Asian Journal of Convergence in Technology **Volume V Issue I**
ISSN No.:2350-1146, I.F-5.11

To Achieve Higher Security in Automatic Variable Key Technique towards Optimum Data Transfer with Noise Burst in Cryptosystem

Moumita Das[1], Rajat Subhra Goswami[2] , R. S. Mehta[3] , S. K. Chakraborty[4], P.Pal[5] , C. T.Bhunia[6]
Department of Computer Science & Engineering[1,2,4,6] , National Institute of Technology[1,2,4,6] Arunachal Pradesh[1,2,4,6] - 791112, INDIA, Department of Computer Science & Engineering[3,5,6]
Durgapur Institute of Advanced Technology & Management[3,5,6], West Bengal-713212, INDIA

Abstract- *In this manuscript, we have proposed new key generation techniques with noise burst based on established variable key generation techniques. To verify the true randomness of the proposed techniques, we have tested the randomness of successive generated keys by using National Institute of Standards and Technology (NIST) statistical tool and tested with the standard algorithm RC4 and proved that the generated keys are truly random. The proposed techniques provide maximum level of security as compared to those related existing techniques as the newly generated keys are more random. Due to the enhanced randomness, it can be stated that proposed techniques provide more security in real time applications.*

Keywords— ***Noise Burst, Randomness, Standard Deviation, KVM, LSAVK.***

I. INTRODUCTION

For the revolution of network, information is now distributed over a distance. Keeping this in mind, higher security of shared information can be assured if the encryption can be made by random secret keys. The practical approach Automatic Variable Key (AVK) of better security was invented by Bhunia [6-7] in the year 2006. There are many other researchers namely, Goswami [9-11], Banerjee and Dutta et.al. [8] have proposed a few more secure techniques based on the working principle of Automatic Variable Key (AVK) in terms of randomness, root mean square and standard deviation. The idea behind AVK technique can be stated as:

Let us assume, K_0 be the initial key which will be exchanged between sender and receiver in a secret mode. Subsequent keys for the data D_i to be sent will be automatically generated by $K_i = K_{i-1} \oplus D_{i-1}$

The following are the algorithms based on the principle of AVK and have been used while proposing our algorithms in this manuscript.

In case of Key Variation with Matrix (KVM) [22] the subsequent keys are generated based on the following algorithms:

Key Generate (Initial key, n, m)
{
for i = 1 to m
$K_{11} \leftarrow$ CLS (Initial Key, i)
for j= 1 to n do
for k=1 to n do
if (j==1 && k==1) then
continue
else if (k==1) then
$K_{j,k} \leftarrow$CLS $(K_{j-1,n-1},1) \oplus D_{j-1,n-1}$
else
$K_{j,k} \leftarrow$ CLS $(K_{j,k-1},1) \oplus D_{j,k-1}$
}

Where n= number of keys in square matrix and
m= number of data blocks.

In case of Left Shifting Automatic Variable Key (LSAVK) [21], the following subsequent keys have been generated based on the following algorithms:

Subsequent key K_i (i^{th} stage) is generated by both sender and receiver as follows:

$K_1' \leftarrow K_0 \oplus D_0$
$K_1 \leftarrow CLS(K_1')$
$K_2' \leftarrow K_1 \oplus D_1$
$K_2 \leftarrow CLS(K_2')$

Where K_0= Initial key and D_0= First data set

Where CLS (K_i') is circular left shift of K_0' by n bits and continue this procedure until dataset$\neq \emptyset$.

We have compared our proposed techniques namely, Key Variation with Matrix with noise burst (KVM with NB) and Left Shifting Automatic Variable Key with noise burst (LSAVK with NB) with existing techniques Key Variation with Matrix without noise burst (KVM without NB) and Left Shifting Automatic Variable Key without noise burst (LSAVK without NB) and found that the proposed techniques are more secure than the established ones.

II. *PROPOSED SCHEME*

The main purpose of our research is to enhance the security features by increasing the randomness between two successive keys.

Working principle of the proposed techniques can be stated as:

- Noise burst and initial key (K_0) will be exchanged between the communicating parties.
- Bits of noise burst will be read from left to right and reading of noise burst bit will be continued until the end of all bits of the noise burst.

Example 1: Key Variation with Matrix with noise burst (KVM with NB)

In this example, initial key K_0 = 011110001010010000111110 00100110100101010101000111011010100111100110111100 01010010100111100010001100011001110011010000010100 10110 and noise burst = 10101010010101010100110101011 01101001010110101011110110011010110111010011110101 1000101111010011011010111010100111100010010101001 with the following dataset

"*The naive approach is to announce public keys publicly, Bob can put his public key on his website or announce it in a local or national newspaper, when alice needs to send a confidential message to Bob, she can obtain Bob's public key from his site or from the newspaper, or she can even send a message to ask for it*".

Then the subsequent keys will be generated as per Key Variation with Matrix (KVM) as follows:

1st bit of noise burst is 1, so the next key will be generated as per KVM technique (equation number (1)).

K_1 = 10010000001001000011110001001101001010101010101000 11101101010011110011011110001010010100111100010001 100011001110011010000010100101100

2nd bit of noise burst is 0 so the new key will be:

K_2 = 10010000001001000011110001001101001010101010101000 11101101010011110011011110001010010100111100010001 100011001110011010000010100101100 and procedure is continued until noise burst $\neq \emptyset$.

Example 2: Left Shifting Automatic Variable Key with noise burst (LSAVK with NB)

Here, we have considered initial key K_0= 0111100010100100 00111100010011010010101010101000111011010100111100 11 00111100010011010010101010101000111011010100111100 11 01111000101001010011110001000110001100111001101000 001010010110 and data D_0= 0101010001101000011001010 0 10000001101110011000010110100101110110011001010010 00000110000101110000001110000001110010011011110110 00 01 with noise burst = 1010101001010101010101001101 0101101 10100101011010101111011001101011011101001111010110 0010111101001101101011101010011110001001010101001

Then the subsequent keys will be generated as per Left Shifting Automatic Variable Key (LSAVK) technique as per equation number (2-7):

1st bit of noise burst is 1, so the next key will be generated as follows:

K_1 = 10100101001000000000111011011101000111011001001 110000000011000011111101100101110010111111110101001 101101001101111110110101001001100 and procedure is continued until noise burst $\neq \emptyset$.

Example 3: Explanation of existing Key Variation with Matrix without noise burst (KVM without NB), Left Shifting Automatic Variable Key without noise burst (LSAVK without NB)

Let us assume that sender sends initial key K_0 = 01111000101 00100000111100010011010010101010101000111011010100111 10011011110001010010100111100010001100011001110011 01000001010010110 with data D_0 = 0101010001101000011 0 01010010000000110111001100001011010010111011001100 1 01001000000110000101110000001110000001110010011011 11 01100001. The new key will be as per Key Variation with Matrix (KVM) technique:

K_1 = 1001000000011100000010000111111110111010100101 00100000101100010000110010100011011110111110010000 1 0011010011011110101110111010 00011

In case of Left Shifting Automatic Variable Key (LSAVK) technique, the key will be generated as follows:

K_1 = 10000110110000100101111001110011101010011110 1 01100101010101100101000011011010101100100000100101 1110011100111010100111101011 00101

K_2 = 01011001111101101001001110100100101100000100 10 11011010011000101000011000010010110110100110001010 0011000100001011001111101100 01000

III. PERFORMANCE ANALYSIS

For performance analysis of the proposed techniques, we have assumed initial key as K_0 = 01111000101001000011 11000100110100101010101010001110110101001111001 10 11110001010010100111100010001100011001110011010 10 00001010010110 and noise burst =10101010010101010101 00110101011011010010101101010111101100110101101 11010011110101100010111101001101101011101010011 1100010010101001 with following dataset

Dataset = "*The naive approach is to announce public keys publicly, Bob can put his public key on his website or announce it in a local or national newspaper, when alice needs to send a confidential message to Bob, she can obtain Bob's public key from his site or from the newspaper, or she can even send a message to ask for it".*

We have calculated the standard deviation, randomness and average randomness by using same initial key with noise burst and data set pairs which have been depicted from Figure 1 to 3. For analysis, we have assumed randomness which is a parameter. Randomness is a measure of amount of variation occurred between two successive keys. For example if K_i= 10101011111011 and K_{i+1}= 00111010101100 then the randomness between K_i and K_{i+1} is 7. When we apply noise burst to the existing algorithms, more productive and superior results are obtained.

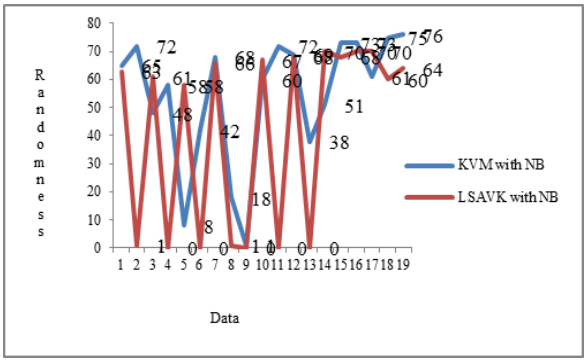

Figure 1: Randomness of keys of KVM with NB, LSAVK with NB

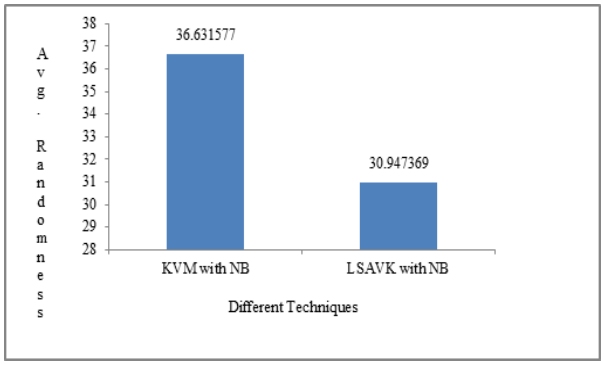

Figure 2: Average Randomness of KVM with NB, LSAVK with NB

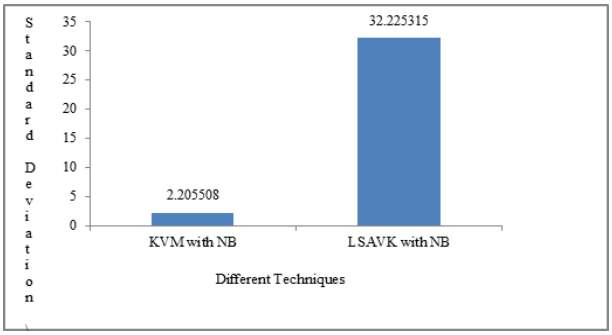

Figure 3: Standard Deviation of KVM with NB, LSAVK with NB

IV. COMPARISON

In this section, we have compared the standard deviation and average randomness of Key Variation with Matrix with noise burst (KVM with NB), Key Variation with Matrix without noise burst (KVM without NB), Left Shifting Automatic Variable Key with noise burst (LSAVK with NB), Left Shifting Automatic Variable Key without noise burst (LSAVK without NB). The comparison among the schemes has been depicted in Figure 4 and 5 in terms of average randomness and standard deviation respectively.

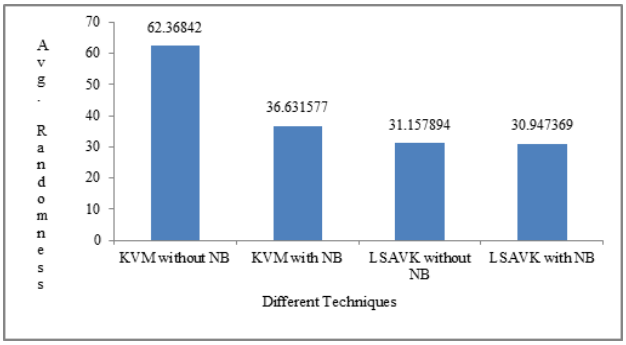

Figure 4: Comparison of Average Randomness of KVM without NB, KVM with NB, LSAVK without NB and LSAVK with NB

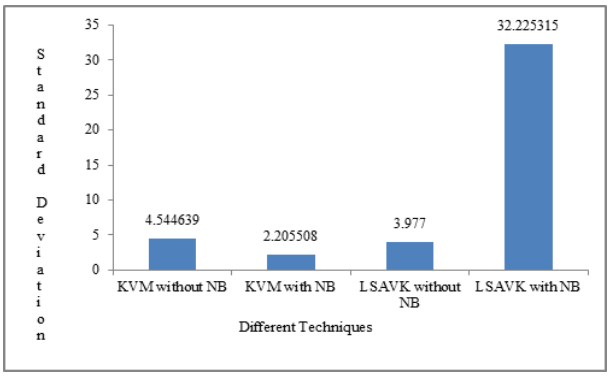

Figure 5: Comparison of Standard Deviation of KVM without NB, KVM with NB, LSAVK without NB and LSAVK with NB

The following observations may be drawn by analyzing the graph of standard deviation & average randomness. From Figure 4, we have found that the average randomness of Key Variation with Matrix with noise burst (KVM with NB) is the maximum than other techniques used for comparison. However, standard deviation of Left Shifting Automatic Variable Key with noise burst (LSAVK with NB) is the highest in Figure 5. Therefore, from the experiments, we have found that the superiority of different techniques may vary from one session to another session.

Here we have also compared these proposed techniques with the standard cryptographic algorithm with RC_4 with the same initial key with same dataset and with similar noise burst and the graphs have been depicted in figure 6 and 7.

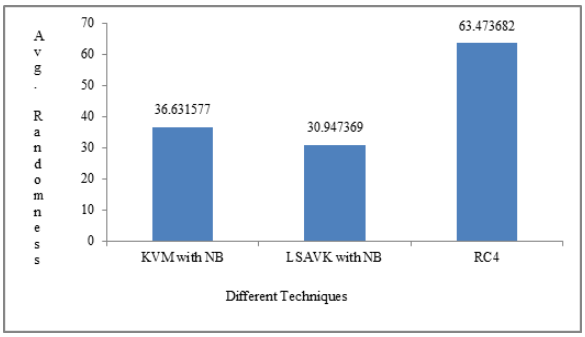

Figure 6: Comparison of Average Randomness of Proposed Techniques (KVM with NB, LSAVK with NB) with RC_4

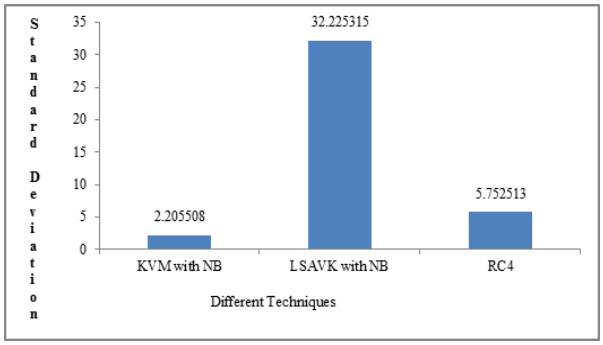

Figure 7: Comparison of Standard Deviation of Proposed Techniques KVM with NB, LSAVK with NB with RC_4

V. RANDOMNESS VERIFICATION

Verification of the randomness among the successive keys, generated by all the experiments defined in the previous section, has been done with the help of National Institute of Standards and Technology (NIST) test suite. NIST test suite is a statistical package containing 15 tests to determine whether a random key generator is suitable for a particular cryptographic application or not. We have examined the randomness of our successive keys based on the following 4 different statistical tests only.

i) Frequency Test
ii) Block Frequency Test
iii) Cumulative Tests
iv) Runs Test

Each test is based on a calculated test statistic value, which is a function of data. If the test statistic value is S and the critical value is t, then the error probability is P (S > t || H_0 is true) = P (reject H_0 | H_0 is true). Another type of error probability is P (S <= t|| H_0 is false) = P (accept H_0 | H_0 is false), here H_0= null hypothesis. The test statistic is used to calculate a p-value that summarizes the strength of the evidence against the null hypothesis. For these tests, each p-value is the probability that a perfect random number generator would have produced a sequence less random than the sequence that was tested, given the kind of non–randomness assesses by the test. If a p-value for a test is equal to 1, then the sequence appears to be perfectly random whereas p-value of zero indicates that the sequence appears to be completely non-random. If the p-value is < 0.01 then it can be inferred that the sequence in non-random otherwise, the sequence is random. The p-values of our experiments have been summarized in Table I:

Table I: Statistical test results of KVM with NB and LSAVK with NB

Techniques	Test	p-value	Remarks
KVM with NB	Frequency Test (FT)	0.290478	Random
	Block frequency Test (BFT)	0.290478	Random
	Cumulative Sum(Forward) (CSF)	0.052938	Random
	Cumulative Sums(Backward) (CSB)	0.037956	Random
	Runs Test (RT)	0.086848	Random
LSAVK with NB	Frequency Test (FT)	0.495779	Random
	Block frequency Test (BFT)	0.495779	Random
	Cumulative Sum(Forward) (CSF)	0.537254	Random
	Cumulative Sums(Backward) (CSB)	0.339879	Random
	Runs Test (RT)	0.129346	Random

VI. CONCLUSION

In this manuscript, after analyzing the experiments, it is found that when we use standard deviation as parameter for comparison then Left Shifting Automatic Variable Key with noise burst (LSAVK with NB) for same dataset is superior to other compared techniques. If we consider average randomness for comparison, Key Variation with Matrix with noise burst (KVM with NB) is superior to other compared techniques. When we have compared these proposed techniques with algorithm RC_4 then we have seen that the technique Left Shifting Automatic Variable Key with noise burst (LSAVK with NB) is more superior in case of standard deviation. The superior results of Key Variation with Matrix with noise burst (KVM with NB), Left Shifting Automatic Variable Key with noise burst (LSAVK with NB) suggest that the new techniques can be applied with standard cryptographic algorithms for encryption and decryption there by increasing the level of security of real time applications.

References

[1] C E Shannon, “Communication Theory of Secrecy System”, the Bell System Tech J, **1949.**

[2] C E Shannon, "A Mathematical Theory of Communication", Bell System Tech J, 27, 379-423, 623-656, **1948**.

[3] M. Diffie, E. Hellman, "Exhaustive Cryptanalysis of the no of bits Data Encryption Standard", Computer, pp.74-84, **1977**.

[4] FIPS 140-1, Security Requirements for Cryptographic Modules, Federal Information Processing standards Publication140-1.U.S, department of Commerce /NIST, National Technical Information science, Springfield ,VA, **1994**.

[5] Rukin A, Soto J, Nechvatal J, Smid M, Barker E, Leigh S, Levenson M, Vangel M, Banks D, Heckert A, Dray J & Vo S, A statistical test suite

for random and pseudorandom number generators for cryptographic applications(NIST special publication) **2010**.

[6] C. T. Bhunia, "New Approach for Selective AES towards Tackling Error Propagation Effect of AE", ASIAN Journal of Information Technology, volume 5990, pp.1017-1022, **2006**.

[7] C. T. Bhunia, "Implementation of AVK with Chaos Theory and Studied Thereof", J IUP Computer Science volume V, No 4, pp.22-32, **2011.**

[8] M. P. Dutta, S. Banerjee, C .T. Bhunia, "Two New Schemes to Generate Automatic Variable Key to Achieve the Perfect Security in Insecure Communication Channel", In preceding of the International Conference on Advanced Research in Computer Science Engineering &Technology (ICARCSET, Eluru, India), **2015**.

[9] Rajat Subhra Goswami, Swarnendu Chakraborty, C. T. Bhunia, Abhinandan Bhunia, "New Approach towards Generation of Automatic Variable Key to Achieve Perfect Security", ITNG, IEEE Computer Society, CPS, USA, Las Vegas, pp.489-491, **2013**.

[10] Rajat Subhra Goswami, Swarnendu Chakraborty, C. T. Bhunia, Abhinandan Bhunia, "Generation of Automatic Variable Key under Various Approaches in Cryptography System", J. Institute Engineering, India Ser. B, 94, 4,215-220, **2014**.

[11] Rajat Subhra Goswami, Swarnendu Chakraborty, Abhinandan Bhunia, C. T. Bhunia, "New Techniques for Generating of Automatic Variable Key in Achieving Perfect Security", J. Institute Engineering, India Ser. B, 95, 3, 197-201, **2014**.

[12] S. Goswami, S. Misra, M. Mukesh, "A PKI Based Time Stamped Secure Signing Tool for e-Documents", Proceedings of 2014 International Conference on High Performance Computing and Applications (ICHPCA), Bhubaneswar, December 22-24, **2014**.

[13] S. Goswami, S. Misra, M. Mukesh, "A replay attach resilient system for PKI based authentication in challenge-response mode for online application", Proceedings of the 3rd International Conference on Echo-friendly Computing and Communication Systems (ICECCS), Surathkal, Mangalore, India, December 18-21, **2014**.

[14] S. Misra, S. Goswami, C. Taneja, A. Mukherjee, M. S. Obaidat, "A PKI Adapted Model for Secure Information Dissemination in Industrial Control and Automation 6LoWPANs", IEEE Access Journal, Volume 3, pp. 875-889, **2015**.

[15] S. Misra, S. Goswami, G. P. Pathak and N. Shah, "Efficient Detection of Public Key Infrastructure-Based Revoked Keys in Mobile Ad Hoc Networks", Wireless Communications and Mobile Computing (Willey), Volume 11, No 2, pp. 146-162, February, **2011**.

[16] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST Special Publication 800-22, April **2010**.

[17] L. Lamport, "Password authentication with insecure communication", Commun of the ACM, Volume 24, 11, pp. 770-772, **1981**.

[18] M. S. Hwang, and L. H. Li, "A new remote user authentication scheme using smart cards", IEEE T Consum Electr, Volume 46, 1, pp. 28-30, **2000**.

[19] C. W. Lin, C. S. Tsai, and M. S. Hwang, "A new strong password authentication scheme using one-way Hash functions", J Comput Sys Sc Int+, Volume 45, 4, pp. 623-626, **2006.**

[20] M. Das, R. S. Goswami, C. T. Bhunia, "Implementation of New Method to Generate a Key in Automatic Variable Key for Perfect Security", International Journal of Security and Its Applications, Volume 10, No 4, pp. 367-376, **2016.**

[21] M. Das, P. Roy, R. S. Goswami, C. T. Bhunia, "Investigation a New Technique of Automatic Variable Key Using Two Dimensional Matrix Approach to Achieve Perfect Security", International Journal of Communication Networks & Distributed Systems, Vol. 20, No. 2, pp. 214-225, **2018.**

[22] M. Das, R. S. Goswami, M. P. Dutta, S. K. Chakraborty, C. T. Bhunia, "Technique to Generate Variable Keys with Key Variation with Noise Burst Bit for Achieving perfect Security in Cryptology towards Optimum Data Transfer", International Journal of Security and Its Applications, Volume 11, No 3, pp. 39-50, **2017**.

[23] M. Das, R.S. Goswami, M. P. Dutta, S. K. Chakraborty, C. T. Bhunia, "Methods to Generate Variable Keys with Noise Burst Bit in Modern Cryptosystem for Achieving Perfect Security", 4th International Conference on Image Information Processing (ICIIP 2017) , pp.1-6, DOI**:** 10.1109/ICIIP.2017.8313695, **2017**.