ATLANTIS PRESS

Advances in Intelligent Systems Research, volume 134

2nd International Conference on Control, Automation, and Artificial Intelligence (CAAI 2017)

The Fountain-codes-based Encryption and Decryption Algorithm Research

Ming Hu, Wen Li, Fagao Yu and Xinrong Hu

College of Mathematics and Computer Science, Wuhan Textile University, Hubei Province Wuhan, 43000

***Abstract*—Fountain code uses randomized coding to ensure the reliability of data, the paper uses the randomized coding of fountain code to enhance the security of encryption algorithm. FEA is a symmetric encryption algorithm, and its keys-lengths are variable and expansive to meet users' requirement with the setting of keys-lengths according to the important degree of information, so users can effectively manage keys and information. FEA carries out encryption operation by table to reduce calculative amount and improve encryption efficiency, so it meets user's requirement with encryption efficiency.**

Keywords-fountain code; keys-lengths; encryption efficiency

I. INTRODUCTION

With the rapid development of Internet, users receive or send plenty of information everyday, but the security of information was broken by viruses and trojans. Nowadays, network information are transmitted by fountain code[1], whose randomized coding can ensure the reliability of information. In order to the security of network information, the paper will apply the randomized coding of fountain code to carry out encryption algorithm.

In recent years, many researchers proposed much novel improvements with fountain code. For examples, the literature[2] reduced the complexity of decoding; the literature[3] enhanced transmission efficiency, reduced protocol complexity. In contrast, symmetric encryption algorithms, such as DES[4], 3DES[5] and AES[6], carry out encryption operation for large datum, and its advantage is high encryption efficiency. In recent years, The literature[7] was high encryption efficiency. The literature[8] enhanced the security of information and reduced the complexity of algorithm.

Therefore, the paper proposed the Fountain codes-based Encryption Algorithm (FEA). FEA is a symmetric encryption algorithm, and its key-lengths are variable and expansive that users can effectively manage keys and information. FEA reduced the calculated amount by table, so it improved encryption efficiency.

II. FOUNTAIN CODE

Fountain code carries out randomized encoding operation for k groups of original data as a matrix X=[x1,x2,...,xk] by a encoding key as a matrix C=[C1,C2,...,Cn] (1<=i<=n) and Ci = [gi1,gi2,...,gik], producing n groups of encoding data as a matrix Y=[y1,y2,...,yn],which are carried out randomized decoding operation by a decoding key as a matrix C-1=[C1,C2,...,Ck]-1 (1<=i<=n) and Ci -1= [gi1,gi2,...,gin]-1 when n is slightly bigger than k , so original data are recovered by high probability, as follows:

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} \mathbf{C_1} \\ \mathbf{C_2} \\ \vdots \\ \mathbf{C_n} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix} = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1k} \\ g_{21} & g_{22} & \cdots & g_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ g_{n1} & g_{n2} & \cdots & g_{nk} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix} \quad (1)$$

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix} = \begin{bmatrix} \mathbf{C_1} \\ \mathbf{C_2} \\ \vdots \\ \mathbf{C_k} \end{bmatrix}^{-1} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix}^{-1} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} \quad (2)$$

The above equations are shown that a matrix C is a reversible matrix that is a matrix C-1, therefore, the randomized coding of fountain code will be applied to encryption algorithm.

III. THE ENCRYPTION AND DECRYPTION OF FEA

A. *The Encryption Mode and Decryption Mode of FEA*

The encryption model and decryption model of FEA in Figure 1: plaintext data is carried out randomized cyclic shift and iteration xor operations by encryption keys to produce encryption data, which is carried out disturbing xor operation by encryption keys to produce ciphertext data; ciphertext data is carried out inversely disturbing xor operation by decryption keys to produce decryption data, which is carried out inversely randomized cyclic shift and iteration xor operations by decryption keys to recover plaintext data.

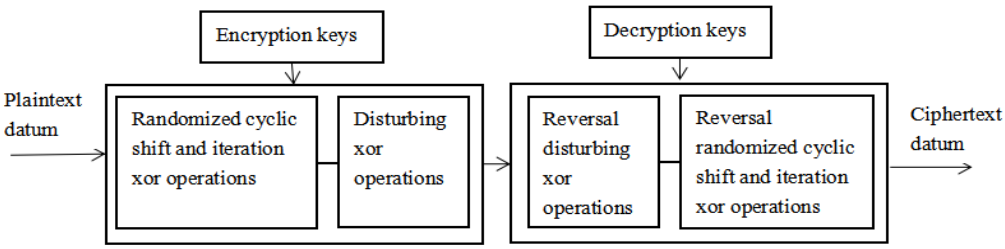

FIGURE I. THE ENCRYPTION AND DECRYPTION MODEL OF FEA

B. The Keys Algorithm

FEA is a symmetric encryption algorithm, and its keys-length is variable and expansive. The keys theory of FEA is shown that n bytes of keys K can produce n subkeys Keyi (1<=i<=n), one of which can produces 8 rounds of randomized numbers Rj(0<=j<=7), therefore, n bytes of keys K can produce 8×n rounds of randomized numbers Rj(0<=j<=7).Encryption randomized number matrix C(Rij) which is a binary matrix is produced by 8 rounds of randomized numbers Rj ;encryption randomized controlling matrix E(Keyi) equals to the result of multiplying eight encryption randomized number matrices C(Rij)(0<=j<=7); encryption keys disturbing matrix B(Keyi) consists of 8 rounds of randomized numbers Rj(0<=j<=7). 1 subkey Keyi produces 8 rounds of randomized numbers Rj(0<=j<=7),as follows:

$$\text{where}\quad k=0,\begin{cases} m_0 = Key_i \oplus k \oplus 6 \\ R_0 = ((k+7)(m_0+5)) \bmod 8;\ \ j=0 \end{cases}$$

$$\text{where}\quad k\in[1,7],\begin{cases} \text{if}\ \ Key_i\ \text{is even},\ \ Key_i\ \text{move to the right one}; \\ \text{if}\ \ Key_i\ \text{is odd},\ \ Key_i\ \text{move to the right one},\begin{cases} Key_i = Key_i \oplus 128 \\ R_{j\text{-}1}\ \ \text{move to the right one} \end{cases}; \end{cases} \tag{3}$$

$$\Rightarrow \begin{cases} m_k = Key_i \oplus k \oplus 6 \\ R_j = ((k+7)(m_k+5)) \bmod 8;\ j\in[1,7] \end{cases}$$

Where mk is a parameter ,1<=i<=n, 0<=k<=7,0<=j<=7, 0<=Keyi<=255, 0<=Rj <=7, Keyi is the (i)th round of subkey,and Rj is randomized numbers.The values of different subkeys Keyi from 0 to 255 can produce the values of 8 rounds of randomized numbers Rj according to Eq.3,as follows in Table 1.

TABLE I. 8 ROUNDS OF RANDOMIZED NUMBERS RJ OF SUBKEY

Subkey Key_i	8 round of randomized numbers R_j (0<=j<=7)
0	(5, 0, 7, 4, 5, 0, 3, 4)
1	(2, 4, 3, 4, 5, 0, 7, 0)
2	(7, 1, 0, 6, 3, 0, 3, 4)
3	(3, 3, 2, 2, 7, 0, 7, 0)
4	(1, 0, 3, 4, 5, 0, 3, 4)
5	(0, 6, 1, 0, 1, 0, 7, 0)
6	(3, 1, 0, 6, 3, 0, 3, 4)
7	(1, 0, 3, 4, 5, 0, 7, 0)
8	(5, 0, 5, 2, 7, 0, 3, 4)
.....	.....
255	(1, 0, 0, 0, 3, 1, 0, 5)

From the Table 1, the keys algorithms can produce the different values of 8 rounds of randomized numbers Rj when users inputted different subkey Keyi ,therefore, 8 rounds of randomized numbers Rj are unique and random characters, and E(Keyi) are also unique and random characters according to the producing theory of E(Keyi).

C. The Encryption Algorithm

The computer read 8 bytes from plaintext file which are divided into 8 groups of plaintext data as a plaintext matrix X, which equals to a encryption matrix Y0. Y0 will be carried out randomized recursion encryption operations: where 1<=i<=n, a encryption matrix Yi-1 is carried out the (i)th round of randomized cyclic shift and iteration xor operation by E(Keyi) to produce encryption data, which is carried out the (i)th round of disturbing xor operation by B(Keyi) to produce a encryption matrix Yi; a encryption matrix Y0 is carried out in total n rounds of encryption operations to produce a encryption matrix Yn, which equals to a cipheretext matrix Y when i only equals to n,as follows.

$$\begin{cases} \mathbf{Y_0} = \mathbf{X}; i=0 \\ \mathbf{Y_i} = \mathbf{E(Key_i)Y_{i-1}} \oplus \mathbf{B(Key_i)}; 0<=i<=n \\ \mathbf{Y} = \mathbf{Y_n}; i=n \end{cases}$$

$$\text{where}\begin{cases} \mathbf{E(Key_i)} = \mathbf{C(R_{i0})}\cdot\mathbf{C(R_{i1})}\cdot\cdots\cdot\mathbf{C(R_{i7})} \\ \mathbf{B(Key_i)} = [R_{i0}, R_{i1}, \cdots, R_{i7}]^T \\ \mathbf{Y_i} = [y_{i0}, y_{i1}, ..., y_{i7}]^T \end{cases} \tag{4}$$

Where E(Keyi) is a encryption randomized controlling matrix, B(Keyi) is a encryption key disturbing matrix , X is a plaintext matrix, Yi is a encryption matrix, Y is a cipheretext matrix. C(Rij) is a encryption randomized number matrix, namely, C(Rij) is also a binary matrix. C(0) moves the right cyclic zero bit when Rij equals to 0; C(1) moves to the right cyclic one bit when Rij equals to 1;...; C(7) moves to the right cyclic seven bit when Rij equals to 7. For example 1,C(0) and C(4) are shown when Rij equal to 0 and 4, as follows:

$$\mathbf{C(0)} = \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 1&1&0&0&0&0&0&0 \\ 1&1&1&0&0&0&0&0 \\ 1&1&1&1&0&0&0&0 \\ 1&1&1&1&1&0&0&0 \\ 1&1&1&1&1&1&0&0 \\ 1&1&1&1&1&1&1&0 \\ 1&1&1&1&1&1&1&1 \end{bmatrix}$$

$$\mathbf{C(4)} = \begin{bmatrix} 0&0&0&0&1&0&0&0 \\ 0&0&0&0&1&1&0&0 \\ 0&0&0&0&1&1&1&0 \\ 0&0&0&0&1&1&1&1 \\ 1&0&0&0&1&1&1&1 \\ 1&1&0&0&1&1&1&1 \\ 1&1&1&0&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \end{bmatrix}$$

The Eq.4 is described about the theory of matrix multiplication, and its “add(+)” operation will be abstractly

seen as "xor(⊕)" operation.For example 2,C=AB

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} \Rightarrow \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} \Rightarrow \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_1 \oplus b_2 \\ b_1 \oplus b_2 \oplus b_3 \end{bmatrix}$$

D. The Decryption Algorithm

The computer read 8 bytes from ciphertext file which are divided into 8 groups of ciphertext data as a ciphertext matrix Y, which equals to a decryption matrix X0'. X0' will be carried out inversely randomized recursion operations: where 1<=i<=n,a decryption matrix Xi-1' is carried out the (i)th round of inversely disturbing xor operation by B(Keyn-i+1) to produce decryption data, which is carried out the (i)th round of inversely randomized cyclic shift and iteration xor operations by E(Keyn-i+1) -1 to produce a decryption matrix Xi' ;X0' be carried out in total n rounds of decryption operations to produce a decryption matrix Xn',which equals to a ciphertext matrix X when i only equals to n,as follows:

$$\begin{cases} \mathbf{X_0^{'}} = \mathbf{Y}; i = 0 \\ \mathbf{X_i^{'}} = \mathbf{E(Key_{n-i+1})^{-1}(X_{i-1}^{'} \oplus B(Key_{n-i+1}))}; 0 <= i <= n \\ \mathbf{X} = \mathbf{X_n^{'}}; i = n \end{cases} \tag{5}$$

$$where \begin{cases} \mathbf{E(Key_{n-i+1})^{-1} = C(R_{(n-i+1)0})^{-1} \cdot C(R_{(n-i+1)1})^{-1} \cdots C(R_{(n-i+1)7})^{-1}} \\ \mathbf{B(Key_{n-i+1})} = [R_{(n-i+1)0}, R_{(n-i+1)1}, \cdots, R_{(n-i+1)7}]^T \\ \mathbf{X_i^{'}} = [x_{i0}^{'}, x_{i1}^{'}, \cdots, x_{i7}^{'}]^T \end{cases}$$

Where E(Keyn-i+1) -1 is a decryption randomized controlling matrix, B(Keyn-i+1) is a decryption key disturbing matrix, Y is a cipheretext matrix, Xi' is a decryption matrix and X is a plaintext matrix.C(R(n-i+1)j)-1 is a decryption randomized controlling matrix,and it is the inverse matrix of encryption randomized controlling matrix C(Rij), which will be carried out the inverse matrix operations to obtain C(R(n-i+1)j)-1. For example 3, C(0)-1 and C(4)-1 are shown when R(n-i+1)j equal to 0 and 4,as follows:

$$\mathbf{C(0)^{-1}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 \end{bmatrix}$$

$$\mathbf{C(4)^{-1}} = \begin{bmatrix} 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

IV. The Theoretical Analysis and the Results of Experiment

A. The Security Demonstration of FEA

From the Table 1, 8 rounds of randomized numbers Rj are unique and random characters, and E(Keyi) is also unique and random character because it was produced by C(Rij). And Yi-1 are carried out in total n rounds of randomized recursion encryption operations including randomized cyclic shift , iteration xor and disturbing xor. Firstly, randomized cyclic shift operation can randomly changes the shift of data to enhance the diffusion of data between plaintext data and encryption data. Secondly, randomized iteration xor operation can hides the relationship of between plaintext data and encryption data to enhance the randomized disorder of encryption datum. Thirdly, disturbing xor operation can also enhances the disorder of encryption data. Therefore, the functions of three operations can improve the complexity of FEA.

In conclusion, The security of FEA is higher.

B. The Key Management

With the fast growing of network data, users want to set as the keys-lengths so that they can effectively manage information and keys according to the important degree of information. DES's keys-length is 56bit, 3DES's keys-lengths are 112 and 168 bit, and AES's keys-lengths are 128,192 and 256 bit. In contrast, FEA's key-length is 8×n bit. Consequently, we have known that the keys-lengths of DES, 3DES and AES are constant, however, the keys-lengths of FEA are variable and expansive. Therefore, FEA is more suitable for users to manage information and keys according to the important degree of information than DES, 3DES and AES.

C. The Results of Encryption Time

The randomized function Rand() can produces randomized data, which are inputted to plaintext file,as follows:

$$\begin{cases} When\ Rand\_Max = 2\text{^}15, x = n*1024, n >= 1, z = (x+1)/2+1 \\ y_0 = 255*rand()/Rand\_Max; where\ x\ is\ odd \\ y_i = 65535*rand()/Rand\_Max; where\ 0 <= i < z-1 \\ y_i = 0; where\ i = z-1 \end{cases} \tag{6}$$

Where x is a integer, yi is a randomized data. The capacities of plaintext files were 10M, 20M and 40M. The abbreviation of plaintext file and encryption time is respectively seen as PF and ET.FEA,DES,3DES and AES all carry out encryption operations to obtain their encryption time, as follows in Table2.

TABLE II. THE ENCRYPTION TIME OF DES, 3DES,AES AND FEA

PF's capacity	FEA's ET(s)--64bit	DES's ET(s)--64bit	FEA's ET(s)--128bit	3DES's ET(s)--128bit	AES's ET(s)--128bit	FEA's ET(s)--192bit	3DES's ET(s)--192bit	AES's ET(s)--192bit	FEA's ET(s)--256bit	AES's ET(s)--256bit
10M	5.774	24.846	11.347	78.744	21.334	18.137	78.744	25.335	22.642	29.336
20M	11.649	50.087	22.573	150.574	43.042	33.440	150.574	56.417	45.896	69.792
40M	22.648	90.575	44.302	270.565	85.237	66.363	270.565	104.422	88.596	123.607

From the Table 2, when the capacities of plaintext files and their keys-lengths are all equal, FEA's encryption time

are all less than DEA,3DES and AES, then, FEA's encryption efficiency are all higher than DEA,3DES and AES, therefore, FEA meets the users' requirement with the encryption efficiency of large files.

V. CONCLUSION

FEA is a symmetric encryption algorithm, there are three advantages:(1) The paper has been proved that the security of FEA is higher;(2)The keys-lengths of FEA are variable and expansive, whereas, the keys-lengths of DES,3DES and AES are constant, therefore, FEA is more suitable for users to manage keys and information according to the important degree of information than DES,3DES and AES; (3) The encryption efficiency of FEA is higher than DES, 3DES and AES, therefore, FEA meets the requirement of users for the encryption efficiency of large files.

ACKNOWLEDGEMENTS

This research was financially supported by the Research the Textile Networking Support Technology (RTNST) and Nation Natural Science Foundation of China (NSFC).

REFERENCES

[1] Luby M. LT Codes [J]. Proc 43rd Annual IEEE Symposium on Foundation of Computer .Science, 2002, 2 (07):271-282.

[2] LI Lu-ying, LI Zong-yan, WANG Wen-bo. Adaptive iteration for fountain decoding [J]. The Journal of China Universities of Posts and Telecommunications.2010, 17(2):22-25.

[3] Lifang Feng, Rose Qingyang Hu,Jianping Wang, Peng Xu. Fountain code-based error control scheme for dimmable visible light communication systems [J].optics communication.2015, 347: 20-24.

[4] Luo ZuLing. Database encryption based on DES algorithm [J].Equipment Manufacturing Technology.2007, (6): 81-82, 98.

[5] Zhang Jie,Zhu LiJuan.The encryption algorithm of DES analysis and implementation[J]. Software Guide, 2007, (3): 95-97.

[6] J Daemen, V Rijmen. The Design of Rijndael: AES-The Advanced Encryption Standard [M]. Berlin: Springer-Verlag.2002.

[7] Fu YongGui,Ma ShangCai. An improvement symmetric key dynamic generation [J] algorithm and application.2011, 20(6): 169-172.

[8] Sourabh Chandra,Bidisha Mandal, Sk. safikul Alam, Siddhartha Bhattacharyya. Content based double encryption algorithm using symmetric key cryptography [J]. Procedia Computer Science .2015, 57: 1288-1234.