International Journal of Advances in Computer Science & Its Applications
Volume 6 : Issue 1 *[ISSN 2250-3765]*
Publication Date : 18 April, 2016

Generation of Variable Session Keys Based on Piggybacking Strategy

Manash Pratim Dutta, Subhasish Banerjee, C. T. Bhunia

***Abstract*— Since the dawn of computer networks, protecting information from unauthorized users becomes like a battle field for the researchers and the attackers. Whenever any new solutions have been designed by the researchers to achieve the confidentiality and integrity towards the shared information, a new problem is always arisen by the attackers who are always ready to find out the loopholes. One of the solutions is to achieve and make difficult for the attacker by changing the keys frequently during the message transmission. In this regard, Automatic Variable Key (AVK) is an alternative approach to fulfill the requirements of such key variations. Therefore, in this article we have analyzed such approaches and given the contributions by proposing a new method to generate the keys which can enhance the security issues by increasing the randomness among the set of auto generated keys.**

***Keywords*— AVK, randomness, security, session keys**

I. Introduction

As such computer networks are expanding in exponential order; therefore, it becomes an indispensable part of human life which is used to fulfill all their daily requirements such as e-banking, online shopping, e-trading etc.. Hence, maintaining confidentiality of such shared information becomes an emerging arena of research among the researchers. From the last few decades, many schemes [1-6] have been designed to exchange the information secretly between the authorized entities. But, keeping the keys secret from the attackers is one of the most difficult problems in practical scenario. Whenever none of the attempts goes right in favor of the attackers and almost become tired to search all possible prospects to break the confidentiality then brute force attack may remain as the last hope and most of times get success even. To tackle such problems, one of the vital solutions is to make the key long enough so that attacker cannot try all possible combinations. Due to computing process is not limited anymore; assuring such method may not be further sustainable. In this regard, a famous scientist namely, Vernum [7-10] proposed that difficulty can be added in breaking the long keys if the key changes from session to session or time to time. Therefore, in the year 2006, Bhunia [11-13] introduced the concept of time variant key generation technique which makes the key variable in nature by demonstrating the AVK mechanism. As per the literature survey, the AVK is one of the novel and simplest approaches to achieve the important security requirements such as confidentiality and integrity. After forth, many researchers namely, Chakraborty et al. [14], Goswami et al. [15 - 19], Banerjee et al. [20 - 22] and Dutta et al. [23] have given the contributions in this era and brought many new methods to generate the AVKs to enhance the security than previous existing ones. In this article, we have analyzed the security factors of the existing schemes and proposed a new approach to generate the AVKs based on piggybacking strategy namely, AVKPS. The rest of the article is organized as follows: the proposed scheme has been illustrated in section II, followed by key generation examples in section III. Result analysis of the proposed scheme has been shown in section IV and section V contains the performance comparison of our scheme with the existing schemes. Lastly, we have concluded our paper in section VI.

Manash Pratim Dutta
National Institute of Technology, Arunachal Pradesh
India
manashpdutta@gmail.com

Subhasish Banerjee
National Institute of Technology, Arunachal Pradesh
India
subhasishism@gmail.com

C. T. Bhunia
National Institute of Technology, Arunachal Pradesh,
India
ctbhunia@vsnl.com

II. Proposed scheme

In this section, we have proposed our new approach, namely AVKPS to generate the keys for secure data transmission. The following algorithm defines the key generation procedure after establishing the initial key between the sender and receiver. In this scheme, a new random number of bits size $\log_2 n$ is always used to append with each block of message to generate the next key where, n is the size of the key. The complete description of our proposed scheme has been defined below and the graphical representation of the entire method is plotted in Figure 1.

$Key\_Generator\ (Initial\ key\ of\ n\ bits)$
{
$K_1 \leftarrow Initial\ Key\ of\ n\ bits$
$R \leftarrow rand()\%n$
$i \leftarrow 1$
$While\ (Data\ blocks! = \emptyset)$
{
$C_i \leftarrow E_{K_i}(D_i, R)$
$i \leftarrow i + 1$
$K_i \leftarrow (R||D_{i-1}) \oplus CLS(K_{i-1}, R)$
$R \leftarrow rand()\%n$
}
}

Where:
$R \leftarrow$ Auto generated random number of bit size $\log_2 n$
$D_i \leftarrow$ i[th] block of data with block size $n - \log_2 n$
$CLS(x, y) \leftarrow$ Circular left shift of x by y bits position
$C_i \leftarrow$ i[th] block of cipher text
$E \leftarrow$ Encryption mechanism

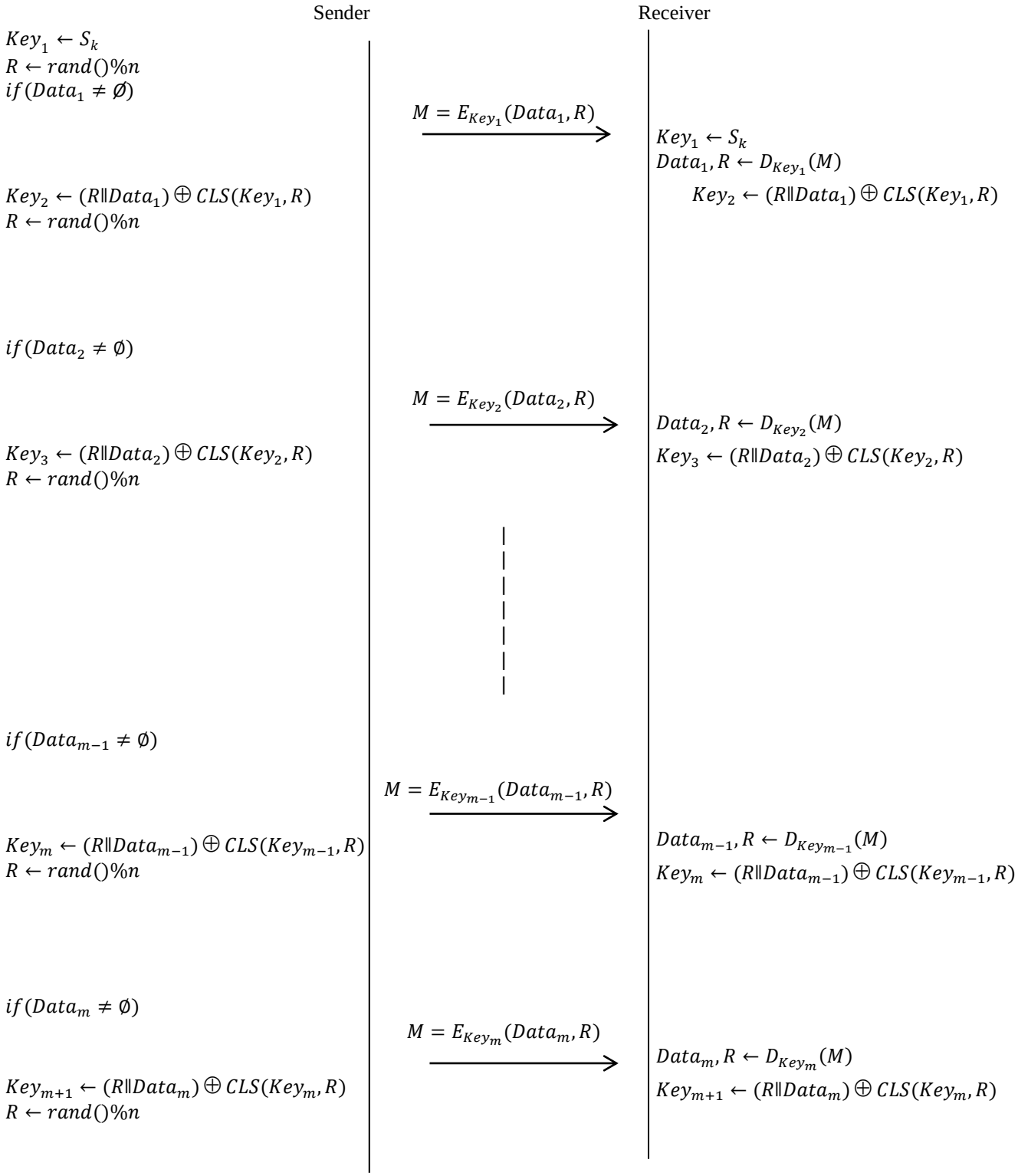

Figure 1. Key generation procedure

III. Key Generation Examples

Here, we have demonstrated the above AVKPS procedure to generate the successive keys based on data set and negotiated initial key between the sender and receiver. For simplicity, we have considered the key size of 8 bits (i.e. n) and the data set as "11000111" and "PLAIN" respectively. The binary sequence of the data set = "01010000010011000100100101000001010011 10" and bit size of the random number, $R = \log_2 n = \log_2 8 = 3$.

Therefore, the block size of the data will be $n - \log_2 n = 8 - 3 = 5$. If the last block of data is not multiple of 5 then extra bits will be appended as parity bits which will be discarded by the receiver. Hence, the 1st block of data, D_1 = 01010, 2nd block of data, D_2 = 00001 and so on.

First key, K_1=11000111 and assume the auto generated random number R= $\text{rand}()\%n = 2$. Therefore, generation of 2nd key, K_2 will be$(R||D_1) \oplus CLS(K_1, R) = 2||01010 \oplus CLS(11000111,2) = 01001010 \oplus 00011111 = 01010101$.

For the third Key K_3, assume that the auto generated random number R = $\text{rand}()\%n = 4$. Hence, 3rd key $K_3 = (R||D_2) \oplus CLS(K_2, R) = 4||00001 \oplus CLS(01001101, 4) = 10001010 \oplus 11010100 = 11011110$.

Similarly, if we assume that the auto generated random number R= 5 then, the next key will be computed as $(R||D_3) \oplus CLS(K_3, R) = 5||00110 \oplus CLS(10000000, 5) = 10100110 \oplus 00010000 = 10110110$.

Similarly, the rest of the keys are generated as per the availability of the data set and/or necessity.

IV. Experimental Results

In this part, we have carried out some experiments of our scheme with some real set of data. Here, we have taken the total length of each key as 8 bits only and the block size of individual data set is also restricted to the same size. Where, first 3 bits has been appended as a random number and rest bits are meant for actual message. We have assumed the initial establish key K_0 as 10111011 to perform all the following experiments 1 to 3. To make the experimental result easier to understand, only first 86 auto generated keys are used to define the randomness.

Experiment 1: In this experiment, we have used "*A brute-force attack involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained.*" as a data set. The computed value of randomness among the auto generated successive keys is shown in Figure 2.

Experiment 2: "*Frequency analysis is based on the fact that, in any given stretch of written language, certain letters and combinations of letters occur with varying frequencies.*" is considered as the data set for this experiment. The experimental result for randomness is shown in Figure 3.

Experiment 3: The following data set is considered for this experiment and the corresponding generated graph is shown in Figure 3.
"*An encryption scheme is said to be computationally secure if either of the foregoing two criteria are met*."

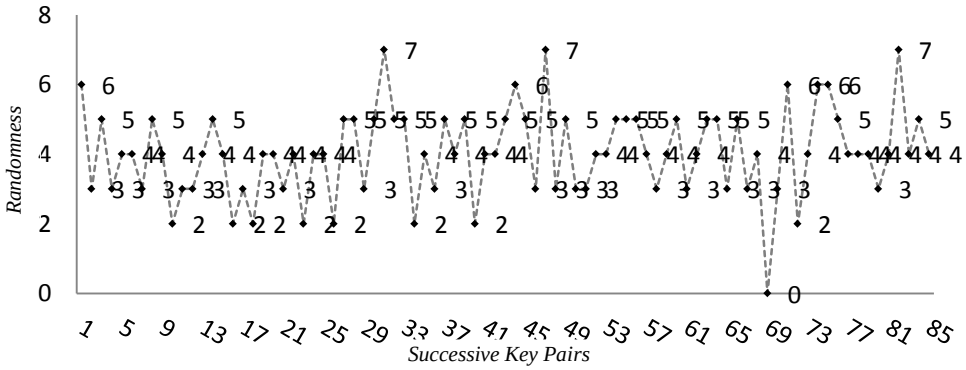

Figure 2. Randomness among the successive keys for the experiment 1

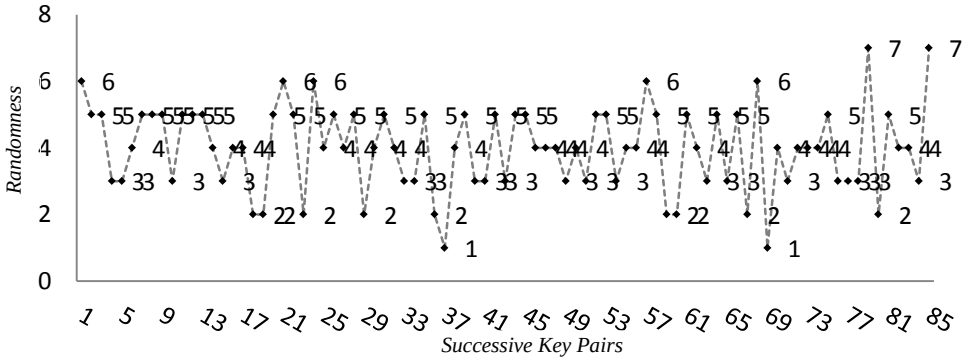

Figure 3. Randomness among the successive keys for the experiment 2

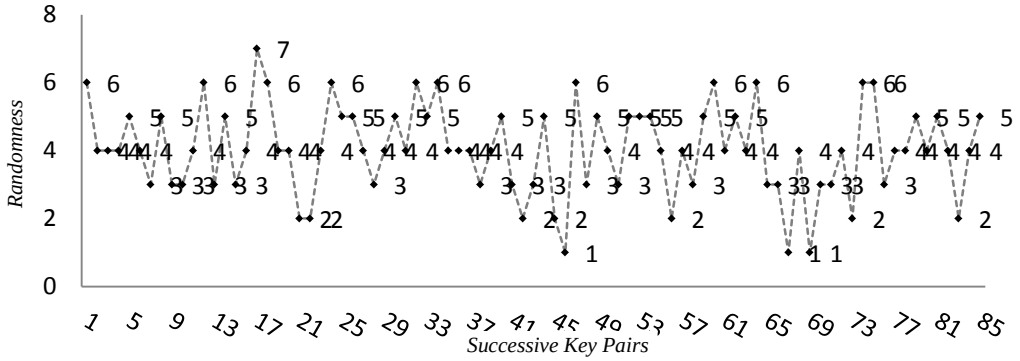

Figure 4. Randomness among the successive keys for the experiment 3

v. Performance Analysis

In this section, we have summarized the effectiveness of our proposed scheme by comparing the average randomness with that of existing related schemes. We have used the same method to compute the average randomness as it is described in the compared schemes. As the generation of keys always depends on initial key and the data set pair, we have taken all the above experiments 1 to 3 into our account for comparison purpose and their corresponding results are depicted from Figure 5 to 7 respectively. The x axis in the graphs indicates the techniques considered for experimental study where as y axis represents the average randomness.

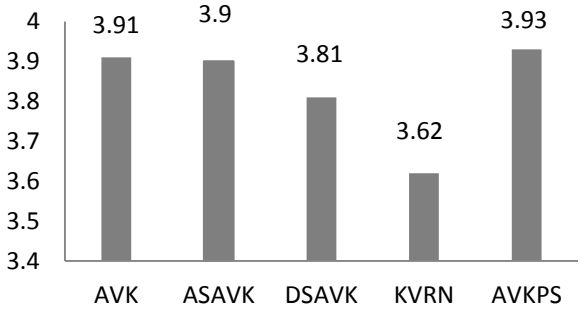

Figure 5: Average randomness comparison of experiment 1

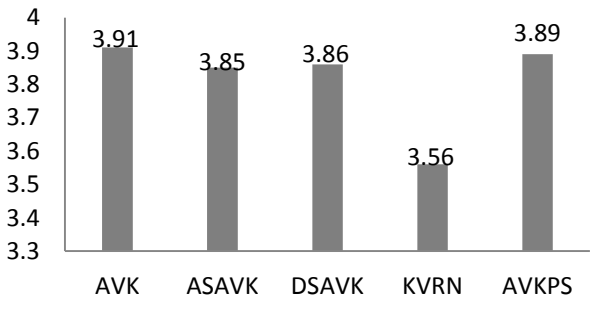

Figure 6: Average randomness comparison of experiment 2

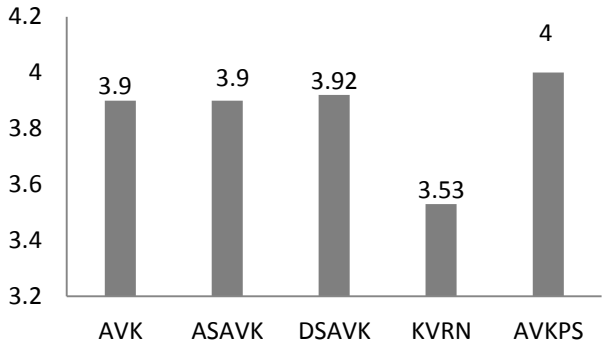

Figure 7: Average randomness comparison of experiment 3

vi. Conclusion

In this article, we have proposed a new and effective key generation procedure to generate the variable session keys to fulfill the essential requirements of the cryptosystem. To prove the effectiveness, we have compared our scheme with the other related schemes. From the comparison graphs depicted in performance analysis section, we can conclude that the new scheme is superior to other schemes in terms of average randomness among the auto generated keys.

References

[1] L. Lamport, "Password authentication with insecure communication," communication of the ACM, vol. 24, 11, pp. 770-772, 1981.

[2] M. S. Hwang, and L. H. Li, "A new remote user authentication scheme using smart cards," IEEE Transaction on Consumer Electronics, vol. 46, 1, pp. 28-30, 2000.

[3] C. W. Lin, C. S. Tsai, and M. S. Hwang, "A new strong password authentication scheme using one-way Hash functions," Journal of Computer and Systems Sciences International, vol. 45, 4, pp. 623-626, 2006.

[4] K. C. Baruah, S. Banerjee, M. P. Dutta, and C. T. Bhunia, "An Improved Biometric-based Multi server Authentication Scheme using Smart Card," International Journal of Security and Its Application, vol. 9, 1, pp. 397-408, 2015.

[5] S. Banerjee, M. P. Dutta, and C. T. Bhunia, "Cryptanalysis and Security Enhancement of an Efficient and Secure Dynamic ID Based Remote User Authentication Scheme for Multi-Server Environments," Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET 2015), March 6-7; Eluru, India, 2015.

[6] S. Banerjee, M. P. Dutta, and C. T. Bhunia, "An Improved Smart Card based Anonymous Multi-Server Remote User Authentication Scheme," Internation Journal of Smart Home, vol. 9, 5, pp. 11-22, 2015.

[7] M. Diffe, and E. Hellman, "Exhaustive cryptanalysis of the nbs data encryption standard," computer, pp. 74-84, 1977.

[8] E. Biham, "A fast new DES implementation in software. In Proeedings of the Intentional," Symposium on Foundations of Software Engineering, pp. 260-273, 1997.

[9] H. Eberle, "A high speed des implementation for network application," In Proceedings of the International Conference on Cryptology, pp. 521-539, 1992..

[10] B. Schneir, "Applied cryptography," 2nd edn. John Willey & Sons Inc., New York, 1996.

[11] C. T. Bhunia, "New approaches for selective aes towards tackling error propagation effect of AES," Asian J. Inf. Tech, vol. 5, 9, pp. 1017-1022, 2006.

[12] C. T. Bhunia, "Application of AVK and selective encryption in improving performance of quantum cryptography and networks," http://www.Ictp.it/~pub_off, IC/2006/045.

[13] C. T. Bhunia, G. Mondal, and S. Samaddar, "Theory and application of time variant key in RSA and that with selective encryption in AES," In Proceedings of EAIT (Elsevier Publications, Calcutta CSI), pp. 219-221, 2006.

[14] P. Chakarabarti, B. Bhuyan, A, Chowdhuri, and C. T. Bhunia, "A novel approach towards realizing optimum data transfer and automatic variable key (AVK) in cryptography," Int. J. Comput. Sci. Netw. Secur, vol. 8, 5, pp. 241-250, 2008.

[15] C. T. Bhunia, S. K. Chakraborty, and R. S. Goswami, "A new technique (CSAVK) of automatic variable key in achieving perfect security," 100th Indian Science Congress Association, 2013.

[16] R. S. Goswami, S. K. Chakraborty, A. Bhunia, and C. T. Bhunia, "New techniques for generating of automatic variable key in achieving perfect security," J. Inst. Eng. India Ser. B. vol. 95, 3, pp. 197-201, 2014.

[17] R. S. Goswami, S. K. Chakraborty, A. Bhunia, and C. T. Bhunia, "New approaches towards generation of automatic variable key to achieve perfect security," In Proceedings of the 10th International Conference on Information Technology, IEEE Computer Society, pp. 489-491, 2013.

[18] R. S. Goswami, S. K. Chakraborty, A. Bhunia, and C. T. Bhunia, "Generation of automatic variable key under various approaches in cryptography system," J. Inst. Eng. India Ser. B, vol. 94, 4, pp. 215-220, 2014.

[19] R. S. Goswami, S. K. Chakraborty, A. Bhunia, and C. T. Bhunia, "Various new methods of implementing AVK," In Proceedings of the 2nd International Conference Advanced Computer Science and Engineering, pp. 149-152, 2013.

[20] S. Banerjee, M. P. Dutta, and C. T. Bhunia, "A novel approach to achieve the perfect security through avk over insecure communication channel," J. Inst. Eng. India Ser. B (Communicated).

[21] S. Banerjee, M. P. Dutta, and C. T. Bhunia, "A New three dimensional based key generation technique in AVK," J. Inst. Eng. India Ser. B (Communicated).

[22] B. K. Singh, S. Banerjee, M. P. Dutta, and C. T. Bhunia, "Generation of automatic variable key to make secure communication," In Proceedings of the International Conference on Recent Cognizance Wireless Communication & Image Processing (ICRCWIP-2014), 2015.

[23] M. P. Dutta, S. Banerjee, and C. T. Bhunia, "Two new schemes to generate automatic variable key (avk) to achieve the perfect security in insecure communication channel," In Proceedings of the International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET, Eluru, India), 2015. DOI= http://dx.doi.org/10.1145/2743065.2743080.

About Author (s):

Manash Pratim Dutta received his M.Tech degree in Information Technology from Sikkim Manipal University, Sikkim, India in 2012. Currently, he is working as Assistent Professor and persuing his Ph.D in the Department of Computer Science and Engineering in National Institute of Technology, Arunachal Pradesh. His research activities are mainly focused on crytography and infornation secutity.

Subhasish Banerjee received his M.Tech degree in Computer Application from Indian School of Mines, Dhanbad, India in 2012. Currently he is persuing his Ph.D and also working as Assistent Professor in the Department of Computer Science and Engineering in National Institute of Technology, Arunachal Pradesh. His research activities are mainly focused on crytography and infornation secutity.

Prof. Chandan Tilak Bhunia did his B. Tech. in Radio physics and Electronics in 1983 from Calcutta University. He received his M. Tech. in Radio physics and Electronics in 1985 and then joined North Bengal University as a lecturer of Computer Science & Applications in 1988. He became Assistant Professor of ECE at NERIST, Govt. of India in 1990. He got P. hd. in Computer Science & Engineering from Jadavpur University. He became a full Professor in 1997 at NERIST. Currently, he is working as a Director of National Institute of Technology, Arunachal Pradesh. He has published around 150 research papers in various national and internatiol journals of repute. Under his supervision, five P. hd. scholars got awarded and nine scholars are currently working in various fields.