius Caesar used a cryptosystem in his wars, which is now referred to as Caesar cipher. It is an additive cipher with the key set to three. Each character in the plaintext is shifted three characters to create cipher text.

From this test it is resulted that cryptanalysis will be difficult in using single letter frequency statistics to break the cipher text.

VIII. CRYPTANALYS

- Brute Force Attack:** In this reversible machine, there two public used. The first key is 2×2 cipher matrix of mod 127. The number of such keys that can be formed (non-trivial and invertible) 250047000. Moreover, the other public key the initial state q_0 which will be one out of 126 non-trivial state. Thus, altogether there will be effectively 3.1×10^{10} number of symmetric keys available, Therefore it is highly difficult to find out the key by the brute-force attack.
- Differential Crypto Analysis:** Since the key for encryption and the key for decryption are different differential analysis may be an effective attack It is experimentally found that there is no correlation between frequency of occurrence plain text and the cipher text as shown in fig.1.3 and Fig. 1.4

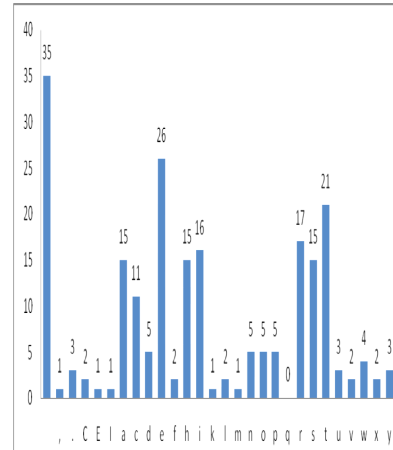


Fig.1.3 Frequency of plain texts

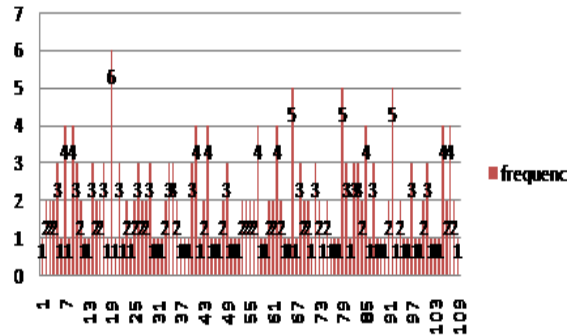


Fig. 1.4 Frequency of cipher text

Therefore, it becomes difficult to predict the key in differential crypto-analysis. Moreover, when this scheme is extended to large prime number to represent the characters and states, then it becomes almost impossible to obtain private key.

VIII. CONCLUSION AND FUTURE WORK

To enhance the power of security further research is in progress. By introducing known state at any arbitrary position the encryption can be made more robust. Moreover, block of characters can be encrypted by using large prime number

REFERENCES

- [1] Behrouz A. Forouzan, Cryptography & Network Security
- [2] G. P. Saradhi Varma & B.Thirupathi Rao, Theory of Computation
- [3] Williams Stalling, Cryptography and Network Security.
- [4] J Storrs Hall, An Electroid Switching model for reversible computer architecture, Proc. 1992 Physics of Computation Workshop, IEEE
- [5] J K Mantri & T.K. Tripathy, A modern Approach to Discrete Mathematics and structure.
- [6] Morris Mano, Digital Electronics
- [7] V.U.K.Sastry, V. Janaki, "On the Modular Arithmetic Inverse in the Cryptology of Hill Cipher", Proceeding of North American Technology and Business Conference, September 2005.
- [8] S. Udaya Kumar, V.U.K.Sastry, A Vinaya babu, "A Block Cipher Basing Upon a Revisit to the Feistel Approach and the Modular Arithmetic Inverse of a Key Matrix", IAENG International Journal of Computer Science, 32:4, IJCS_32_4_1.
- [9] Yi-Shiung, Tzong-Chen Wu, "Private Key Crypto System based on enforced Random Substitution Scheme" CH3031-2/91/0000-03.19 1991 IEEE.
- [10] T.R.N. RAO, FELLOW, IEEE, AND KIL-HYUNNAM, "Private-Key Algebraic-Code Encryptions", IEEE Transactions on Information Theory, Vol. 35, No. 4. JULY. 1989.