International Journal of Computer and Internet Security.
ISSN 0974-2247 Volume 3, Number 1 (2011), pp. 41-50
© International Research Publication House
http://www.irphouse.com

Reliable Data Transmission by using S-Boxes in Multi-Station Network by using Various Keys

Ajay Kakkar, M.L. Singh and P.K. Bansal

Thapar University, Patiala, India
G.N.D.U., Amritsar, India
Ex-Professor, TU, India.

Abstract

The requirement of data security is an important parameter for all the industries and government for their survival in the world. Government requires the technique which provides the highest level of the security with minimum number of overheads; moreover the model does not allow the hacker to penetrate the security area, i.e the number of attempts made by the hacker should be reduced, it can be done by reducing the time during transmission. The key must be generated from the data based on permutation. The paper deals with the various factors: Latency, energy consumption, Index of Coincidence, Measure of Roughness, Compression Factor; important to provide the information about the security level of the algorithm.

Keywords: Encryption, S-Boxes, Measure of Roughness, Index of Coincidence, Compression Factor.

Introduction

Security is an important parameter; almost all the industries and organization required this in order to protect their secret information to their competitors. To achieve security various techniques are used such as passwords, encryption techniques, biometrics and many more, but out of all these cryptography with good encryption algorithm having large key length is used [3]. The passwords are not treated as reliable for this task. It is easy to guess passwords due to its short range [1,2,4]. The cryptography technique is used to avoid unauthorized access of data, which is used for web security. The algorithm generally open to the other members of the community where as the key is kept secret. Earlier the key used for encryption/decryption was very large in size; assumed that impossible to guess. The results show that the software available in the market breaks the key within seconds. The expansion of key leads to the overheads therefore it is preferred to use S-boxes with multiple keys of short length (combination of alphabets and numbers). Encryption is the science of scrambling data to make it indecipherable to all, except the intended person. Almost all the credit card transaction taking place on the internet, Due to recent developments in software and hardware, some consumer level encryption products are now so powerful that law enforcements officials say they can't crack them, even with massive supercomputers. The main purpose of cryptography is to protect the interests of parties communicating in the presence of adversaries.

Related Work

In India the work is done on DES, TDES, Blowfish, AES, RSA used in addition with S-Boxes to provide more security. All these techniques are effective to provide security but at the same time they have their own limitations, like time consuming, key transmission from sender to receiver, station failures, and key lost. The keys are based upon mathematical expression so many times they result in error during decryption process [2,5,10]. Currently, the concept of multiple techniques is used, at present it is possible to break key having1028 word length (bits) with in 10 minutes that means increasing the length of key is just a time consuming process for the designer, not a reliable technique. So instead of increasing the key, multiple techniques are used where more then two functions are used to make the system optimized and reliable. i.e the output of first operation is given to the second and output of the second to the third and so on. Depending upon the requirement the numbers of levels (Round Functions) are taken. Combination of Public and private key cryptography results in modern key cryptography, widely used in abroad [9,11,12].

Proposed Work

Modern cryptography involves the use of keys for data signing, encoding, and decoding. Some keys are distributed privately keys between the parties, while others allow the parties to use public keys that can be broadcast openly [13]. Level of protection is varied for every situation and also dependent upon the work and technique used, some encryption techniques provide a virtually unbreakable barrier to information theft; others just require a determined attacker with moderate resources to be broken. One way to compare techniques on this level is to estimate how much CPU time would be required on a machine of a given processing speed to iterate through all the possible keys to the encoded data, based upon the permutation. System-wide security always required to make sure that it is safe; data is safe for some time by using security techniques but overall system is not safe, by using the information about timing, power consumption, and radiation of a device when it executes a cryptographic algorithm, cryptanalysts have been able to break system. So aim should be to make the combination secure.

Parameters

Where $D_{i,j}$=Data, S_1, S_2...... S_5 = S-Boxes, C = Capacity, N = Noise, S_n = maximum number of S-boxes. g, h= buffers, E= Initial Encryption, $\grave{S}_1$ = Stage1. K= Key Size,

S'_n = Round Functions, l_{Si} = Smallest value of Latency. E_T = Encryption Time. P_l = probability of linear expression, P_o = probability of optimized linear expression, N_S = Number of S-boxes used in linear expression. P_i =Probability of arbitrarily selected character of alphabet / numbers, M = Total number of Messages.

Problem

During the transmission of data if any station fails, due to the attacks made by the hacker or by other means (atmospheric conditions) then it make the overall model weak. So to maintain the security over a model, all the parameters such as nodes, key generation mechanism, latency, e.t.c need continuous attention, they must be upgraded w.r.t. time. Each station required to be packed up by the recovery mechanism. It is important to calculate the latency time concerned with particular station. We know that all the keys are functions of mathematical properties so the Initial permutations, IP are calculated w.r.t Round Functions (8,16,64) based upon the algorithm for each stage. Encrypted data then compressed by using DCT technique. The frequency and the measure of roughness also determined because they are used to compress the data which saves the buffer space [3,4,5].

Table 1

Initial Permutation				
$S^{`}_1$	$S^{`}_2$	$S^{`}_3$	$S^{`}_4$	$S^{`}_5$
43	12	56	34	55
24	25	64	13	10
55	46	45	57	59

Table 2

Data Length(Bits)	Key Size (Bits)	Compression Factor	Index of Coincidence	Measure of Roughness
8	8	0.21	0.024	0.021
16	8	0.29	0.034	0.038
32	8	0.32	0.047	0.041
64	8	0.34	0.055	0.053
256	8	0.55	0.059	0.059

Encryption process is based upon the Count (∑ (Data, Key, Compression, Padding))/36*36 ≤ 1

Shown in Table 3 for each user). The database needs at least a mechanism which restricts the sum of all the parameters less than or equal to 1. Increasing from the limit creates a burden over the system also it permits the facility to the hacker to go for no. of attacks. For n data lengths, the count lies: n ≤ (Encryption Key) ≤ N-n and n ≥ 0

Table 3

User A	User B	User C	User D	User E
0.001	0.041	0.023	0.043	0.054
0.041	0.031	0.032	0.052	0.008
0.065	0.009	0.034	0.075	0.073
0.012	0.017	0.022	0.047	0.056
0.024	0.078	0.010	0.055	0.035

Model:

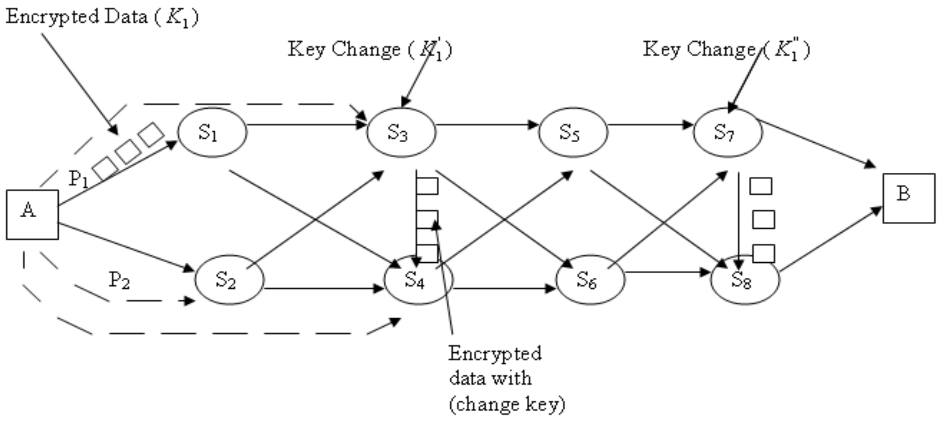

Fig 3: Multiple stations having various paths in Multinode Network

Let us take a case in which user A wants to transmit the data through the channel having stages (S_1, S_2,……… S_8). Multiple paths are provided to send the data in the figure. P_1 is the path where encrypted packets are transmitted by A. Similarly other P_2, P_3 and other paths can be made. For a secure system all the intermediate nodes/stations should be under the control of A. If any node gets an attack from the hacker then it should be comes under the knowledge of A immediately, required actions must be taken i.e. change of path and re-encryption by using the change key [5,6].

$$Path\ P_1 : A \rightarrow S_1 \in (K_1) \rightarrow S_3 \in (K_1, K_1^{'}) \rightarrow S_4 \rightarrow S_5 \rightarrow S_7 (K_1, K_1^{'}, K_1^{''}) \rightarrow S_8 \rightarrow B$$

In figure S_3 is the weak station then either change key for the encryption:

$$Path\ P_1 : A \rightarrow S_1 \in (K_2) \rightarrow S_3 \in (K_2, K_2^{'}) \rightarrow S_4 \rightarrow S_5 \rightarrow S_7 (K_2, K_2^{'}, K_2^{''}) \rightarrow S_8 \rightarrow B$$

or change path:

(i) $Path\ P_1 : A \rightarrow S_2 \in (K_1) \rightarrow S_3 \in (K_1, K_1^{'}) \rightarrow S_4 \rightarrow S_5 \rightarrow S_7 (K_1, K_1^{'}, K_1^{''}) \rightarrow S_8 \rightarrow B$

(ii) $Path\ P_2 : A \rightarrow S_2 \in (K_2) \rightarrow S_3 \in (K_2, K_2^{'}) \rightarrow S_4 \rightarrow S_5 \rightarrow S_7 (K_2, K_2^{'}, K_2^{''}) \rightarrow S_8 \rightarrow B$

For highly secure system transmission done from $A \rightarrow S_4$.

Note: All the station has the power to change the key and encrypt the data with it only iff A permits

Example

If $X_1 = inputs, S_1 = WeakStations, \overline{S_1} = StrongStations$

Case 1: When two stations are under the attacks made by hacker (failures of 2 S-boxes in a given model):

In this case it is required to change the key for the particular stations but it will be not treated as a reliable method, so it will be preferred to change the path, for this it is required to determine the input data as concerned to weak stations.

Calculations

$$X_1 \xrightarrow{Key} S_1, X_2 \xrightarrow{Key} S_2 \ \& \ X_{1,2} \xrightarrow{Key} S_1 \ \& \ S_2$$

We know that

$$S_1 = X_1 \cup X_{1,2}, S_2 = X_2 \cup X_{1,2} ....(1)$$

On the other side,

$$S_1 \cap S_2 = (X_1 \cap X_2) \cup X_{1,2} ....(2)$$

If

$$x_i = P_r(X_i), \quad x_{i,j} = P_r(X_{i,j})$$

Compliment

$$P_r(X_i^C) = 1 - P_r(X_i) ....(3)$$

$$\sum_i^N P(X_i) = 1....(4)$$

Compliment

$$\sum_i^N P_r(X_i^C) = \sum_i^N 1 - P_r(X_i) = N - 1....(5)$$

Similarly we can determine the probabilities of S-boxes are

$$s_i = P_r(S_i), \quad s_{i,j} = P_r(S_{i,j}) ....(6)$$

By using equation 2 we can write

$$s_1 = x_1 + x_{1,2} - x_1.x_{1,2}$$

$$s_2 = x_2 + x_{1,2} - x_2.x_{1,2}$$

$$s_{1,2} = x_1.x_2 + x_{1,2} - x_1.x_2.x_{1,2} .....(7)$$

Rearrange the equation in order to get the probability of $x_1, x_1 \ \& \ x_{1,2}$

$$x_1 = \frac{x_1 - x_{1,2}}{1 - x_2},$$

$$x_2 = \frac{x_2 - x_{1,2}}{1 - x_1},$$

$$x_{1,2} = \frac{x_{1,2} - x_1 . x_2}{1 - x_1 - x_2 - x_{1,2}} \ldots .(8)$$

Similarly for 4 weak stations in a model it is required to determine the single failure S_i, double failures $S_{i,j}$, triple failures $S_{i,j,k}$ and quadrate failures $S_{i,j,k,m}$. For strong stations R_i the probabilities are determined by using complements (eq.3). $P_r(R_i) = P_r(X_i^C)$ or $r_i = P_r(R_i), \quad = 1 - x_i$

In terms of strong stations

$$P_r(\overline{S_1}) = 1 - x_1 = r_1 \cdot r_{1,2} \cdot r_{1,3} \cdot r_{1,4} \cdot r_{1,2,3} \cdot r_{1,3,4} \cdot r_{1,2,4} \cdot r_{1,2,3,4}$$

$$P_r(\overline{S_2}) = 1 - x_2 = r_2 \cdot r_{1,2} \cdot r_{2,3} \cdot r_{2,4} \cdot r_{1,2,3} \cdot r_{1,2,4} \cdot r_{2,3,4} \cdot r_{1,2,3,4}$$

$$P_r(\overline{S_3}) = 1 - x_3 = r_3 \cdot r_{1,3} \cdot r_{2,3} \cdot r_{3,4} \cdot r_{1,2,3} \cdot r_{1,3,4} \cdot r_{2,3,4} \cdot r_{1,2,3,4}$$

$$P_r(\overline{S_4}) = 1 - x_4 = r_4 \cdot r_{1,4} \cdot r_{2,4} \cdot r_{3,4} \cdot r_{1,2,4} \cdot r_{1,3,4} \cdot r_{2,3,4} \cdot r_{1,2,3,4} \ldots .\theta)$$

Also

$$P_r(\overline{S_1} \cap \overline{S_2}) = P_r(\overline{S_1 \cup S_2}) = 1 - s_1 - s_2 + s_{1,2} = r_1 \cdot r_2 \cdot r_{1,2} \cdot r_{1,3} \cdot r_{2,3} \cdot r_{1,4} \cdot r_{2,4} \cdot r_{1,2,3} \cdot r_{1,3,4} \cdot r_{1,2,4} \cdot r_{1,2,4} \cdot r_{2,3,4} \cdot r_{1,2,3,4}$$

$$P_r(\overline{S_1} \cap \overline{S_3}) = P_r(\overline{S_1 \cup S_3}) = 1 - s_1 - s_3 + s_{1,3} = r_1 \cdot r_3 \cdot r_{1,2} \cdot r_{1,3} \cdot r_{2,3} \cdot r_{1,4} \cdot r_{3,4} \cdot r_{1,2,3} \cdot r_{1,3,4} \cdot r_{1,2,4} \cdot r_{2,3,4} \cdot r_{1,2,3,4}$$

$$P_r(\overline{S_1} \cap \overline{S_4}) = P_r(\overline{S_1 \cup S_4}) = 1 - s_1 - s_4 + s_{1,4} r_1 \cdot r_4 \cdot r_{1,2} \cdot r_{1,4} \cdot r_{1,3} \cdot r_{2,4} \cdot r_{3,4} \cdot r_{2,4} \cdot r_{1,2,3} \cdot r_{1,2,4} \cdot r_{1,3,4} \cdot r_{1,2,4} \cdot r_{2,3,4} \cdot r_{1,2,3,4}$$

$$P_r(\overline{S_2} \cap \overline{S_3}) = P_r(\overline{S_2 \cup S_3}) = 1 - s_2 - s_3 + s_{2,3} = r_2 \cdot r_3 \cdot r_{1,2} \cdot r_{1,3} \cdot r_{2,3} \cdot r_{2,4} \cdot r_{3,4} \cdot r_{1,2,3} \cdot r_{1,2,4} \cdot r_{1,3,4} \cdot r_{2,3,4} \cdot r_{1,2,3,4}$$

$$P_r(\overline{S_2} \cap \overline{S_4}) = P_r(\overline{S_2 \cup S_4}) = 1 - s_2 - s_4 + s_{2,4} = r_2 \cdot r_4 \cdot r_{1,2} \cdot r_{1,4} \cdot r_{2,3} \cdot r_{2,4} \cdot r_{2,4} \cdot r_{3,4} \cdot r_{1,2,3} \cdot r_{1,2,4} \cdot r_{1,2,4} \cdot r_{1,3,4} \cdot r_{2,3,4} \cdot r_{1,2,3,4}$$

$$P_r(\overline{S_3} \cap \overline{S_4}) = P_r(\overline{S_3 \cup S_4}) = 1 - s_3 - s_4 + s_{3,4} = r_3 \cdot r_4 \cdot r_{1,2} \cdot r_{1,3} \cdot r_{1,4} \cdot r_{2,3} \cdot r_{2,4} \cdot r_{3,4} \cdot r_{1,2,3} \cdot r_{1,2,4} \cdot r_{1,3,4} \cdot r_{2,3,4} \cdot r_{1,2,3,4}$$

$$P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3}) = P_r(\overline{S_1 \cup S_2 \cup S_3}) = 1 - s_1 - s_2 - s_3 + s_{1,2} + s_{1,3} + s_{2,3} - s_{1,2,3} = r_1 \cdot r_2 \cdot r_3 \cdot r_{1,2} \cdot r_{1,3} \cdot r_{2,3} \cdot r_{1,4} \cdot r_{2,4} \cdot r_{3,4} \cdot r_{1,2,3} \cdot r_{1,3,4} \cdot r_{1,2,4} \cdot r_{2,3,4} \cdot r_{1,2,3,4}$$

$$P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_4}) = P_r(\overline{S_1 \cup S_2 \cup S_4}) = 1 - s_1 - s_2 - s_4 + s_{1,2} + s_{1,4} + s_{2,4} - s_{1,2,4} = r_1 \cdot r_2 \cdot r_4 \cdot r_{1,2} \cdot r_{1,4} \cdot r_{1,3} \cdot r_{2,3} \cdot r_{2,4} \cdot r_{1,4} \cdot r_{2,4} \cdot r_{3,4} \cdot r_{1,2,3} \cdot r_{1,2,4} \cdot r_{1,3,4} \cdot r_{2,3,4} \cdot r_{1,2,3,4}$$

$$P_r(\overline{S_1} \cap \overline{S_3} \cap \overline{S_4}) = P_r(\overline{S_1 \cup S_3 \cup S_4}) = 1 - s_1 - s_3 - s_4 + s_{1,3} + s_{1,4} + s_{2,4} - s_{1,2,4} = r_1 \cdot r_3 \cdot r_4 \cdot r_{1,2} \cdot r_{1,3} \cdot r_{1,4} \cdot r_{2,3} \cdot r_{2,4} \cdot r_{3,4} \cdot r_{1,2,3} \cdot r_{1,2,4} \cdot r_{1,3,4} \cdot r_{2,3,4} \cdot r_{1,2,3,4}$$

$$P_r(\overline{S_2} \cap \overline{S_3} \cap \overline{S_4}) = P_r(\overline{S_2 \cup S_3 \cup S_4}) = 1 - s_2 - s_3 - s_4 + s_{1,2} + s_{2,3} + s_{2,4} - s_{1,2,4} = r_2 \cdot r_3 \cdot r_4 \cdot r_{1,2} \cdot r_{1,3} \cdot r_{1,4} \cdot r_{2,3} \cdot r_{2,4} \cdot r_{3,4} \cdot r_{1,2,3} \cdot r_{1,2,4} \cdot r_{1,3,4} \cdot r_{2,3,4} \cdot r_{1,2,3,4}$$

$$P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3} \cap \overline{S_4}) = P_r(\overline{S_1 \cup S_2 \cup S_3 \cup S_4}) = 1 - s_1 - s_2 - s_3 - s_4 + s_{1,2} + s_{1,3} + s_{1,4} + s_{2,3} + s_{2,4} + s_{3,4} - s_{1,2,3} - s_{1,2,4} - s_{1,3,4} - s_{2,3,4} + s_{1,2,3,4}$$

$$= r_1 \cdot r_2 \cdot r_3 \cdot r_4 \cdot r_{1,2} \cdot r_{1,3} \cdot r_{1,4} \cdot r_{2,3} \cdot r_{2,4} \cdot r_{3,4} \cdot r_{1,2,3} \cdot r_{1,2,4} \cdot r_{1,3,4} \cdot r_{2,3,4} \cdot r_{1,2,3,4}$$

Now determine the values of $x_i, x_{i,j}, x_{i,j,k}, x_{i,j,k,l}$

$$x_1 = 1 - \frac{P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3} \cap \overline{S_4})}{P_r(\overline{S_2} \cap \overline{S_3} \cap \overline{S_4})}$$

$$x_2 = 1 - \frac{P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3} \cap \overline{S_4})}{P_r(\overline{S_1} \cap \overline{S_3} \cap \overline{S_4})}$$

$$x_3 = 1 - \frac{P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3} \cap \overline{S_4})}{P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_4})}$$

$$x_4 = 1 - \frac{P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3} \cap \overline{S_4})}{P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3})}$$

$$x_{1,2} = 1 - \frac{P_r(\overline{S_1} \cap \overline{S_3} \cap \overline{S_4}) \cdot P_r(\overline{S_2} \cap \overline{S_3} \cap \overline{S_4})}{P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3} \cap \overline{S_4}) \cdot P_r(\overline{S_3} \cap \overline{S_4})}$$

$$x_{1,3} = 1 - \frac{P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_4}) \cdot P_r(\overline{S_2} \cap \overline{S_3} \cap \overline{S_4})}{P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3} \cap \overline{S_4}) \cdot P_r(\overline{S_2} \cap \overline{S_4})}$$

$$x_{1,4} = 1 - \frac{P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3}) \cdot P_r(\overline{S_2} \cap \overline{S_3} \cap \overline{S_4})}{P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3} \cap \overline{S_4}) \cdot P_r(\overline{S_2} \cap \overline{S_3})}$$

$$x_{2,3} = 1 - \frac{P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_4}) \cdot P_r(\overline{S_1} \cap \overline{S_3} \cap \overline{S_4})}{P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3} \cap \overline{S_4}) \cdot P_r(\overline{S_1} \cap \overline{S_4})}$$

$$x_{2,4} = 1 - \frac{P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3}) \cdot P_r(\overline{S_1} \cap \overline{S_3} \cap \overline{S_4})}{P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3} \cap \overline{S_4}) \cdot P_r(\overline{S_1} \cap \overline{S_4})}$$

$$x_{3,4} = 1 - \frac{P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3}) \cdot P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_4})}{P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3} \cap \overline{S_4}) \cdot P_r(\overline{S_1} \cap \overline{S_2})}$$

$$x_{1,2,3} = 1 - \frac{P_r(\overline{S_1} \cap \overline{S_4}) \cdot P_r(\overline{S_2} \cap \overline{S_4}) \cdot P_r(\overline{S_3} \cap \overline{S_4}) \cdot P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3} \cap \overline{S_4})}{P_r(\overline{S_4}) \cdot (P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_4})(P_r(\overline{S_1} \cap \overline{S_3} \cap \overline{S_4})(P_r(\overline{S_2} \cap \overline{S_3} \cap \overline{S_4}))}$$

$$x_{1,2,4} = 1 - \frac{P_r(\overline{S_1} \cap \overline{S_3}) \cdot P_r(\overline{S_2} \cap \overline{S_3}) \cdot P_r(\overline{S_3} \cap \overline{S_4}) \cdot P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3} \cap \overline{S_4})}{P_r(\overline{S_3}) \cdot (P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3})(P_r(\overline{S_1} \cap \overline{S_3} \cap \overline{S_4})(P_r(\overline{S_2} \cap \overline{S_3} \cap \overline{S_4}))}$$

$$x_{1,3,4} = 1 - \frac{P_r(\overline{S_1} \cap \overline{S_2}) \cdot P_r(\overline{S_2} \cap \overline{S_3}) \cdot P_r(\overline{S_2} \cap \overline{S_4}) \cdot P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3} \cap \overline{S_4})}{P_r(\overline{S_2}) \cdot (P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3})(P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_4})(P_r(\overline{S_1} \cap \overline{S_3} \cap \overline{S_4}))}$$

$$x_{2,3,4} = 1 - \frac{P_r(\overline{S_1} \cap \overline{S_2}) \cdot P_r(\overline{S_1} \cap \overline{S_3}) \cdot P_r(\overline{S_1} \cap \overline{S_4}) \cdot P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3} \cap \overline{S_4})}{P_r(\overline{S_1}) \cdot (P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3})(P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_4})(P_r(\overline{S_1} \cap \overline{S_3} \cap \overline{S_4}))}$$

$$x_{1,2,3,4} = 1 - \frac{P_r(\overline{S_1}) \cdot P_r(\overline{S_2}) \cdot P_r(\overline{S_3}) \cdot P_r(\overline{S_4}) \cdot P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3}) \cdot}{(P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_3} \cap \overline{S_4}) \cdot P_r(\overline{S_1} \cap \overline{S_2}) \cdot P_r(\overline{S_1} \cap \overline{S_3})} \, \frac{P_r(\overline{S_1} \cap \overline{S_2} \cap \overline{S_4}) \cdot P_r(\overline{S_1} \cap \overline{S_3} \cap \overline{S_4}) \cdot P_r(\overline{S_2} \cap \overline{S_3} \cap \overline{S_4})}{\cdot P_r(\overline{S_1} \cap \overline{S_4}) \cdot P_r(\overline{S_2} \cap \overline{S_3}) \cdot P_r(\overline{S_2} \cap \overline{S_4}) \cdot P_r(\overline{S_3} \cap \overline{S_4})}$$

So by using equation (2.a) all the values of $x_i, x_{i,j}, x_{i,j,k}, x_{i,j,k,l}$ are calculated. The cryptographic key pair needs maintenance; in order to keep up with the increasing processing power available for breaking the keys, the keys need to be replaced periodically [6,7]. This will also limit the possibility of damage in a situation where somebody has managed to steal a copy of the secret key. Buffers g,h (fig 1) are provided to each stations to store the incoming data and the key used to re-encrypt the data. Probability of optimized linear expression is calculated by:

$$\left|P_l - 0.5\right| \le 2^{N_S} \cdot \left|P_o - 0.5\right|^{N_S} \text{....(10)}$$

The size of the key and the data length after the encryption process, provide the flexibility to choose the desired round functions as shown in table 4.

Table 4

Key Size and Data Length after Encryption				
Round Functions		36	1296	46656
	8	4.5	162	5832
	16	2.25	81	2916
	32	1.125	40.5	1458
	64	0.5625	20.25	729

For Asymmetric key different operations are required. (i) X-OR and use of S-boxes (ii) generation of key from the data. It has been observed that all the alphabets have their own frequency, i.e. occurrence of alphabet in given information. If all the common alphabets were processed in one step then it will reduce the overheads of the system.

For a given message M in a set of $Y_{0,}Y_{1,\ldots\ldots\ldots\ldots}Y_{n-1}$, the probability $\sum_{i=0}^{n-1} P(Y_i) = 1$, the conditional probability of message X in a given message Y is $P_Y(X)$, also be written as $P(X/Y)$. The joint probability messages X & Y:

$$P(X,Y) = P_Y(X)P(Y)$$

The entropy is calculated as

$$H_Y(X) = \sum_{X,Y} P(X,Y)\log_2(1/P_Y(X))$$

$$H_Y(X) = -\sum_{X,Y} P(X,Y)\log_2 P_Y(X)$$

or

$$H_Y(X) = \sum_{Y} P(Y)\sum_{X} P_Y(X)\log_2(1/P_Y(X))$$

$$H_X(Y) = \sum_{X} P(X)\sum_{Y} P_X(Y)\log_2(1/P_X(Y))$$

We know that probability always $0 \leq P_i \leq 1$. For $n \to \infty$ the chance of getting the exact alphabet is reduce [9]. $P_i \cong 0$ Means increase in the bits of information in one processing unit results increase in security of the model. So it would be preferred to increase the no. of bits at the Transmitter side with increase in number of rounds so that all the S boxes gets almost equal number of bits. For alphabet and numbers:

$$P_i = \sum_{i=0}^{35} (M - 1/36)^2$$

$$P_i = \sum_{i=0}^{35} (M)^2 - 2/36 \sum_{i=0}^{35} (M)^2 + 36(1/36)^2$$

For identical M second data is same with first. i.e. $\sum_{i=0}^{35} (M)^2 = 1$

$$\therefore P_i = \sum_{i=0}^{35} (M)^2 - 2/36 + 1/36 \qquad P_i = \sum_{i=0}^{35} (M)^2 - 0.084$$

The above example is applicable if model contains few stages. For larger stages the probability of finding the correct message (P_M) is: $P_M = \frac{S(k)}{D} = \frac{\log_2 d!}{D}$

S(k)= number of stages, D= total data handled by the model, d= data of individual stage, e= bits used in encryption process.

For $D \to \infty$ and large data for a stage $d \to n$ the equation changes:

$$P_M = \frac{\log_2 n!}{D}$$

From the last equation correct message is obtained which would provide the information about the number of bits used for the encryption process.

Conclusion & Future Scope

For a secure system key when generated from the data. The information about the input data provide is required in order to choose the operation and select the number of keys and Round function. It is also important to calculate the number of bits required for the encryption; basically they provide the knowledge about the key length. Moreover in case of multiple S-Boxes different keys are used, although it creates a burden over the model but at the same time increases the security level. Table 7 shows that how different keys are generated from the different data. For the future work; the time required for the processing of video data is too large, so it is main task in now a days how to make it minimize. So that it not put a limit on the model. Further if the final data obtain after the encryption process made compressible to 37% then it can be used in adhoc networks. The goal of efficient encryption is to provide *near-prefect confidentiality* with a minimum of overhead.

References

[1] W.G. Tzeng, “A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy,” IEEE Trans. Knowledge and Data Eng., Proc. Sixth ACM Symp. Access Control Models and Technologies (SACMAT ’01), vol. 14, no. 1, pp. 182-188, Jan./Feb. 2002.

[2] Z. S. Wang Lingqun, Zheng Yingping. Application of data mining and data protection in medicine. Computer Engineering, 31(10):54-56,May 2005

[3] J. Jung, V. Paxson, A.W. Berger, and H. Balakrishnan, “Fast Portscan Detection Using Sequential Hypothesis Testing,” Proc. IEEE Symp. Security and Privacy, pp. 211-225, 2004.

[4] C.C. Zou, W. Gong, and D. Towsley, “Code Red Worm Propagation Modeling and Analysis,” Proc. ACM Conf. Computer and Comm. Security, pp. 138-147, 2002.

[5] C.C. Zou, L. Gao, W. Gong, and D. Towsley, “Monitoring and Early Warning for Internet Worms,” Proc. ACM Conf. Computer and Comm. Security, pp. 190-199, 2003.

[6] Jing Deng, Yunghsiang S. Han, “Multipath Key Establishment for Wireless Sensor Networks using just-Enough Redundancy Transmission”, IEEE Transactions on Dependable and Secure Computing, pp177-190, Vol. 5, No. 3, July-September 2008.

[7] Jussi K. Vaurio, “Treatment of General Dependencies in System Fault-Tree and Risk Analysis” IEEE Transactions on Reliability, Vol. 51, No. 3, September 2002, pp. 134–157.

[8] H.-Y. Chien, “Efficient Time-Bound Hierarchical Key Assignment Scheme,” IEEE Trans. Knowledge and Data Eng., vol. 16, no. 10, pp. 1302-1304, Oct. 2004.

[9] X. Yi, “Security of Chien’s Efficient Time-Bound Hierarchical Key Assignment Scheme,” IEEE Trans. Knowledge and Data Eng., vol. 17, no. 9, pp. 1298-1299, Sept. 2005.

[10] S. Ross, Stochastic Processes, second ed. John Wiley & Sons, 1996.

[11] S. V. Amari, J. B. Dugan, and R. B. Misra, “A separable method for incorporating imperfect fault-coverage into combinatorial models,” *IEEE Trans. Reliability*, vol. 48, no. 3, pp. 267–274, Sep. 1999.