A Study on the Stream Cipher Embedded Magic Square of Random Access Files

rock@phate.tw

Abstract

Magic square and stream cipher issue are very interest well-tried topic. In this paper, we are proposed a new scheme which stream cipher application for random access file that based on magic square method. By the way, there are two thresholds to secure ours data, if decrypts only by the stream cipher. It isn't to recovery original source. In other hand, we improve the model of cipher stream to strong the defense efficiently, it also own high speed calculate to most parts of key stream generator.

Keywords: Stream Cipher, Magic Square, Key Stream Generator, Quadratic Residue

1. Introduction

Symmetric key cryptosystems are an important type of modern cryptosystem [1, 2, 4, 5, 8, 11, 13]. Symmetric key systems are cryptosystems where the same key is used for both encryption and decryption. This class of cryptosystem is important in modern cryptography because, in general, symmetric key cryptosystems are much faster than public key cryptosystems. Stream ciphers, on the other hand, process plaintext in small blocks (sometimes as small as a single bit). In contrast to block ciphers, stream ciphers keep some sort of memory, or state, as it processes the plaintext and uses this state as an input to the cipher algorithm [14-15]. In this paper, we are proposed a new scheme stream cipher contain magic matrix [3, 6, 7, 9, 10], to strong a random access file that you already to protect it. Section 2 will describe what kind of cipher schema did we concept in practice. Section 3 is discussing magic square that it will apply in random access file while encryption already implements early. Part 4, it is analysis the reliability with decrypt and encrypt; Conclusion and future research will be mention in final section.

2. Implementation Stream Cipher

The original file will be encrypting step by two stages. First step is key stream generator using by stream cipher [17-19], it used quadratic residue for the kernel of generator, and second step is proposed for magic square [20-24]. The key stream generator had some property which size of file is always same for plain text and cipher text. In other hand, current state had to generate next state. If you want to get the next state, the current state must be known.

In this section, we implement BBS Generator [16] conception to strong stream cipher. The notation is stated as follow:

A : Denote a secret key.

Q : Denote a public key.

Q^{-1} : Denote a multiplicative inverse of Q .

E : Denote an output value.

P : Denote a large prime number

e : Denote an output value of quadratic residue E .

2.1 Algorithm

$$E_0 \equiv (A \cdot Q) + Q^{-1} (mod \quad P)$$
$$e_0 \equiv E_0^2 (mod \quad P)$$
$$E_1 \equiv (e_0 \cdot A) + Q (mod \quad P)$$
$$e_1 \equiv E_1^2 (mod \quad P)$$
$$E_2 \equiv (e_1 \cdot e_0) + A (mod \quad P)$$
$$e_2 \equiv E_2^2 (mod \quad P)$$
$$E_3 \equiv (e_2 \cdot e_1) + e_0 (mod \quad P)$$
$$\vdots$$
$$E_n \equiv (e_{n-1} \cdot e_{n-2}) + e_{n-3} (mod \quad P)$$

2.1.1 Definition

The quadratic residuosity problem (QRP) is following: given an odd composite inter n and $e \in J_n$, decide whether or not e is a quadratic residue modulo n.

2.2 Key Generation Phase

Step 1: User U_i randomly selects a private key A to computes $E \equiv (A \cdot Q) + Q^{-1} (mod \quad P)$.

Step 2: User U_i computes $e \equiv E^2 (mod \quad P)$.

Step 3: Repeat the step 2 until the end of operating.

For Example:

Lets A =23, Q^1 =18, Q^{-1} =78 and P =101.

Therefore, we compute $E = (23 \cdot 18) + 73 (mod \quad 101) = 487 (mod \quad 101) = 83$, after calculate $e = E^2 (mod \quad p)$. $e = 487^2 (mod \quad 101) = 21$. The key generation procedure is shown in Table 1.

Table 1 Procedure of Key Generation Phase.

Order	Value A	Value Q	Inverse of Q	$e = E^2 (mod \quad 101)$	$E = (A \cdot Q) + Q^{-1} (mod \quad 101)$
1	23	18	73	21	83
2	21	23	18	16	97
3	16	21	23	5	56
4	5	16	21	0	0
5	0	5	16	54	16
6	54	0	5	25	5
7	25	54	0	56	37
8	56	25	54	85	40
9	85	56	25	30	38
…	…	…	…	…	…
…	…	…	…	…	…
100	0	49	92	81	8464

2.3 Encryption Phase

Table 2 Procedures of Encode and Decode Phase.

Order	e	Random Number	Encode	Decode
1	21	89	98	89
2	16	18	46	18
3	5	111	92	111
4	0	80	0	80
5	54	14	12	14
6	25	27	28	27
…	…	…	…	…
10	97	23	88	23

Step 1: Selects an initial value such as A and Q.

Step 2: Generates a random number.

Step 3: Computes $encode = (2000 - e - random\ \ number)(mod\ \ 128)$.

For example:

$encode = (2000 - e - random\ \ number)(mod\ \ 128)$
$encode = (2000 - 21 - 98)(mod\ \ 128)$
$encode = (1881)(mod\ \ 128)$
$encode \equiv 98(mod\ \ 128)$

According to the Table 2, we will show encode and decode status by random number. Any users just set initial value. In other hand, he can selects any random function. In this section, the random function is use by Visual Basic. The concept of diagram is shown in Figure 1.

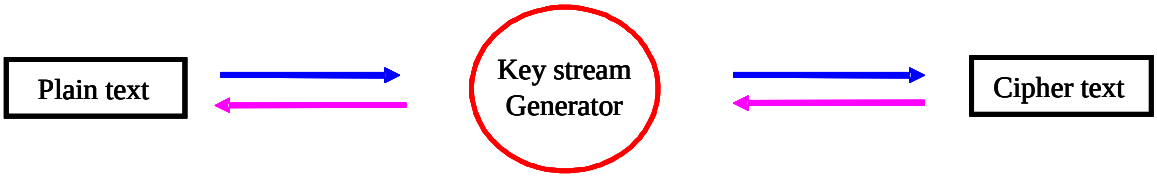

Figure 1. The file used by stream cipher to encrypt it.

3. Implementation Magic Square

A magic square is a square array of numbers consisting of the distinct positive integers 1, 2, …, n^2 arranged such that the sum of the n numbers in any horizontal, vertical, or main diagonal line is always the same number. The unique normal square of order three was known to the ancient Chinese, who called it the Lo Shu. A version of the order-4 magic square with the numbers 15 and 14 in adjacent middle columns in the bottom row is called Dürer's magic square. Magic squares of order 3 through 8 are shown as following.

8	1	6
3	5	7
4	9	2

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

17	24	1	8	15
23	5	7	14	16
4	6	13	20	22
10	12	19	21	3
11	18	25	2	9

32	29	4	1	24	21
30	31	2	3	22	23
12	9	17	20	28	25
10	11	18	19	26	27
13	16	36	33	5	8
14	15	34	35	6	7

30	39	48	1	10	19	28
38	47	7	9	18	27	29
46	6	8	17	26	35	37
5	14	16	25	34	36	45
13	15	24	33	42	44	4
21	23	32	41	43	3	12
22	31	40	49	2	11	20

64	2	3	61	60	6	7	57
9	55	54	12	13	51	50	16
17	47	46	20	21	43	42	24
40	26	27	37	36	30	31	33
32	34	35	29	28	38	39	25
41	23	22	44	45	19	18	48
49	15	14	52	53	11	10	56
8	58	59	5	4	62	63	1

Figure 2. Magic Square of order 3 through 8. [23]

In this article, we first proposed new conception use by magic square to embed in a random access file with stream cipher. The random access file is kind of sequence data that is one dimension serial in storage. Thus, it is easy implant magic square from file fill the contents. Block cipher is enciphering the data into blocks.

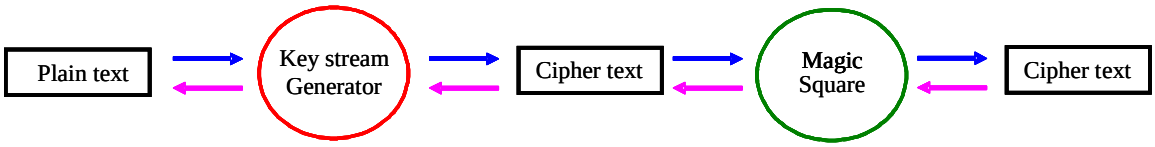

Figure 3. A file embedded stream cipher with magic square.

3.1 Implant Phase

Step 1: Select N dimension magic square.

Step 2: Choose a file, which it could be encrypt.

Step 3: Read the file into memory, and translate the sequence, according to the magic square location.

Step 4: Repeat the step 3 until the end of file.

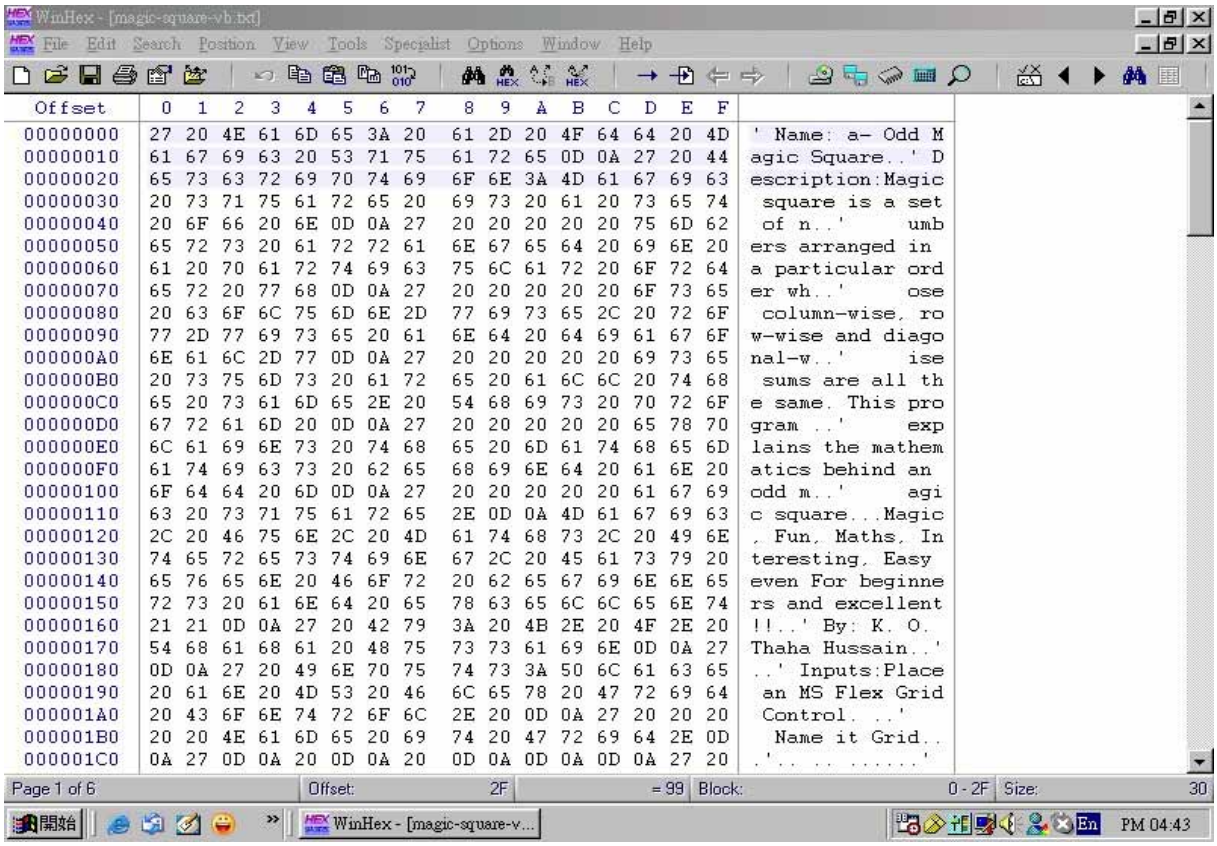

Figure 4. A source file content is shown on hexadecimals code.

Table 3. The size of 5 * 5 Matrix.

17	24	1	8	15
23	5	7	14	16
4	6	13	20	22
10	12	19	21	3
11	18	25	2	9

3.2 Restore Phase

Step 1: Rewrite the file while it had reallocated the position.

Step 2: Compare the original file and encrypted file.

As we know, the table 3 is 5 * 5 matrix. It is clearly to get the order of elements located on the position. Here, we

through the matrix to reorder a file. Therefore, this file is encrypted. It is a kind of block cipher actually. Figure 3 is source file that it is not encrypt. Table 4 is a file implanted magic square procedure. All of procedure will include stream cipher and magic square. Of course, it can choose one or two way to protect files. However, the magic square and stream cipher are independence each other. User just selects his demand for the file often.

Table 4. A file implanted Magic Square.

61	75	27	20	20
71	6D	3A	64	4D
61	65	64	63	53
2D	4F	69	20	4E
20	67	61	20	61

4. Security Analysis

In this paper, we used dual mode to protect our data, one is stream cipher and others is magic square.

4.1 Magic Square

We proposed random access file used by stream cipher embedded magic square first. In our scheme, the magic square mean for normal type. If users want encrypt his data by normal magic square. We opinion the orders have to above five. An order four normal magic square has 880 types. However, it is over 275305224 types of order 5. Therefore, they choose higher order that get more safety actually. Most kind of magic square is shown on Append 1.

4.2 Stream Cipher

If attack get the parameter e, then he is hard to computes parameter E. Attacker has to face Quadratic Residue problem. If p is a prime, then it is easy to decide whether $e \in \mathbb{Z}_p^*$ is a quadratic modulo p since, by definition, $e \in Q_p$ if and only if $(\frac{a}{p})=1$, and the Legendre symbol $(\frac{a}{p})$ can be efficiently get by definition.

5. Conclusion

Stream ciphers are generally faster then block ciphers in hardware, and have less complex hardware circuitry. They are also more appropriate, and in some cases mandatory (e.g., in some telecommunications applications), when buffering is limited or when characters must be individually processed as they are received. Because they have limited or no error propagation, stream ciphers may also be advantageous in situations where transmission errors are highly probable.

6. References

[1] 楊吳泉，現代密碼學入門，全華科技有限公司，1997 年，11 月，初版二刷

[2] 賴溪松、韓亮、張真誠，近代密碼學及其應用，松崗電腦圖書資料股份有限公司，1999 年，11 月，初版六刷

[3] Asker-Ali Abiyeva, Adil Baykaso glub, Turkay Derelib, I. Huseyin Filizc and Azer Abiyevd, 'Investigation of center of mass by using magic squares and its possible engineering applications', Robotics and Autonomous Systems, Vol.49, 2004, pp.219-226.

[4] Bart Prened, 'State of the art cipher for commercial applications', Computers and Security, Vol.18, 1999, pp.67-74.

[5] Bruce Schneier, 'Applied Cryptography：Protocols, Algorithms and Source Code in C', John Wiley and Sons Inc. 1994.

[6] Bruce W. Westbury, 'R-Matrixes and the magic square', Journal of Physics A: Mathematical and General,Vol. 36, 2003, pp.1947-1959.

[7] C.H. Barton and A. Sudbery, 'Magic squares and matrix models of Lie algebras', Advances in Mathematics,

Vol.180, 2003, pp.596-647.
[8] Changho Seo, Sangjin Lee, Yeoulouk Sung, Keunhee Han, and Sangchoon Kim, 'A Lower Bound on the Linear Span of an FCSR', IEEE Transaction on Information Theory, Vol. 46, No. 2, March 2000.
[9] D. M. Collison, Algorithm 117-118 Magic Square (Even and Odd Order), Communication of ACM, pp.435-436.
[10] Ezra Brown, 'Magic Squares, Finite Planes and Points of Inflection on Elliptic Curves', The College Mathematics Journal, The Mathematical Association of America,Vol. 32, No. 4, September 2001, pp.260-267.
[11] Frank. Emmerich, 'Equidistribution properties Of Quadratic Congruential Pseudorandom Number', Journal of Computational and Applied Mathematics, Vol. 79, 1997, pp.207-214.
[12] J. M. Landsberg and L. Manivel, 'The Projective Geometry of Freudenthal's Magic Square', Journal of Algebra, Vol. 239, 2001, pp.477-512.
[13] Jorge. Jimenez Urroz, 'Note Congruence For The Partition In Certain Arithmetic Progressions', Discrete Mathematics, Vol. 211, 2000, pp275-280.
[14] Jovan Dj. Golic, 'How to Construct Cryptographic Primitives Stream Ciphers', Computer & Security, Vol. 20, No. 1, 2001, pp.79-89.
[15] Jovan Dj. Golic, 'Stream cipher encryption of random access files', Information Processing Letters, Vol.69, 1999, pp.145-148.
[16] L. Blum, M. Blum and M. Shub, ‘A Simple Unpredictable Pseudo-Random Number Generator,’ SIAM Hournal n Computer, Vol. 15, No. 2, 1986, pp.364-383.
[17] Michael. Mascagni, 'Parallel Linear Congruential Generators With Prime Model, Parallel Computing, 1998, pp.923-936.
[18] Paul Camion, Miodrag MihaljeviC and Hideki Imai,'On Employment of LFSRs over GF(q) in Certain Stream Ciphers', ISlT 2002, Lausanne, Switzerland, June 30 -July 5, 2002
[19] S. J. Shepherd, 'Public Key Stream Cipher', IEE Colloquium on Security & Cryptography Applications to Radio System, Savoy Place, London , 3 June 1994.
[20] Thomas R. Hagedorn, 'Magic rectangles revisited', Discrete Mathematics, Vol. 207, 1999, pp.65-72.
[21] Thomas R. Hagedorn, 'On the existence of magic n-dimensional rectangles', Discrete Mathematics, Vol. 207, 1999, pp.53-63.
[22] Zhu Jiacheng, Sun Rongguo, Cheng Murong, 'A construction of addition-multiplication magic square of order 18', Journal of Statistical Planning and Inference, Vol. 51, 1996, pp.331-337.
[23] Walter Trump, ‘Number of magic squares’, http://www.trump.de/magic-squares/howmany.html
[24] Magic Square, http://mathworld.wolfram.com/MagicSquare.html

Append 1 How many magic squares are there? [22]

Order	semi-magic (A)	normal (B)	associative (C)	pandiagonal (D)	ultramagic (E)
3	**9**	**1**	**1**	**0**	**0**
4	**68 688**	**880**	**48**	**48**	**0**
5	**579 043 051 200**	**275 305 224**	**48 544**	**3 600**	**16**
6	**9.4597** (13) $\cdot 10^{22}$	**1.775399** (42) $\cdot 10^{19}$	**0**	**0**	**0**
7	**4.2848** (17) $\cdot 10^{38}$	**3.79809** (50) $\cdot 10^{34}$	**1.125151** 51) $\cdot 10^{18}$	**1.21** (12) $\cdot 10^{17}$	**20 190 684**
8	**1.0804** (13) $\cdot 10^{59}$	**5.2210** (70) $\cdot 10^{54}$	**2.5228** (14) $\cdot 10^{27}$	**C8 + ?**	**4.677** (17) $\cdot 10^{15}$
9	**2.8997** (69) $\cdot 10^{84}$	**7.8448** (38) $\cdot 10^{79}$	**7.28** (15) $\cdot 10^{40}$	**81·E9 + ?**	**1.363** (21) $\cdot 10^{24}$
10	**1.477** (29) $\cdot 10^{115}$	**2.4160** (35) $\cdot 10^{110}$	**0**	**0**	**0**