International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online), Volume 2, Special Issue 4, June 2014)
International Research Conference on Engineering, Science and Management 2014 (IRCESM 2014)

Sparse approach for realizing AVK for Symmetric Key Encryption

Shaligram Prajapat[1], Shashank Swami[2], Bhagirath Singroli[3], Dr. R. S. Thakur[4], Ashok Sharma[5], D. Rajput[6]
[1,4,6]*M.A.N.I.T. Bhopal, INDIA*
[2]*V.I.T.M., Gwalior, INDIA*
[3]*Presidency College, Raisen, INDIA*
[5]*B. U., Bhopal, INDIA*
shaligram.prajapat@gmail.com[1], shashank.swami2011@gmail.com[2], raj.sit@gmail.com[3], ramthakur2000@yahoo.com[4], ashoksharmamca@gmail.com[5], dharm_raj85@yahoo.co.in[6]

***Abstract*—Symmetric key cryptography has been a hot topic because of exchange of secure communication through various networks ligand Investigation of reversible XOR like function for symmetric key cryptography has been a big challenge. Moreover it is also desired that the reversible XOR function must be as efficient as traditional XOR. In the literature related to Automatic Variables Key, Fibonacci-Q matrix based key generation has also been proposed and used. This paper proposes a algorithm for cryptographic information exchange without transmitting key to end user. The proposed algorithm has been proposes new perspectives for secure communication using AVK approach for low power devices together with saving the key computation time.**

***Index Terms*— XOR, cryptography, Automatic Variable Key (AVK), Symmetric key**

I. Introduction

In cryptography, security of key is a major issue and the importance of Key in Cryptographic domain can be better understand by the Kerckoffs's [1883] statement that, "Security of a crypto system must be totally dependent on the secrecy of the key, not on the secrecy of algorithm".

It is still a major concern in current modern era [1]. It has been seen that securing the algorithm is not desirable as the inner working of a cryptosystem cannot be kept secret due to the fact that the underlying algorithm can be discovered by reverse-engineering. Hence for a successful cryptosystem, it is desirable to make the key secret instead of algorithm.

The focus of our proposed work is based on Symmetric approach where encryption key can be calculated from the decryption key and vice versa and in most of the symmetric algorithms the encrypting and decrypting key is the same and in some cases one can be derived from other.

Before starting communication, both the sender and receiver agree on a key so that they can communicate securely.

On the other hand, in an *Asymmetric algorithm*, the decryption key cannot be calculated from the encryption key.

Usually weak keys used in algorithm are easily decrypted by the intruder. The size of key used in any algorithm is one of the key factors as it contributes to the strength of symmetric key algorithms. In practice, state-of-art cryptographic algorithms rely on increasing the key size to strengthen the security of algorithm [2].Hence, Instead of increasing the key size we can fix the key size and vary it from session to session, this is the basis of our AVK approach.

In next sections we would present a scheme based on sparse matrix approach for efficient and secure communication without using any key exchange

II. Related Work

A landmark report[2] by an ad hoc group of cryptographers and computer scientists ,[Jan- 1996] , highlighted the importance of key length over secured data exchange systems employs a combination of conventional or symmetric cryptographic systems for encrypting data and public key or asymmetric systems for managing the keys used by the symmetric systems. Assessing the strength required for the symmetric encryption schemes is therefore an essential step in cryptography for computer and communication security. Technology available during late 1995 makes brute-force attacks against cryptographic systems considered better for the past several years in terms of both speed and cost perspectives.. In this literature it is pointed out that cryptosystems with 40-bit keys offer virtually no protection at this point against brute-force attacks and DES with 56-bit keys are inadequate to provide security. The literature indicates that the cost of very long key length for strong encryption is not an issue related to efficiency. Therefore, to provide adequate protection against the most serious threats keys used to protect data today should be at least 75 bits long.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online), Volume 2, Special Issue 4, June 2014)
International Research Conference on Engineering, Science and Management 2014 (IRCESM 2014)

So, to protect sensitive information adequately for the next 20 years in the face of expected advances in computing power, keys in newly-deployed systems should be at least 90 bits long. Authors have also thrown light over the power of encryption in protecting the privacy of data exchange over network and authors have stated that encryption provides confidentiality for information security and prevents the information against threats from a variety of potential attackers.

Current Technologies permit very strong encryption effectively with the same cost as in case of weaker encryption. This work also highlights the model that infers meaningful and readily available technology that makes Brute-Force Decryption attacks faster and cheaper, also 40-bit key lengths offer virtually no protection, even DES with 56-Bit Keys is increasingly inadequate. There may be smarter approaches of attack than brute force. in the year 1998 authors have strongly recommend a minimum key-length of 90 bits for symmetric cryptosystems.

In the work of [3], authors have proposed an approach for reducing the cryptanalysis attack risk by using a dynamic key theory. Dynamic keys were used once as symmetric cryptographic keys and their dynamic key theory generation scheme and key update mechanism were analyzed. In this work, Key size, sequence length and synchronization problem were investigated for security of symmetric cryptography. The probability of breaking system was reduced. From storage point of view, for higher security more memory space requires for more parameters. Synchronization issue is yet to be resolved in this work.

In [4], AVK has been demonstrated as time variant key technique. Where key is generated by a variable data transmitted in prior session. Some new techniques to generate time variant key has been proposed and compared to find out the best one. Their CSAVK technique found to be superior for some set of keys. The approach is yet to be investigated to examine the effect on brute force attack and differential frequency attack to bit positions of XOR, shifting, shifting, rotation etc.

Recent works in [8,9,10] Fibonacci-Q matrix based AVK approach has been proposed, implemented and analyzed for secure information transmission over noisy channel by hand held devices. The work needed yet further analysis for systematic attacks and hacker's perspective.

From above literature survey it can be inferred that the work and experiments are being constantly done to enhance the security of data exchange over run trusted network. This paper presents novel approach towards symmetric key transmission without using key exchange. The subsequent section describes basic terminologies and then details the working of proposed algorithm.

III. Basic Definitions And Terminology

Sparse Matrix: A sparse matrix is one whose most of it's elements are zero. A sparse matrix allows special techniques to take advantage of the large number of "background" (commonly zero) elements. The number of zeros a matrix needs in order to be considered as "sparse" depends on the structure of the matrix and the desired operations to perform on it. In a randomly generated sparse n × n matrix with p=cn entries scattered randomly throughout the matrix is not sparse in the sense of Wilkinson (for direct methods) since it takes O(n3) time to factor (with high probability and for large enough c=p/n)[5, 6 ,7].

Representation of Sparse Matrix: Substantial memory space reductions can be achieved by storing only the non-zero values. Depending on the number and distribution of the non-zero entries, different data structures can be used and yield huge savings in memory when compared to the basic approach .Consider sparse matrix of order 6 by 6 , A=

$$\begin{bmatrix} 0 & 0 & 19 & 0 & 0 & 0 \\ 15 & 0 & 0 & 11 & 0 & 28 \\ 0 & 12 & 0 & 0 & 14 & 0 \\ 0 & 11 & 29 & 0 & 0 & 0 \\ 11 & 15 & 0 & 0 & 16 & 0 \\ 0 & 0 & 9 & 0 & 0 & 0 \end{bmatrix}$$

Criterion for being a Sparse matrix: We Assume that "p" is the number of nonzero elements in the matrix A. the array of size p would require 3-elements in this array would occupy 3 integers. To find out the reduction in storage space that could be represented by such a representation. consider the space required for storing a m X n integer matrix in a 2-D array. Obviously the size(no. of bytes) required by this array is = m*n*Size_ of_ integer . In spm-version **spmat** would be advantageous would be iff: 3 * p* Size_of_integer < m * n * Size_of_integer => $p < \frac{m*n}{3}$ .If number of non-zero elements is less than one third of the total number of elements in the matrix then the "array of structure" representation is better. Above matrix A may be represented more economically (in terms of space) if conventional 2-D array representation of matrices is not used. The idea is, it is possible to represent to store more information regarding non zero elements only. If this is done, then the matrix may be thought of as an ordered list of nonzero elements only. This 6 X 6 matrix "A" can be described as a 1-Dimensional array, "a", such that :no_of_rows=6, no_of_columns=6, no_of_element=12. this can be expressed also in the a[0] position of following spmat array: csm[0] or .

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online), Volume 2, Special Issue 4, June 2014)
International Research Conference on Engineering, Science and Management 2014 (IRCESM 2014)

Rest of the array a from index [1 ..no_of_element] would be expressed as follows:

csm[1]=[0,2,19],csm[2]=[1.0,15], csm[3]=[1,3,11], csm[4]=[1,5,18], csm[5]=2,1,12], csm[6]=[2,4,14], csm[7]=[3,1,11] aand so on.

[0,2,19 1,0,15 1,3,11 1,5,18 2,1,12 2,4,14 3,1,11 3,2,29 4,0,11 4,1,15 4,4,16 5,2,9]

Information about a nonzero element has only three parts:(i) An integer representing it's row index.(ii)An integer representing it's column index.(iii)The nonzero data associated with this location. Such a 3-tuple can be represented by data structure with 3 fields as follows:

C-Representation

#define max 100

typedef struct element { int row, column, data;} element;

Now a sparse matrix may be defined as:

typedef struct spmat{ int no_of_element; int no_of_column; element data[max];} spmat; OR

element spmat[max], CSM[max];

Here, each element in the array is a 3-tuple, the contents of the array are pictorially shown by means of 3-integers separated by commas.

IV. Propsosed Sparse-AVK Algorithm

For Secure transmission of information over noisy channel, we assume that desirable data of our interest are the nonzero entries of sparse matrix using row major form (assuming standard representation scheme).At transmission end the position of nonzero element would serve as a key for encryption/ decryption using a linear curve, where a and b are row and column indexes of non zero data respectively being the data item being transmitted. The assumption of proposed algorithms is that row and column indexes starts from 1.so reconsidering the original compact sparse matrix representation:

[1,3,19 2,1,15 2,4,11 2,6,18 3,2,12 3,5,14 4,2,11 4,3,29 5,1,11 5,2,15 5,5,16 6,3,9]

Proposed Linear AVK based Encryption Algorithm

Algorithm Linear AVK Encrypt (matrix CSM)

{
// This algorithm accepts plain text from Alice and converts cipher Text for transmission over noisy channel
for each i from 1 to CSM[0][3] do
{
Set a= CSM[i][0], b=CSM[i][1], plainText=CSM[i][2]
Generate cipherText CSM'[i][2]=a+b*plaintext;
Transmit cipherText CSM'[i]
}
}

Algorithm LinearAVKDecrypt (matrix CSM')

{
// This algorithm accepts Compact Sparse Matrix with cipher text and recovers plain text in plaintext_CSM'[i]
for each i from 1 to CSM'[0][2] do
{
Set a= CSM'[i][0], b=CSM'[i][1], plainText=CSM'[i][2]
Generate plainText _CSM'[i]=(CSM'[i][3]-CSM'[i][0])/CSM'[i][1];
return(PlainText_CSM'[i])
}
}

V. Results And Discussion

The algorithm Linear AVK Encrypt() accepts compact form of sparse matrix entries and uses location (index position) as parameter for Cipher generation i.e. it utilizes information of nonzero element it converts the information into ciphertext in linear time. Similarly Linear AVK Decrypt() receives cipher text of data item and based on it's key (using index position of element as parameter) it recovers original information. Since key is not transmitted in the data transfer. so it becomes highly difficult to interpolate any information regarding plaintext or key. Table-I demonstrates the working of proposed scheme:

The sparse matrix recovered by trudy (man in middle) would by as follows:

[1,3,58 2,1,17 2,4,46 2,6,110 3,2,27 3,5,73 4,2,26 4,3,91 5,1,16 5,2,35 5,5,85 6,3,33]

The beauty of proposed algorithm is that similar data (entry no. 3, 7and 9)would be encoded with different bit strings, so patterns of original plain text cannot be generated, this adds an extra security. The data is encrypted by position of the device or data item hence the key would be different for different locations, so same information would have different ciphers making position based variability in data items. The algorithm is memory efficient O(p+1) =O(p) and takes O(n) time for processing ,where p is number of nonzero items.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online), Volume 2, Special Issue 4, June 2014)
International Research Conference on Engineering, Science and Management 2014 (IRCESM 2014)

TABLE I.
ILLUSTRATION OF AVK APPROACH ON SPARSE MATRIX FOR SECURE INFORMATION TRANSMISSION

Index	i	j	M(i,j)	Data Sent by Alice (Binary Plain Text)	Message bits on Noisy Channel	Generated Cipher by Trudy(Man in middle)	Data Received by BOB (Recovered Plain Text)
0	6	6	12	00001100	01001110	78	00001100
1	1	3	19	00010011	00111010	58	00010011
2	2	1	15	00001111	00010001	17	00001111
3	2	4	11	00001011	00101110	46	00001011
4	2	6	18	00010010	01101110	110	00010010
5	3	2	12	00001100	00011011	27	00001100
6	3	5	14	00001110	01001010	73	00001110
7	4	2	11	00001011	00011010	26	00001011
8	4	3	29	00011101	01011011	91	00011101
9	5	1	11	00001011	00010000	16	00001011
10	5	2	15	00001111	00100011	35	00001111
11	5	5	16	00010000	01010101	85	00010000
12	6	3	9	00001001	00100001	33	00001001

VI. CONCLUSION AND FUTURE WORK

This paper presents novel algorithm using fast and secure encryption approach on sparse matrix. The algorithm opens some new direction towards application of sparse matrix in efficient and effective manner. The cipher generation scheme is working fine even for any input size, the work can be extended for various other nonlinear curves and can be compared for efficiency with LinearAVKencrypt() and LinearAVKdecrypt().

Acknowledgment

This work is supported by research project under Fast Track Scheme for Young Scientist from DST, New Delhi, India. Scheme 2011-12, No. SR/FTP/ETA-121/ 2011 (SERB), dated 18/12/201 and This work is supported by research grant from MPCST, Bhopal, India Project ref. No. 1080/CST/R&D/2012, Dated 30/06/2012.

REFERENCES

[1] William and Stalling, Cryptography And Network Security, 4/E. Pearson Education India, 2006.

[2] Matt Blaze, Whitteld Diffe, Ronald L. Rivest, Bruce Schneier, Tsutomu Shimomura, Eric Thompson, Michael Wiener," Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security", A Report by an Ad Hoc Group of Cryptographers and Computer Scientists, January 1996.

[3] Huy Hoang Ngo, Xianping Wu, Phu Dung Le, Campbell Wilson, and B. Srinivasan, "Dynamic Key Cryptography and Applications", International Journal of Network Security, Vol.10, No.3, PP.161-174, May 2010.

[4] R. Goswami, S. Chakraborty,A. Bhunia,C. Bhunia, "Generation of Automatic Variable Key under Various Approaches in Cryptography System", J. Inst. Eng. India Ser. B (December 2013–February 2014) 94(4):215–220.

[5] Gilbert, J. R, Moler, C. Schreiber, R. "Sparse Matrices in MATLAB: Design and Implementation." SIAM J. Matrix Anal. Appl. 13, 333-356, 1992.

[6] Press, W. H., Flannery, B. P., Teukolsky, S. A., Vetterling, W. T. "Sparse Linear Systems." in Numerical Recipes in FORTRAN: The Art of Scientific Computing, 2nd ed. Cambridge, England: Cambridge University Press, pp. 63-82, 1992.

[7] Tim Davis,, http://mathworld.wolfram.com/ topics/ DavisTim.html, April 2014.

[8] ShaligramPrajapat, Amber Jain, Dr. R.S. Thakur, "A Novel Approach For Information Security With AVK Using Fibonacci Q-Matrix, International Journal of Computer & Communication Technology, Vol-3, Issue 3, 2012.

[9] Shaligram Prajapat, Sachin Saxena, Amber Jain, P. Sharma et al., "Implementation of Information Security With Fibonacci-Q matrix", Proceedings of International Conference on Intelligent Computing and Information System, 2012.

[10] Shaligram Prajapat, D.S. Rajput, Dr. R.S. Thakur, "Time variant approach towards Symmetric Key", Science and Information Conference 2013, London, IEEE-2013.