Approach towards Optimum Data Transfer with Various Automatic Variable Key (AVK) Techniques to Achieve Perfect Security with Analysis and Comparison

Rajat S Goswami
Department of CSE
NIT Arunachal Pradesh, India

Swarnendu K Chakraborty
Department of CSE
NIT Arunachal Pradesh, India

Abhinandan Bhunia
Microsoft Corporations, USA

Chandan T Bhunia
Director
NIT Arunachal Pradesh, India

ABSTRACT
Session to session key variation is the only approach for achieving perfect security as per Shannon [1-2]. This paper deals with time variant key technique Automatic Variable Key (AVK) introduced by Bhunia[3-5] and we tried to analyze the performance of different types of new AVK techniques.

Keywords
AVK, CSAVK, ASAVK, DSAVK, KVRN Protocol, Randomness, Perfect Security.

1. INTRODUCTION
In all cryptosystem the Key challenge of the designer is to make key unbreakable. Shannon proposed that key would be impossible to break if the key is made time variant. The time variant key can be implemented by changing key from session to session. AVK was one of the noble approaches for achieving perfect security invented by Bhunia [3-5]. The superiority of time variant key in achieving perfect security is studied elsewhere [6-14].In AVK technique which illustrated in Table-1 the key is made variable by an agreement that creates new key for each data. This is reviewed as below:

Say, K_0 = initial key that may be exchanged by any conventional secret mode between a sender and a receiver.

Subsequent keys for different data (Di-1) to be exchanged are generated are:

$K_i=K_{i-1}$ XOR D_{i-1} for $i\geq0$............................ (1)

The key is made variable with exchanged data between a sender and a receiver. A new key is generated every time a data is exchanged. The new key so generated is used subsequently for further exchange of data.

The illustrated technique of AVK has been extensively applied in both private and public key cryptography. The application is found to reduce brute force attack, frequency attack and differential frequency attack [7-14].

So far applied AVK is based on the generating function XOR as in equation (1).

In CSAVK [14] technique illustrated in below the key is made variable by one agreement that also creates new key for each data.

Say, K_0 = initial key that may be exchanged by any conventional secret mode between a sender and a receiver.

Subsequent keys for different data (D_{i-1}) to be exchanged are generated are:

$K_i = K'_{i-1}$ XOR D'_{i-1} for $i\geq0$..................................... (2)

Table 1: Elucidation of application of simple AVK in cryptology

Session slots	Sender sends his /her private key to receiver	Receiver recovers private key from sender	Receiver sends his / her private key to sender	Sender receives private key from receiver	Remarks
1	Secret key Say 5(101)	101	A secret key Say 7(111)	111	For next slot sender will use 111 as key and receiver 101 as key for transmitting data
2	Sender sends first (random 3) data 011 $\oplus$ 111 =100	Receiver gets original data 011 $\oplus$ 111 $\oplus$ 111=011	Receiver sends first (random data 9) as 1001 $\oplus$ 0101=1100	Sender gets back original data as 1001 $\oplus$ 0101 $\oplus$ 0101	Sender will create new key 0111 $\oplus$ 1001 for next slot receiver will create new key 101 $\oplus$ 011
3	Sender sends new data 4(100) as 0100 $\oplus$ 0111 $\oplus$ 1001	Receiver recovers original data as 0100 $\oplus$ 0111 $\oplus$ 1001 $\oplus$ 0111 $\oplus$ 1001= 0100	Receiver sends next data 8 (1000)1000 $\oplus$ 0101 $\oplus$ 0011	Sender receives original data 1000 $\oplus$ 0101 $\oplus$ 0011 $\oplus$ 0101 $\oplus$ 0011 =1000	Sender computes new key 011 $\oplus$ 100 receiver computes key 1001 $\oplus$ 1000 for transmitting next data

In ASAVK [14] technique illustrated in below the key is made variable by one another agreement that also creates new key for each data.

- Initial key (K_0) is exchanged between the sender and the receiver.
- Subsequent key, K_i (at i^{th} stage) is generated by both sender & receiver as :

Step1: $K_i = K'_{i-1}$ XOR D_{i-1} for $i \geq 0$…...... (3)
Step2: $K_{i+1} = K_{i-1}$ XOR D'_{i-1} for $i \geq 0$....... (4)
Where K'_{i-1} = Block wise shift (Circular) K_{i-1} / the number of shift will be total length of K_{i-1} divided by 2.
D'_{i-1} = Block wise shift (Circular) D_{i-1} / the number of shift will be total length of D_{i-1} divided by 2.

In DSAVK [12] technique illustrated in below the key is made variable by another agreement that also creates new key for each data.

- Initial key (K_0) is exchanged between the sender and the receiver.
- Subsequent key, K_i (at i^{th} stage) is generated by both sender & receiver as :
  $K_i = K'_{i-1}$ XOR D_{i-1} for $i \geq 0$……………..... (5)
  Where K'_{i-1} = Bit wise right shift (Circular) K_{i-1} / the number of shift will be the corresponding decimal value of K_{i-1} XOR D_{i-1}.

In KVRN [14] technique illustrated in below the key is made variable by another agreement that also creates new key for each data.

- Initial key (K_0) and one numeric value (m) is exchanged between the sender and the receiver.
- Subsequent key, K_i (at i^{th} stage) is generated by both sender & receiver as :

$K_i = K_{i-1}+X$ for $i \geq 0$ and X=1 to m ………......... (6)
Where K_{i-1} = Previous key
When X=m, another key (K_m) and another numeric value (n) is exchanged between the sender and the receiver.
Subsequent key will be generated same way as eqn. 6.

In Protocol-I [13] technique illustrated in below the key is made variable by another agreement that also creates new key for each data.

- Initial key (K_0) and one noise burst (m) is exchanged between the sender and the receiver by RSA.
- Subsequent key, K_i (at i^{th} stage) is generated by both sender & receiver as :

$K_i = K_{i-1}$ XOR D_{i-1} (AVK technique) for $i \geq 0$ ..... (7)
When X=m, another key (K_m) and another noise burst (n) is exchanged between the sender and the receiver.
Subsequent key will be generated same way as eqn. 7 & process will repeat.

In Protocol-II [13] technique illustrated in below the key is made variable by another agreement that also creates new key for each data.

- Initial key (K_0) and one noise burst (m) is exchanged between the sender and the receiver by RSA.
- Subsequent key, K_i (at i^{th} stage) is generated by both sender & receiver as :

$K_{i+1} = K'_i$ XOR D'_i (CSAVK technique) for $i \geq 0$ ... (8)
When X=m, another key (K_m) and another noise burst (n) is exchanged between the sender and the receiver.
Subsequent key will be generated same way as eqn. 8 & process will repeat.

In Protocol-III [13] technique illustrated in below the key is made variable by another agreement that also creates new key for each data.

- Initial key (K_0) and one noise burst (m) is exchanged between the sender and the receiver by RSA.
- Subsequent key, K_i (at i^{th} stage) is generated by both sender & receiver as :

$K_i = K'_{i-1}$ XOR D_{i-1} (DSAVK technique) for $i \geq 0$ ...... (9)
When X=m, another key (K_m) and another noise burst (n) is exchanged between the sender and the receiver.
Subsequent key will be generated same way as eqn. 8 & process will repeat.

The key is made variable with exchanged data between a sender and a receiver every time a data is exchanged. The new key so generated is used subsequently for further exchange of data.

2. NEW IDEA

So far in AVK techniques, the main lacuna is to keep the initial key highly secret. In AVK, initial Key is distributed between sender by RSA or by key distribution centre.
We propose a new technique to exchange the initial key of AVK as follows:
Instead of sending one key, we proposed to send three keys. Say "101010101","11001001" and "00100110" are the initial keys exchanged between sender & receiver by RSA. Sender & Receiver will perform bit-wise majority logic operation among three keys to agree upon to the first key. In the example, therefore the first key is generated as;
10101010
11001001
00100110

10101010, after majority logic original initial key under different AVK techniques will be "10101010". The superiority of the proposed technique used in AVK is justified in terms of the probability of Key-breaking. In the probability of Key-breaking is P, as in normal AVK, the same for the proposed technique is P^3 (<P).

3. Illustration of AVK, CSAVK, ASAVK, DSAVK, PROTOCOL-I, PROTOCOL-II and PROTOCOL-III

3.1 Illustration of AVK

Let we assume that sender sends original data (D_0) 00000100 in encrypted form using an initial key (K_0) = 10101010. Then in order to maintain the linearity, the encrypted form is 00000100 XOR 10101010 = 10101110.
At receiver end receiver will perform 10101110 XOR 10101010 and gets 00000100.

3.2 Illustration of CSAVK

Let sender sends initial data D_0 (01010101) in encrypted form using key K_0(10101010). As per technique of CSAVK of eqn. (2) next key will be generated as K_0 =10101010. The process will then be continued.
But in the next data transmission key will be changed by left shifting the previous data (D_0) up to the total number of 1's present in that data (SD_0) XOR with right shifting the

previous key (K_0) up to the total number of 1's present in that key (SK_0).
So the new key will be K_1= SD_0+ SK_0 = 00001000 XOR 10101010 = 10100010.

3.3 Illustration of ASAVK

Let sender sends initial data D_0 (00000000) in encrypted form using key K (11001010). By the technique of ASAVK as in eqn.(3-4), the next key will be generated by block shift operation and will be K_0=10101100.
But in the next data transmission key will be, block shifting of the previous data (D_0) named as (SD_0) XOR with the previous key (K_0) .
So the new key will be K_1= SD_0+ K_0 = 00000000 XOR 10101100 = 10101100.

3.4 Illustration OF DSAVK

Let sender sends initial data D_0 (00000000) in encrypted form using key K (00000110). By the technique of DSAVK as in eqn.5 , the next key will be generated by right shift operation and will be K_0=00011000 (Right shift will be up to decimal equivalent of (D_0 XOR K)).

3.5 Illustration of KVRN

Let sender sends initial data D_0 (00000000) in encrypted form using key K_0 (00000110) and one numeric value m (3). By the technique of KVRN as in eqn. 6 , the next keys will be generated by adding 1 (00000001), 2 (00000010) and 3 (00000011) subsequently with K_0=00011000. So the next keys will be K_0+m_i (i=1, 2 & 3). When the value of m will reach 3, new key (K_m) and another numeric value (n) will be exchange between sender and receiver.

4. ANALYSIS AND COMPARISON

For analysis and comparison of AVK, CSAVK, ASAVK, DSAVK, PROTOCOL-I, PROTOCOL-II AND PROTOCOL-III we assume two parameter explained as below:

4.1 Analysis by randomness

Randomness as a measure of amount of variation made between keys. The randomness for the purpose is defined as the number of bit location in which any two successive key vary. For example if:

K_i=10101010, K_{i+1}=10001111

The randomness between two successive key is 3. We call K_{i+1} is random to K_i by 3.

We measure the randomness for one initial key K_0= 10101010 to perform key generation of AVKs, CSAVKs, ASAVKs, DSAVKs and for KVRN, PROTOCOL-I, PROTOCOL-II, PROTOCOL-III technique the set of initial keys are {10101010, 01101110, 11010010, 10111110, 01101111, 10011011 }, for set of initial data {10000101, 1011001, , 11101, 11101011, 1100001, 1000010, 1001110, 11111, 11100010, 1100001, 1100001, 10011101, 1011001, 10011010, 10000011, 10111011, 100000, 11011110, 10111, 10001100, 1111100, 1101, 10000101, 11110001, 1011, 11101100, 11111001, 11101010, 111111, 1010110, 10011101, 10111101, 11110011, 11010011, 10110110, 1011001, 10010111, 100100, 100001, 10100, 10010000, 1011100, 10111011, 11111001, 1010001, 101111, 10100001, 11011010, 101100, 10101110, 1101110, 101011, 10011001, 1011000, 11010101, 1000010, 10110000, 101001, 1101010, 10011010, 11111100, 11001100, 11011100, 11101111, 10101111, 101011, 1000110, 11111100, 11010111, 1101, 11010101, 11010101, 10010010, 10010000, 1111100, 10001111, 110101, 10110100, 11100100, 1011000, 10110111, 10000001, 11010011, 1101001, 1011011, ,11000000, 10001, 1001001, 10100010, 10111100, 11111000, 100111, 11100110, 11111001, 10000001, 11111011, 1110110, 11000011, 1010010, 10100110 }

The randomness as defined was calculated by run of a programme and results so obtained are portrayed in fig.1, fig.2, fig.3, fig.4, fig.5, fig.6 , fig.7 and fig.8.

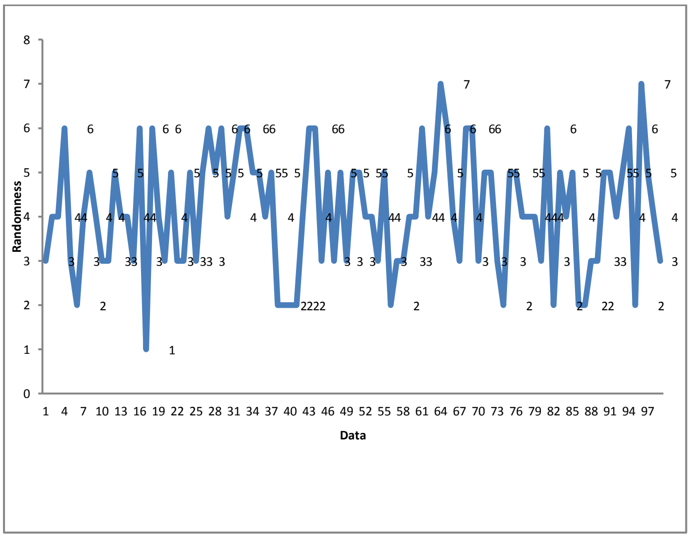

Fig.1: Randomness of keys of AVK

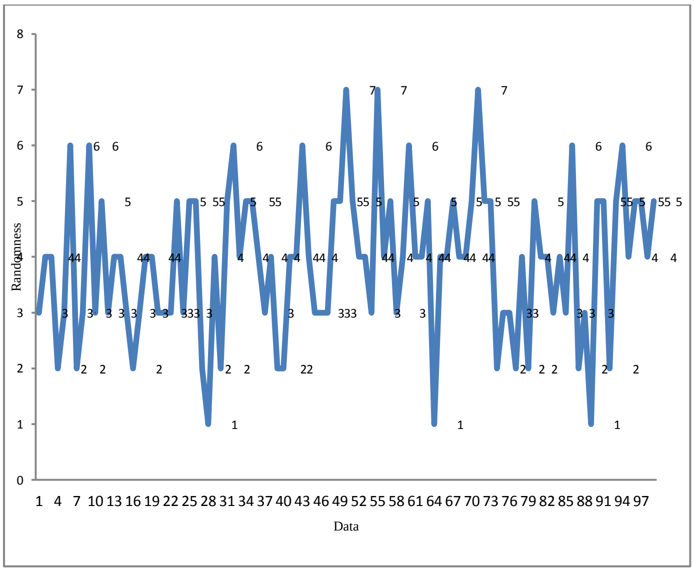

Fig.2: Randomness of keys of CSAVK

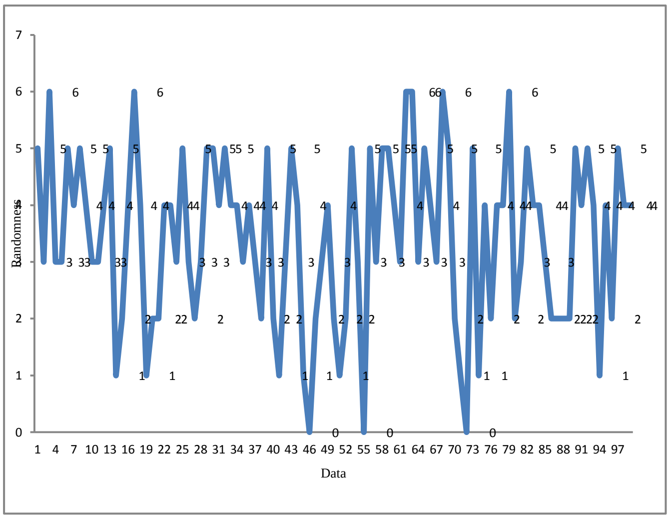

Fig.3: Randomness of keys of DSAVK

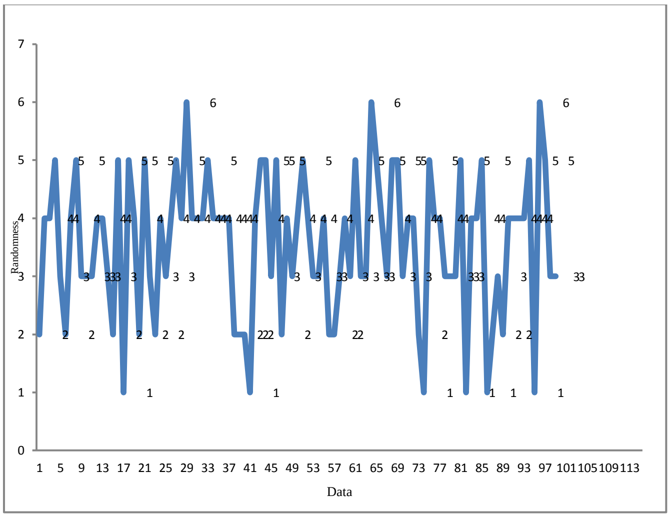

Fig.6: Randomness of keys of Protocol-I

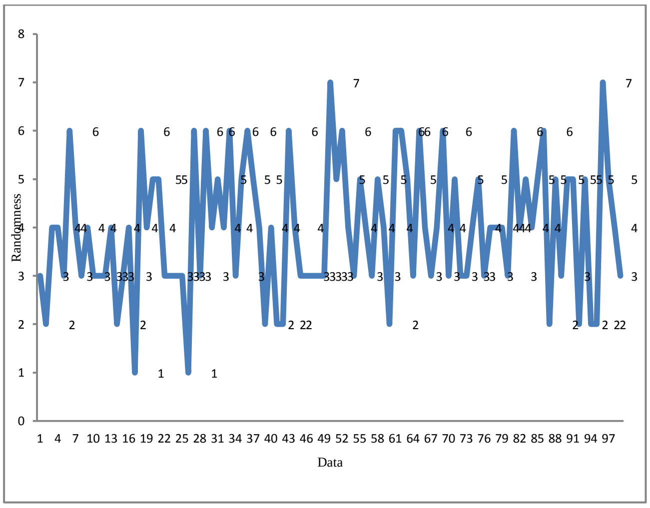

Fig.4: Randomness of keys of ASAVK

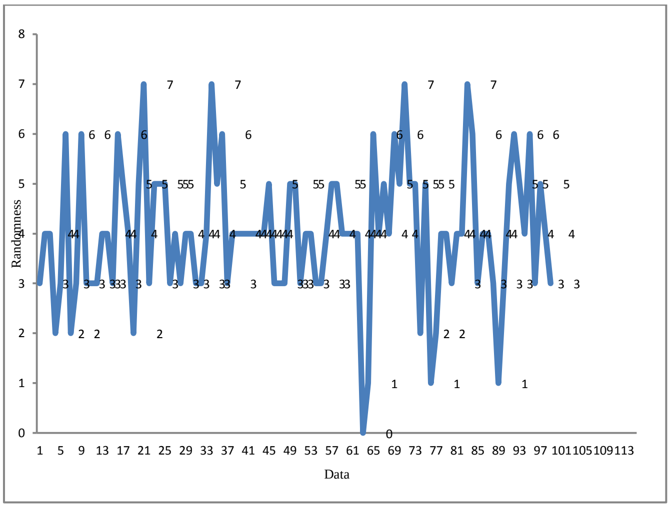

Fig.7: Randomness of keys of Protocol-II

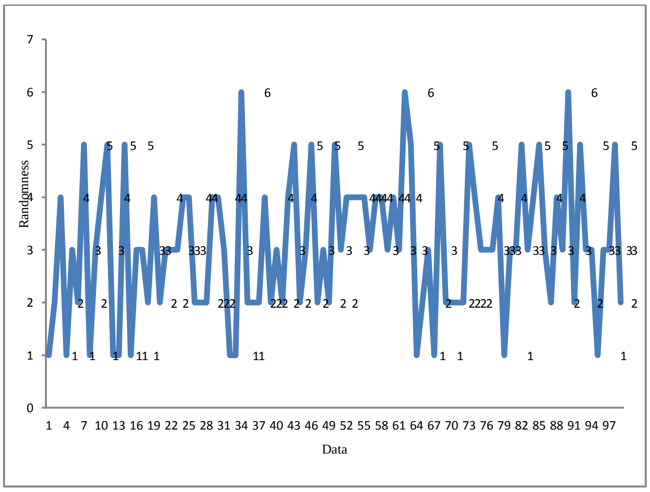

Fig.5: Randomness of keys of KVRN

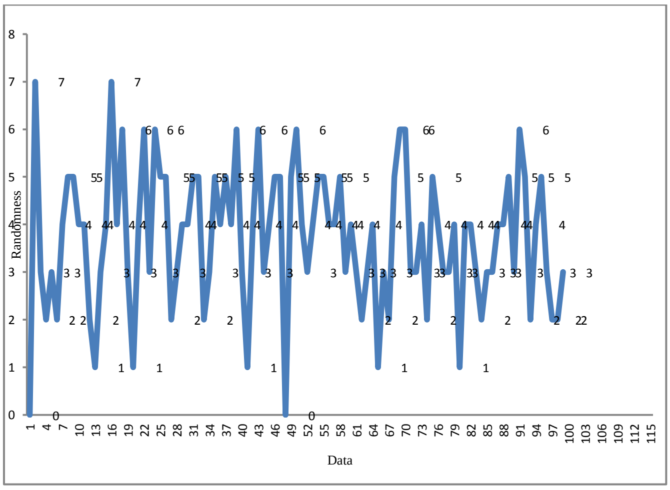

Fig.8: Randomness of keys of Protocol-III

4.2 Analysis by RMS

In all previous studies the variation types of AVKs were compared in terms of absolute measure of randomness that measures the number of position in which bit differs in two successive keys. Such a measure does not reflect a consolidated parameter for comparing the techniques.

We introduce a parameter of RMS of randomness for comparison of the techniques. The measured RMS variation is shown in fig.9.

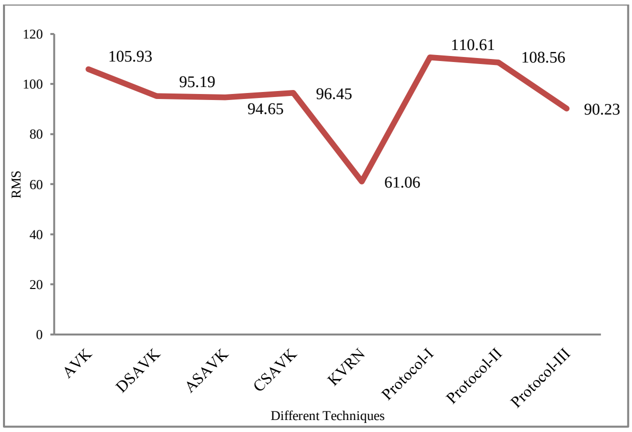

Fig.9: comparison of RMS of AVK, CSAVK, ASAVK, DSAVK, PROTOCOL-I, PROTOCOL-II and ROTOCOL-III

5. CONCLUSIONS

Based on result reported so far we find that so far RMS variation is concerned the proposed Protocol – I and Protocol- II are superior to other techniques. The new approach of initial key fixation by majority logic provides a confidence of application of AVK

6. REFERENCES

[1]. C E Shannon, "Mathematical theory of communication", The Bell System Tech J, Vol. 27,1984, pp. 379-423, 623-656.

[2]. C E Shannon, "Communication Theory of Secrecy System", The Bell System Tech J, 1949.

[3]. C.T.Bhunia, G.Mondal, and S.Samaddar, "Theory and application of time variant key in RSA and that with selective encryption in AES", 2006, Indian Engineering Congress, Kolkata.

[4]. C. T. Bhunia, "New approaches for selective AES towards tackling error propagation effect of AES," Asian Journal of Information Technology, vol.5990, pp.1017-1022,2006.

[5]. P. Chakrabarti, B. Bhuyan, A. Chowdhuri and C.T.Bhunia, "A novel approach towards realizing optimum data transfer and automatic variable key (AVK)," International Journal of Computer Science and Network Security, vol.8,no.5,May2008.

[6]. C Konar, C T Bhunia, "A novel approach towards realizing optimum Data Transfer and AVK in cryptography",International Journal of Computer Science and Network Security, Vol 8, No 5, 2008, pp. 241-250.

[7]. C T Bhunia, "New Approaches for Selective AES towards Trackling Error Propagation Effect of AES", Asian Journal of Information Technology, Pakistan, Volume 5, No. 9, pp 1017- 1022, 2006.

[8]. C T Bhunia et al, "Implementation of Automatic Variable Key with Choas Theory and Studied Thereof", J IUP Computer Science, Vol V, No 4, 2011, pp 22-32.

[9]. C T Bhunia et al, "Theories and Application of Time Variant Key in RSA and that with selective encryption in AES", Proc. EAIT, Elsevier Publications, Calcutta CSI 2006, pp 219-221.

[10]..Chakrabarty, C T Bhunia et al, "A novel approach towards realizing optimum Data Transfer and AVK in cryptography", International Journal of Computer Science and Network Security, Korea, Vol 8, No 5, May 2008, pp. 241-250.

[11].C. T. Bhunia, Swarnendu Kumar Chakraborty, Rajat Subhra Goswami, "A New Technique (CSAVK) of Automatic Variable Key in Achieving Perfect Security", 100th Indian Science Congress Association 3rd – 7th, January, 2013.

[12].Rajat Subhra Goswami, Swarnendu Kumar Chakraborty, Abhinandan Bhunia, C. T. Bhunia, "New approach towards generation of Automatic Variable Key to achieve Perfect Security", 10th International Conference on Internet Technology, Next Generation, ITNG, 2013, 14th – 17th April' 2013, IEEE computer Society, CPS, pp:489-491.

[13].Rajat Subhra Goswami, Swarnendu Kumar Chakraborty, Abhinandan Bhunia, C. T. Bhunia, "Various New Methods of Implementing AVK", 2nd International Conference on Advances in computer Science & Engineering, CSE2013, 1st – 2nd July' 2013, Atlantis Press, pp: 149-152.

[14].Rajat Subhra Goswami, Swarnendu Kumar Chakraborty, Abhinandan Bhunia, C. T. Bhunia, "Generation of Automatic Variable Key under various approaches in Cryptography System", Communicated to Journal of the Institution of Engineers (India).