Various New Methods of Implementing AVK

Rajat Subhra Goswami
Department of Computer Science and Engineering,
National Institute of Technology, Arunachal Pradesh-791112, India
(Email: rajat.nitap@gmail.com)

Swarnendu Kumar Chakraborty
Department of Computer Science and Engineering,
National Institute of Technology, Arunachal Pradesh - 791112, India
(Email:swarnendu.chakraborty@gmail.com)

Abhinandan Bhinia
Microsoft Corporation , USA
(Email:abhi1.bhunia@gmail.com)

C. T. Bhunia
Department of Computer Science and Engineering,
National Institute of Technology, Arunachal Pradesh - 791112, India
(Email:ctbhunia@vsnl.com)

***Abstract*—Researchers have proposed many data encryption techniques / standards to protect data from various types of attacks like brute force attack, frequency attack and differential frequency attack. Shannon [1-2] documented the theory of perfect secrecy with time variant key. An idea of time variant key namely Automatic Variable Key (AVK) was introduced by Bhinia [4-6]. The superiority of AVK was widely experimented by many researchers over a fixed or single key [7-14]. This paper proposed new protocols of Automatic variable Key (AVK) in cryptography.**

Keywords-Perfect Security, RSA, DES, AVK, Computing & Shifting AVK (CSAVK), Decimal Shifting AVK (DSAVK), Randomness.

I. INTRODUCTION

To establish the superiority of time variant key in achieving perfect security is studied in [7-14]. The main challenge for the researchers / designers is to generate a key for producing the cipher document. The famous Vernum code was the first attempt to achieve perfect security but no effective variable key was applied or no concrete theory was established. The fundamental research of Shannon [1-2] in light of perfect security is that, the secret key will vary from session to session. An idea of time variant key, namely Automatic Variable Key (AVK) has been introduced by Bhunia [4-6]. Reasonable amount of research on AVK has been done elsewhere [7-14].

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 (D_{i-1}) to be exchanged are generated are:

$$K_i = K_{i-1} \text{ XOR } D_{i-1} \text{ for } i \geq 0 \quad (1)$$

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 [4-10].

II. VARIOUS NEW IDEAS OF AVK TECHNIQUE

In CSAVK [11,13] 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:

$$K_i = K'_{i-1} \text{ XOR } D'_{i-1} \text{ for } i \geq 0 \quad (2)$$

Where K'_{i-1} = Bit wise right shifted (circular) K_{i-1} / the number of shift will be the number of 1's present in K_{i-1}.

D'_{i-1} = Bit wise left Shifted (Circular) D_{i-1} / the number of shift will be number of 1's present in D_{i-1}.

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 :

$$K_i = K'_{i-1} \text{ XOR } D_{i-1} \text{ for } i \geq 0 \quad (3)$$

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}.

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.

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 ⊕ 111 =100	Receiver gets original data 011 ⊕ 111 ⊕ 111=011	Receiver sends first (random data 9) as 1001 ⊕ 0101=1100	Sender gets back original data as 1001 ⊕ 0101 ⊕ 0101 =1001	Sender will create new key 0111 ⊕ 1001 for next slot receiver will create new key 101 ⊕ 011
3	Sender sends new data 4(100) as 0100 ⊕ 0111 ⊕ 1001	Receiver recovers original data as 0100 ⊕ 0111 ⊕ 1001 ⊕ 0111 ⊕ 1001= 0100	Receiver sends next data 8 (1000)1000 ⊕ 0101 ⊕ 0011	Sender receives original data 1000 ⊕ 0101 ⊕ 0011 ⊕ 0101 ⊕ 0011 =1000	Sender computes new key 011 ⊕ 100 receiver computes key 1001 ⊕ 1000 for transmitting next data

III.NEW IDEAS

We propose various new ways for generation of key in AVK. The objective is to enhance the level of security by making more randomness between successive AVKs.

The new ideas for generation of key are as below:

A. PROTOCOL-I:

i) Initial key (K_0) and one noise burst (m) is exchanged between the sender and the receiver by RSA.

ii) 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 $i \geq 0$ ..... (4)

iii) When X=m, another key (K_m) and another noise burst (n) is exchanged between the sender and the receiver.

iv) Subsequent key will be generated same way as eqn. 4 & process will repeat.

Example: In first case if k_{i-1} =1001, D_{i-1}=1000 and m=2, the subsequent keys will be:

Step 1:First key=1001 ⊕ 1000 = 0001

Step 2: Next key =0001 ⊕ 1001(D_i) = 1000

Step 3: New key and another noise burst will be exchanged between sender and receiver.

B. PROTOCOL-II:

i) Initial key (K_0) and one noise burst (m) is exchanged between the sender and the receiver by RSA.

ii) Subsequent key, K_i (at i^{th} stage) is generated by both sender & receiver as :

$$K_{i+1}=K'_i \text{ XOR } D'_i \text{ (CSAVK technique)}$$
$$\text{for } i\geq 0 \ldots\ldots\ldots \quad \ldots\ldots (5)$$

iii) When X=m, another key (K_m) and another noise burst (n) is exchanged between the sender and the receiver.

iv) Subsequent key will be generated same way eqn. 5 & process will repeat.

Example: In first case if k_{i-1} =1001, D_{i-1}=1000 and m=2, the subsequent keys will be:

Step 1:First key=0110 ⊕ 0001 = 0111

Step 2: Next key =1110 ⊕ 0110 (Assuming previous data = 1001) = 1000

Step 3: New key and another noise burst will be exchanged between sender and receiver.

C. PROTOCOL-III:

i) Initial key (K_0) and one noise burst (m) is exchanged between the sender and the receiver by RSA.

ii) Subsequent key, K_i (at i^{th} stage) is generated by both sender & receiver as :

$$K_i = K'_{i-1} \text{ XOR } D_{i-1} \text{ (DSAVK technique)}$$
$$\text{for } i\geq 0 \ldots\ldots\ldots \quad \ldots\ldots (6)$$

iii) When X=m, another key (K_m) and another noise burst (n) is exchanged between the sender and the receiver.

iv) Subsequent key will be generated same way as eqn. 6 & process will repeat.

Example: In first case if k_{i-1} =100 , D_{i-1}=111and m=2, the subsequent keys will be:

Step 1:First key=111 ⊕ 010 = 101

Step 2: Next key =101 ⊕ 110 (D_{i-1}) = 011

Step 3: New key and another noise burst will be exchanged between sender and receiver.

IV.ILLUSTRATION OF AVK, CSAVK & DSAVK

A. ILLUSTRATION OF AVK

Let we assume that sender sends original data (D_0)00000100 in encrypted form using an initial key (K) = 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.

B. ILLUSTRATION OF CSAVK

Let sender sends initial data D_0(01010101) in encrypted form using key K(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 XOR SK_0 = 00001000 XOR

10101010 = 10100010.

C. 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.3 , 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)).

V. ANALYSIS AND COMPARISON

For analysis and comparison of Protocol -I, Protocol -II, Protocol -III we assume a parameter of randomness as a measure of amount of variation made between the successive 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.

For the three new technique the set of initial keys are {11001010, 10101100,11111111 }, initial numeric numbers are {16,16,16 } and perform key generation for the set of initial data {00000000, 00000001, 00000010, 00000011, 00000100, 00000101, 00000110, 00000111, 00001000, 00001001, 01010, 00001011, 00001100, 00001101, 0001110, 00001111, 00010000, 00000000, 000001, 00000010, 00000011, 00000100, 00000101, 00000110, 00000111, 00001000, 00001001, 0000110, 00001011, 00001100, 00001101, 00001110, 00001111, 00010000, 00000000, 00000001, 00000010, 00000011, 00000100, 00000101, 00000110, 00000111, 00001000, 00001001, 0000010, 00001011, 00001100, 00001101, 00001110, 00001111, 00010000 }.

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

VII. CONCLUSIONS

From the comparison of the results portrayed in fig. (1-3) it is found that:

- Randomness for the set of data and set of initial key under experiment, is more in protocol-II and in protocol-III than that in protocol-I
- Randomness as measure under the same experiment is more in protocol-II than that in protocol-III.
- In term of randomness in variant key, protocol-II is superior to both protocol-III & protocol-I.

We propose to apply the techniques in AES; and examine brute force attack & differential frequency attack in subsequent studies.

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] P.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 Information

Technology, ITNG, 2013, IEEE Computer Society, Proceedings pp-102.

[13] Rajat Subhra Goswami, Swarnendu Kumar Chakraborty, Abhinandan Bhunia, C. T. Bhunia, "New Techniques for generating of Automatic Variable Key in Achieving Perfect Security", Communicated to Journal of the Institution of Engineers (India).

[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).

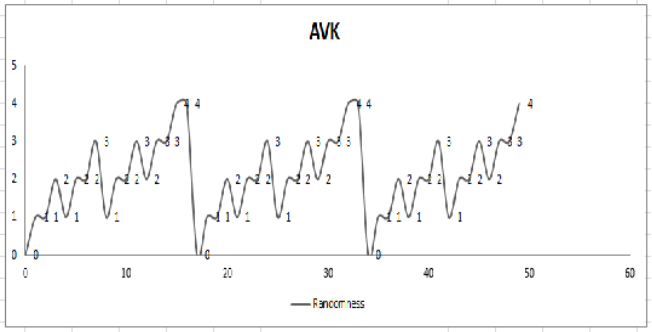

fig.1: Randomness of keys of Protocol-I

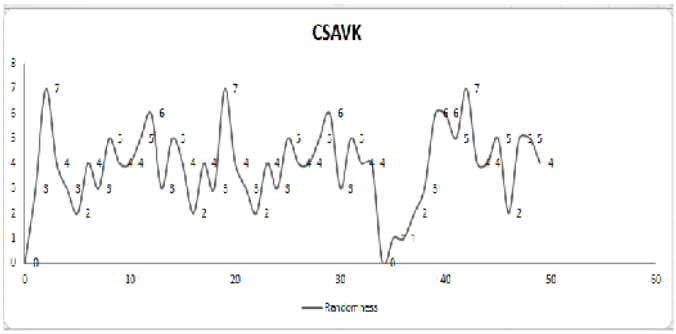

fig.2: Randomness of keys of Protocol -II

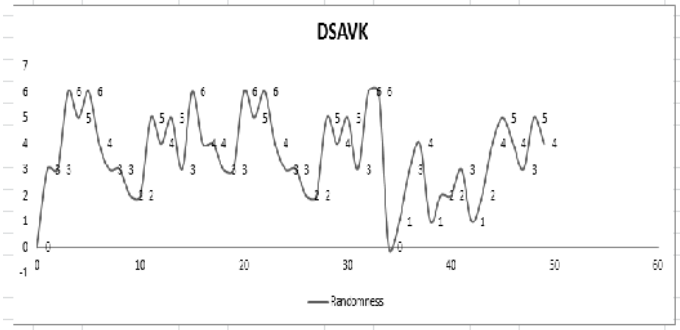

fig.3: Randomness of keys of Protocol -III