International Journal of Security and Its Applications
Vol.9, No.10 (2015), pp.147-154
http://dx.doi.org/10.14257/ijsia.2015.9.10.13

An Approach to Generate 2-Dimensional AVK to Enhance Security of Shared Information

Manash Pratim Dutta[1]*, Subhasish Banerjee[2]* and C. T. Bhunia[3]*

[*]*Department of Computer Science & Engineering, National Institute of Technology, Arunachal Pradesh, India*
manash.cse@nitap.in[1], subhasish.cse@nitap.in[2], ctbhunia@vsnl.com[3]

Abstract

As the sharing of information through the communication channels increases, the indispensability of maintaining confidentiality of those shared information also increases proportionally. Providing reasonable security over the insecure channel is a challenging research. Due to the advancement of computational efficiency, confidentiality of the information cannot be assured with the help of a static key. Keeping this in mind, many researchers have proposed several time variant key generation techniques, out of which Automatic Variable Key (AVK) is a novel approach. In conventional AVK and in different variations of AVK; the key varies every time as new data is exchanged between sender and receiver while the key size remains constant throughout the data communication. Therefore, to increase the randomness among the successive keys that is the key for ensuring the greater security, we have proposed a 2-dimensional AVK in which the auto generated keys not only vary in bits sequence (i.e. session by session) but also in size.

Keywords: *AVK, Security, Size-variant key, Time-variant key*

1. Introduction

From the last few decades, a great amount of research has been carried out to secure the shared data from various well known attacks. The important criterion in all such proposed techniques is that neither the key will be disclosed nor it can be computed by any adversary means. One solution is to prevent the keys from cipher text only attack (brute force attack, frequency attack, etc.); make the keys larger enough so that the attacker cannot try all such possible combinations in linear polynomial time. Due to the advancement of technology and computational speedup, such mechanism is about to become obsolete. Meanwhile, in 1949, Shannon [1, 2], 'the father of information theory', addressed the theory of perfect secrecy. According to this, a crypto system should possess the characteristics-if the key can be made variable in nature and if its size is as same as that of the plain text then the attacker would not be able to break the code by guessing the keys successfully. Later, Vernum [3-6] added that the generated key would be difficult to break if it would change from session to session or time to time during data communication. In this regard, Bhunia [7-9] introduced the idea of AVK. In AVK, a new key is generated every time whenever a new data is exchanged. After forth, many researchers namely, Chakarboty et al. [10], Goswami et al. [11-15], Banerjee et al. [16-18] and Dutta et al. [19-22] stretches this idea and proposed some modified techniques in AVK. However, in most of the proposed techniques, only the auto generated keys may vary in bits sequences while the size of the key remains constant. To enhance the randomness among the auto generated keys and to increase the level of security, we have proposed a 2-dimensional AVK with random number (2DAVKRN) where the keys not only vary in bit sequences but also in size as well. The rest of the paper is organized as follows. The enhanced technique of AVK is described in section 2, followed by examples to generate the keys in section 3. To show the efficiency of our algorithm, the randomness

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2015 SERSC

among successive keys has been defined through various experiments in section 4. In section 5, we have compared our scheme with the other related schemes and named as performance analysis. Finally, the paper has been concluded in section 6.

2. Proposed Technique

In this section, we have proposed our scheme "2DAVKRN" to generate the automatic variable keys. In the algorithm, the key generator generates the keys after establishment of initial key and a random number between the sender and receiver. The algorithm has been defined below:

```
Key Generator (Initial key of n bits, Random Number)
{
K1 ←Initial Key of n bits
R ← Random Number
i ← 2
do
{
      if ( keysize==2n)
        Ikey ←CBOX(key_{i-1})
      else
         Ikey ← key_{i-1}
       if ( Number of set bits in R == even)
            {
                  key_i ← EBOX(R, Ikey)
                    R ← R ⊕ Data_{i-1}
            }
      else

            {
                  key_i ← Ikey ⊕ Data_{i-1}
                  R ← R ⊕ Ikey
               }
             i++
     } while (Data blocks !=∅ )
}
```

Where:

```
CBOX (key_{i-1})
{
  for i =0 to n/2 -1
 Ikey = key_{i-1}[i] ⊕ key_{i-1}[n-i]
 return (Ikey)
}

EBOX (R, Ikey)
{
for i=0 and j=0 to i<n and j<n/2
  do
          key[i] = Ikey[j]
          key[i+1] = R[j]
         i=i+2
         j++
```

 Copyright ⓒ 2015 SERSC

done
return (*key*)
}

3. Examples of key Generation

Let us assume that 8 bit initial key (K_1) is 10001010 and a random number (R) is 00010010, which are exchanged between sender and receiver. Moreover, 8 bit initial data (D_1) is considered as 10101010 for this example. The successive steps to produce the auto generated keys are summarized as below.

Step 1. As the number of set bits in R is even, the 2nd key (K_2) will be expanded and therefore, K_2 = 0100001001001100 and the random number (R) will be updated by 00010010⊕ 10101010=10111000.

Step 2. To compute 3rd key, we assume that previous dataset D_2 is 01000011, as K_2 is a 16 bit key therefore, CBOX produces 8 bit intermediate key (Ikey) = 01110000. As the number of set bits in R is even, the next key, K_3 = 1001111110000000 and random number R will be updated by 0111000⊕ 01000011= 11111011.

Step 3. In this case, D_3 is assumed as 11100101. Now, to compute K_4, 16 bit K_3 is converted to 8 bit Ikey, 10011110 by CBOX. Since the number of set bits in R is odd, therefore, next generated key K_4=10011110⊕ 11100101=01111011 and the new value of R will be 11111011⊕ 10011110=01100101.

Similarly, the rest of the keys are generated as per the availability of the data set.

4. Experimental Results

In this section, we have defined various experiments to show the efficiency of our proposed scheme. For the experimental purpose, we have assumed that the length of all the individual datasets is 8 bits. To make our experiments simpler, we have restricted the size of both initial key and negotiated random number to 8 bit each. In all the following experiments, we have assumed that initial key (K_1) and random number (R) are 10001010 and 00010010, respectively. While plotting the graph, we have considered the first 86 keys only.

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 1.

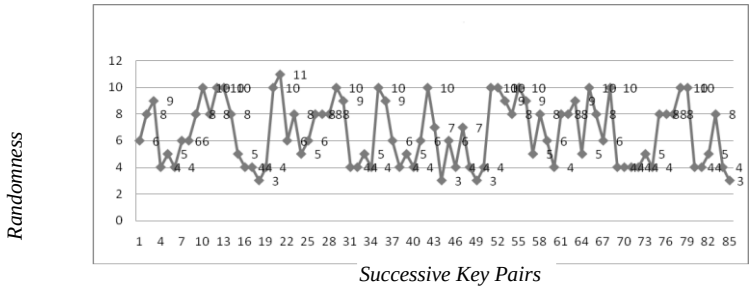

Figure 1. Randomness among the Successive Keys

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 2.

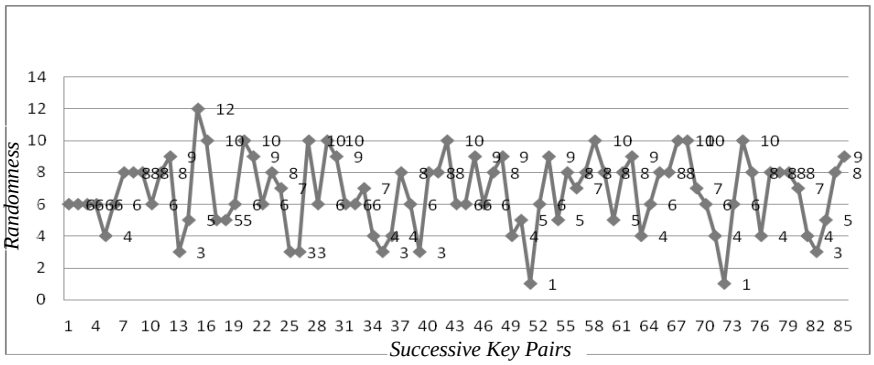

Figure 2: Randomness among the Successive Keys

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.*"

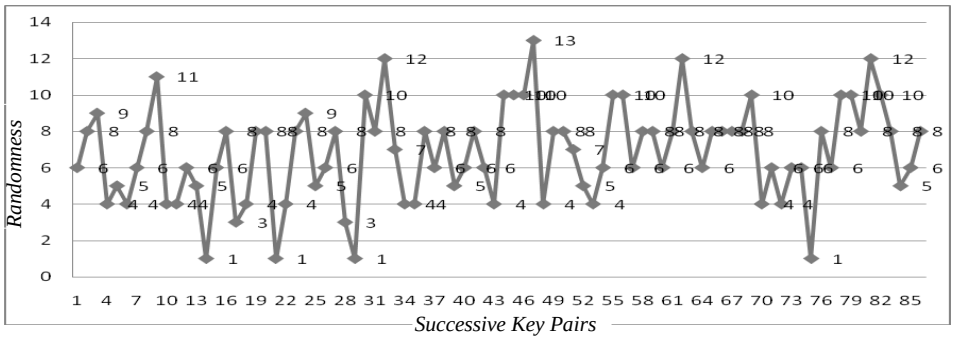

Figure 3. Randomness among the Successive Keys

5. Performance Analysis

In this section, we have proved the efficiency of our technique by comparing it with the related techniques in terms of average randomness. Average randomness is computed in the same way as performed for the previous existing techniques. We have compared resultant average randomness of our proposed scheme with the other techniques for all the mentioned experiments 1 to 3 and comparisons are given from Figure 4 to 6 respectively. The x axis in the graphs indicates the techniques considered for experimental study where as y axis represents the average randomness of those schemes.

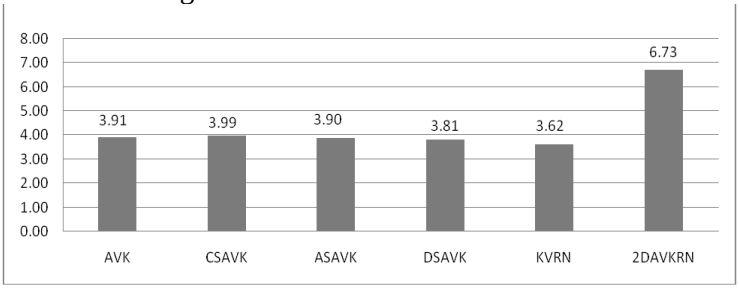

Figure 4. Average Randomness Comparison of Experiment 1

 Copyright ⓒ 2015 SERSC

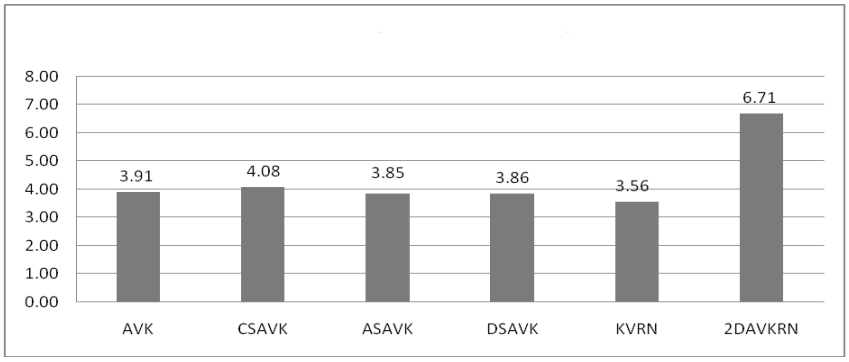

Figure 5. Average Randomness Comparison of Experiment 2

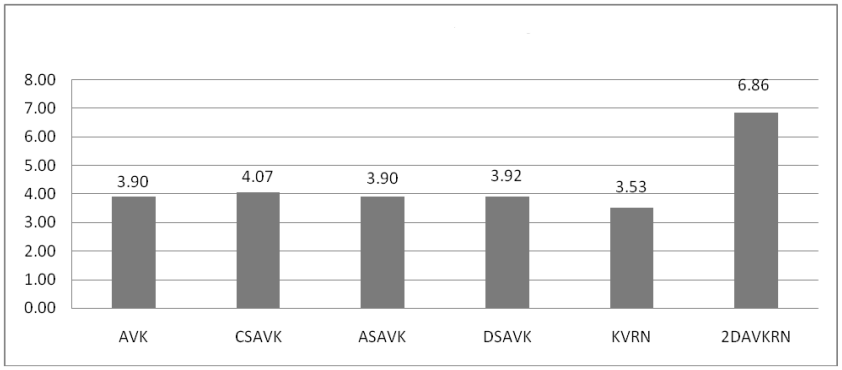

Figure 6. Average Randomness Comparison of Experiment 3

To define the degree of heterogeneity among the successive keys, average randomness alone is not sufficient to reveal all the characteristics and hence the standard deviation (SD) is also used as second parameter for comparison with the previous schemes. The standard deviation gives an idea of how close the entire set of data is to the average value. Data sets with the large standard deviation have data spread out over a wide range of values. The results of comparison of experiments 1, 2 and 3 have been depicted from Figure 7 to 9 respectively. In the following Figures, the x axis also indicates the various techniques where as y axis represents the standard deviation.

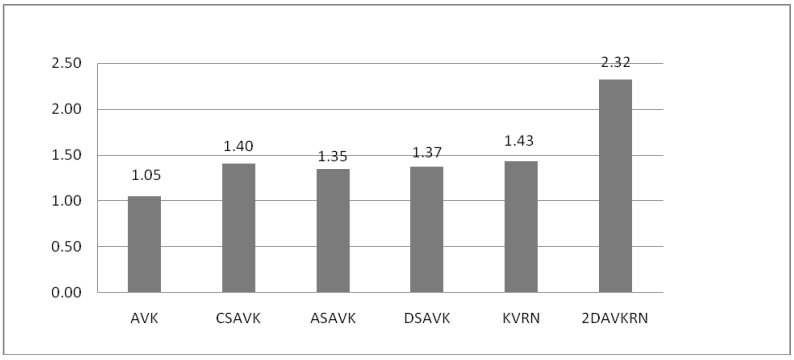

Figure 7. Standard Deviation Comparison for Experiment 1

Copyright ⓒ 2015 SERSC

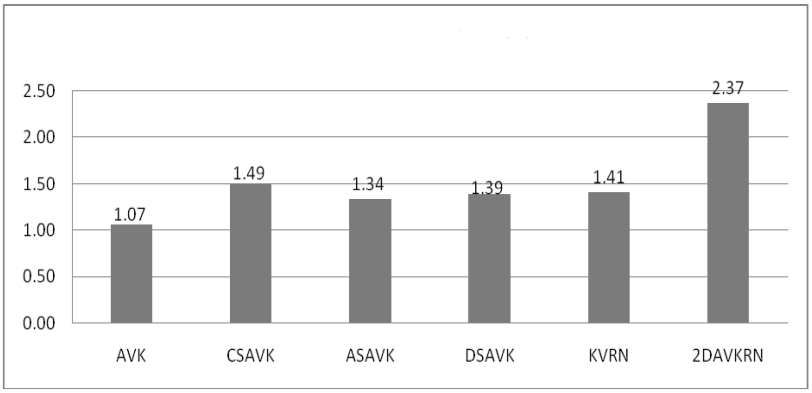

Figure 8. Standard Deviation Comparison for Experiment 2

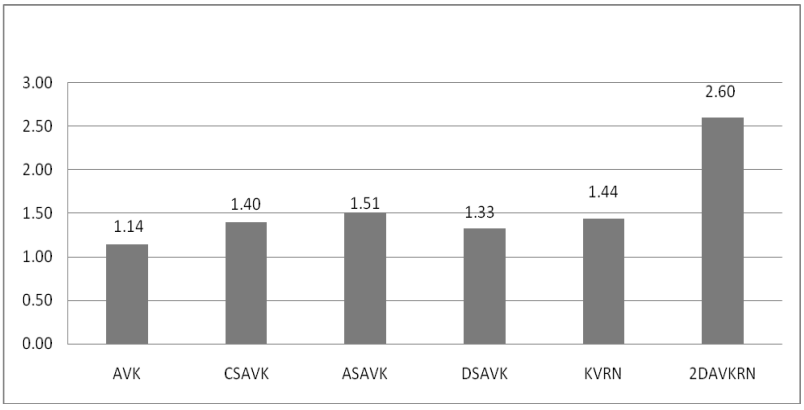

Figure 9. Standard Deviation Comparison for Experiment 3

6. Conclusion

In this paper, we have have proposed a 2 dimensional AVK with random number to enhance the security of shared information. We have shown that our proposed scheme increases the randomness among the auto generated successive keys by not only changing their bit sequences but also in sizes as well. In the performance analysis, we have illustrated that our scheme provides higher degree of heterogeneity among the key set. As our proposed scheme does enhance the auto generated keys to twice of its original size, it can be effectively implementable in AES.

References

[1] C. E. Shannon, "A Mathematical Theory of Communication", Bell Syst. Tech. J. Vol. 27, **(1948)**, pp - 379–423, 623–656.
[2] C. E. Shannon, "Communication Theory of Secrecy Systems", Bell Syst. Tech. J. **(1949)**, pp. 656-715 (1949).
[3] W. Diffe, M. E. Hellman, "Exhaustive Cryptanalysis of the NBS Data encryption standard", Computer, **(1977)**, pp. 74-84.
[4] E. Biham, "A fast new DES implementation in Software", Proc. Int. Symp. Foundations of Software Engineering, **(1997)**, 260-273.
[5] H. Eberle, "A High Speed DES Implementation for Network Application", Proc. Int. Conf. Cryptology, **(1992)**, pp. 521-539.
[6] B. Schneir, Applied Cryptography, 2nd edn.(John Willey & Sons Inc., New York, 1996).
[7] C. T. Bhunia, New Approaches for Selective AES towards Tackling Error Propagation effect of AES, Asian J. Inf. Tech. Vol. 5, no. 9, **(2006)**, 1017-1022.
[8] 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.

 Copyright ⓒ 2015 SERSC

[9] C. T. Bhunia, G. Mondal, S. Samaddar, Theory and Application of Time Variant Key in RSA and that with Selective Encryption in AES, Proc. of EAIT (Elsevier Publications, Calcutta CSI), **(2006)**, pp. 219-221.
[10] P. Chakarabarti, B. Bhuyan, A. Chowdhuri, C. T. Bhunia, A Novel Approach towards Realizing Optimum Data Transfer and Automatic Variable Key (AVK) in Cryptography, Int. J. Comput. Sci. Netw. Secure. Vol 8, no. 5, **(2008)**, pp. 241-250.
[11] C. T. Bhunia, S. K. Chakraborty, R. S. Goswami, A New Technique (CSAVK) of Automatic Variable Key in Achieving Perfect security, 100th Indian science Congress Association, January, 2013.
[12] R. S. Goswami, S. K. Chakraborty, A. Bhunia, C. T. Bhunia, New Techniques for generating of Automatic Variable Key in Achieving Perfect Security, J. Inst. Eng. India Ser. B, Publ. online (2014).
[13] R. S. Goswami, S. K. Chakraborty, A. Bhunia, C. T. Bhunia, New Approaches towards generation of Automatic Variable Key to achieve Perfect Security, 10th Int. Conf. Inf. Tech., IEEE Computer Society, 102 (2013).
[14] R. S. Goswami, S. K. Chakraborty, A. Bhunia, C. T. Bhunia, Generation of Automatic Variable Key under various approaches in Cryptography System, J. Inst.Eng. India Ser. B, Vol. 94, no. 4, **(2014)**, pp. 215-220.
[15] R. S. Goswami, S. K. Chakraborty, A. Bhunia, C. T. Bhunia, Various New Methods of Implementing AVK, 2nd Int. Conf. Adv. Comp. Science Eng. , **(2013)**, pp. 149-152.
[16] S. Banerjee, M. P. Dutta, C.T. Bhunia, A Novel Approach to Achieve the perfect security through AVK over Insecure Communication Channel, Communicated in Journal of the Institute of Engineering (India).
[17] S. Banerjee, M. P. Dutta, C.T. Bhunia, A New Three Dimensional Based Key Generation Technique in AVK, Communicated in Journal of the Institute of Engineering (India).
[18] B. K. Singh, S. Banerjee, M. P. Dutta, C.T. Bhunia,Generation of Automatic Variable Key to Make Secure Communication, International Conference on Recent cognizance in wireless communication & image processing-ICRCWIP-2014, 16 -17th January, 2015.
[19] M. P. Dutta, S. Banerjee, and C. T. Bhunia, "Two new schemes to generate automatic variable
[20] 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.
[21] DOI= http://dx.doi.org/10.1145/2743065.2743080.
[22] Rajat Subhra Goswami, Subhasish Banerjee, Manash Pratim Dutta, Chandan T Bhunia, "Absolute Key Variation Technique of Automatic Variable Key in Cryptography", In Proceeding SIN '15 of the 8th International Conference on Security of Information and Networks (Sochi, Russia), 8 -10th September, 2015. DOI=10.1145/2799979.2800021.
[23] M. P. Dutta, S. Banerjee, M. Das, R. S. Goswami and C. T. Bhunia, "Key Variation Technique based on Piggybacking Strategies under Public Key Environments", Communicated to Journal of Discrete Mathematical Sciences & Cryptography.
[24] M. P. Dutta, S. Banerjee, and C. T. Bhunia, "Generation of Variable Session Keys Based on Piggybacking Strategy", Accepted in 3rd International Conference on Advances in Computing, Electronics and Communication (Zurich, Switzerland), 10-11th October, 2015.

Authors

Manash Pratim Dutta, he is an Assistant Professor in the Department of Computer Science and Engineering in National Institute of Technology, Arunachal Pradesh. He is currently working towards his Ph. D degree in the field of cryptography and information security at the same institute.

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

Copyright ⓒ 2015 SERSC

Chandan Tilak Bhunia, he 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 Ph. D 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 international journals of repute. Under his supervision, five Ph. D scholars got awarded and nine scholars are currently working in various fields.

Copyright ⓒ 2015 SERSC