Int. J. Communications, Network and System Sciences, **2012, 5, 850-853**
http://dx.doi.org/10.4236/ijcns.2012.512090 Published Online December 2012 (http://www.SciRP.org/journal/ijcns)

Improvement of the Round Key Generation of AES

Junshe Wang, Han Xu, Mingqiu Yao
Department of Communication and Information System, Hebei University of Science and Technology, Shijiazhuang, China
Email: kingkaiser@163.com

Received August 13, 2012; revised September 27, 2012; accepted November 10, 2012

ABSTRACT

The key generation algorithm of AES was introduced, the weaknesses of the key generation design of AES were investigated. According to the key demand put forward a kind of new design idea, and this designing strategy was developed, which can be used to improve the key generation algorithm of AES. An analysis shows that such improvement can enhance the safety of the original algorithm without reducing its efficiency.

Keywords: AES; Data Encryption Standard (DES); Key Generation; Rijndeal

1. Introduction

In modern society, computer network has already been covered. In people's daily lives, the information technology industries have become ubiquitous. In the civil and military, commercial's security which is playing an important role is very prominent [1]. Therefore, the importance of information security has been paid more and more attention. Encryption technology as an important field of information security technology, which is widely considered as the most effective means to ensure information security. Because of advances in computer technology and the needs of reality, the cryptology had the development which progresses by leaps and bounds. In the field of block ciphers, DES was already unable to satisfy requirements of the security, the United States had collected and selected the Rijndael algorithm as the new Advanced Encryption Standard (Advanced Encryption Standard = AES). Compared with 3DES, the security of the AES algorithm is better, AES Algorithm is more simple and flexible.

First, algorithm of AES is based on group encryption algorithm. Algorithm including massive shifting algorithm, and the shift operation belongs to the time instruction. It cannot conduct simultaneously with other instructions, and reduces the efficiency of the algorithm. Second, the rounds of encryption using a loop operation, cyclic operation may cause the instruction block, so the instruction. Therefore, the paper made the improvement slightly in the AES algorithm foundation, and reduced shift operation and improved the round key, thereby reducing the encryption and decryption without the premise of improving the efficiency of its security.

2. Encryption Algorithm Round Transformation

The AES encryption algorithm's main body is the encryption round the transformation round transformation includes mainly ByteSub, ShiftRow, MixColumn and AddRoundKey.

A. ByteSub transformation

It is each byte in the state which is transformed by ByteSub instead of s-boxes transformation. This transformation made up of two steps:

1) Multiplicative inverses of each byte in the State.

2) The results which is obtained by (2) to (1) do transformation $y = f(x)$.

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

B. ShiftRow transformation

ShiftRow transform the line of state which increasing the offset of circulation moves left, first line unchanged, second line loop left 1 byte, third line loop left 2 bytes, fourth line loop left 3 bytes.

C. MixColumn transformation

MixColumn transformation makes confuse transforms to columns in the state. In MixColumn transformation, the data of state column as 32-bit, and then carries on the

matrix multiplication transformation to it:

$$Sj'(x) = c(x) \cdot Sj(x) \quad (1)$$

$$c(x) = 0.3x^3 + 0.1x^2 + 0.1x + 0.2 \quad (2)$$

D. AddRoundKey transformation

The AddRoundKey transformation let each byte in state and the round sub-key corresponding to the byte XOR, the value of the AddRoundKey transformation are the result of state. The round key transformation in pseudo C code represented as follows:

```
Round(State,Roundkey[i]){
ByteSub(State);
ShiftRow(State);
MixColumn(State);
AddRoundKey(State,Roundkey[i]);
}
```

3. Key Analysis of the AES Encryption Algorithm

The AES algorithm expands directly the seed key to get the keys. And each 32 bit word k_i and k_{i-1} and k_{i-4} are related, in other words, if it obtained k_{i-4} and k_{i-1} can obtain k_i. Similarly, if it knew k_i and k_{i-1} may obtain k_{i-4}, knew k_i and k_{i-4} may obtain k_{i-1}. Although, each round word which produces in a round key can be carried on by 4 integral multiples the complication, the correlation of key generation cannot be changed by this kind of the complication. Suppose, a round of the AES key k_i, k_{i+1}, k_{i+2}, k_{i+3} is known now. Then, it may be through k_{i+1}, k_{i+2} obtain k_{i-1}, through k_{i+1}, k_{i+2} obtain k_{i-2}, through k_i, k_{i+1} obtain k_{i-3}, through k_{i-1}, k_i obtain k_{i-4} again, the preceding round of the round keys of all sub-keys have been obtained. It also through k_i, k_{i+3} obtain k_{i+4}, through k_{i+1}, k_{i+4} obtain k_{i+5}, through k_{i+2}, k_{i+5} obtain k_{i+6}, through k_{i+3}, k_{i+6} obtain k_{i+7}, and then get the last round keys.

The above key generation process is analyzed to get the following properties:

Nature 1: Direct expansion of the key enables itself to have highly effective;

Nature 2: The preceding round key is only replied by the generation of the new key, the generation of the new key can participate encryption and decryption, immediately [2]. Therefore, the generation algorithm of the key has timeliness;

Nature 3: If one of the round keys is obtained by the aggressor then the complete seed key will be obtained by the aggressor. Namely: The sub-key and the seed key had the relevance.

Security of the key generation algorithm is reduced by the nature 3. AES has the high efficiency of the nature 1, the main reason is the seed key which is conducted on the basis of the direct expansion. The latter round key is obtained by the preceding round key, through the first round of the key as the seed key. Generally speaking, since the latter round key can be promoted by preceding round key, preceding round key is obtained by the latter round key, this is the reason which the nature 3 appears [3].

4. Algorithm Improvements

A. 44 *keys are generated by dispatching*

The AES algorithm's 128 seed key is produced by using 44 sub-keys. First, the seed key was divided into four words: k_0, k_1, k_2, k_3, the remaining sub-keys are produced by using a scheduling algorithm in **Figure 1**.

And F is: 32 byte position rotate left one byte. Namely: RotByte(a,b,c,d) = (b,c,d,a).

B. Cipher

The function cipher is the real McCoy, doing the actual encryption of the 16 byte long input vector of plaintext into the output ciphertext vector ai illustrated in **Figure 2**. Further input parameters of the vipher, that have been created by the initialization function aes_init are the substitution table s-box, the key schedule w, and theological matrix poly_mat. [4]

The cipher rearranges the plaintext vector into the state matrix and iteratively loops the state through add_round _key, sub_bytes, shift_rows, and mix_coulumns.

C. The new algorithm's advantage—Round Keys Exchange

Take 10 round AES algorithm as the example, the initial 4 words seed key expands to 44 word sub-key. Among them, Key dependent relationship for: k_i depends on k_{i-1} and k_{i-4} $(i = 4,5,\cdots,43)$. First, it generates the original key. Then, 40 words sub-keys generated by the seed key and the gradual transformation as **Figure 3**.

Taking 2nd round and the 3rd round key as a group, Exchange k_7 and k_9;Taking 4th round and the 5th round key as a group, Exchange k_{15} and k_{17}; Taking 6th round and the 7th round key as a group, Exchange k_{23} and k_{25}; Taking 8th round and the 9th round key as a group, Exchange k_{31} and k_{33}; Taking 10th round and the 11th round key as a group, Exchange k_{39} and k_{41}; After exchanging 44 words sub-key, It still takes 4 words as new round of all 11 round. Take 2nd round and 3rd round new sub-key as the example, it analyzes the correlations of each round key after the exchange. Before the exchange, it may derive the 3rd round key through the 2nd round key, it may also derive the 2nd round key according to the 3rd round key [5]. 2nd round of keys become k_4, k_5, k_6, k_9 and 3rd round of keys becomes k_8, k_7, k_{10}, k_{11} after exchange the 8th word and the 10th word. Then re-use the relationship between them, it can only through the 2nd round key obtain the 3rd round

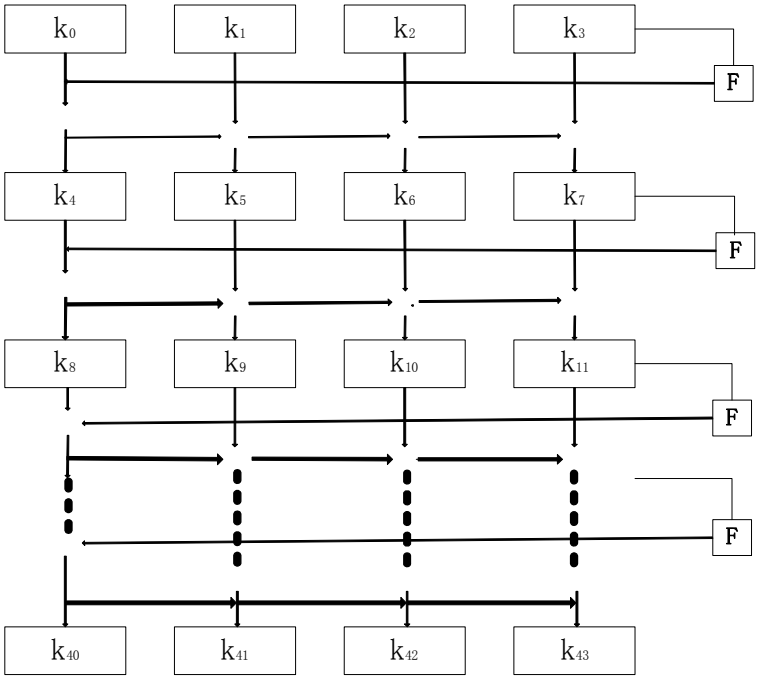

Figure 1. Wheel key generation.

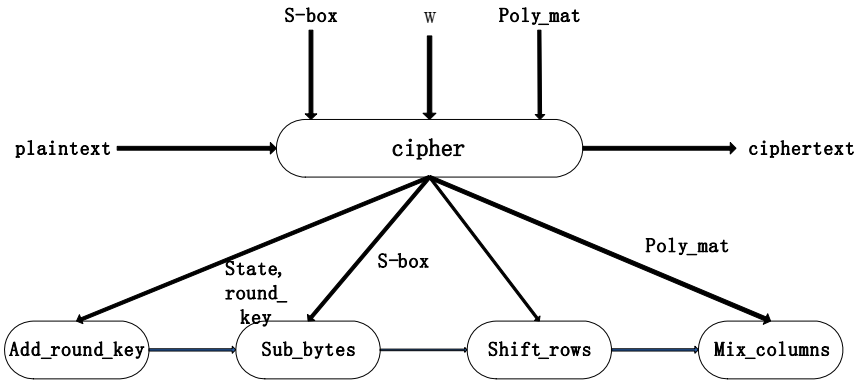

Figure 2. Encryaption funtion cipher.

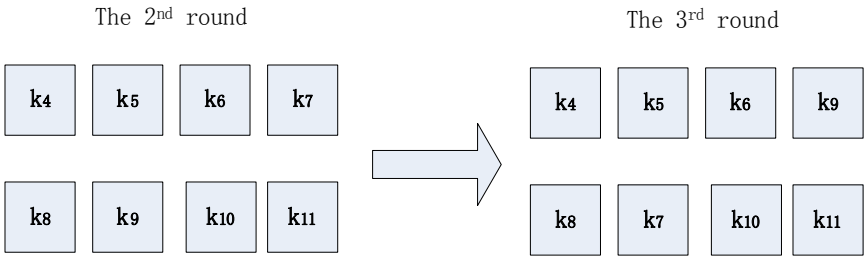

Figure 3. Column hybrid transformation.

key k_8 and through the 3rd round key can only obtain a 2nd round key k_4.

It cannot obtain the preceding round sub-key completely through the generation algorithm if the aggressor obtains one of the new round sub-key. It maintains basically high speed of the original algorithm in the performance because of increasing just 5 times in exchange in the original algorithm, and improving the security of the algorithm. Such improvements cannot avoid the correlation between each round key completely because of obtaining one word of each round key, but it enhanced security of the original algorithm actually [6]. It is the method that

the sub-key for the key rotation when produces two new round sub-key every time, therefore, the nature 2 (real-time) of the original AES algorithm have not been destroyed by improving the algorithm, and it has not reduced the efficiency to strengthen security of the original algorithm [7].

D. New algorithm encryption experiment

The new improved algorithm is simulated by using matlab. Cipher the **Figure 4** completely, which obtains the encryption documents of **Figure 4**.

In the **Figure 5**, it is a result of the cipher of the improved algorithm and the original algorithm. It can see directly, the improved algorithm is more complex than the original algorithm(the black spots are more crowded). Response time of the two algorithms program as the following table (see **Table 1**).

Figure 4. The picture of original.

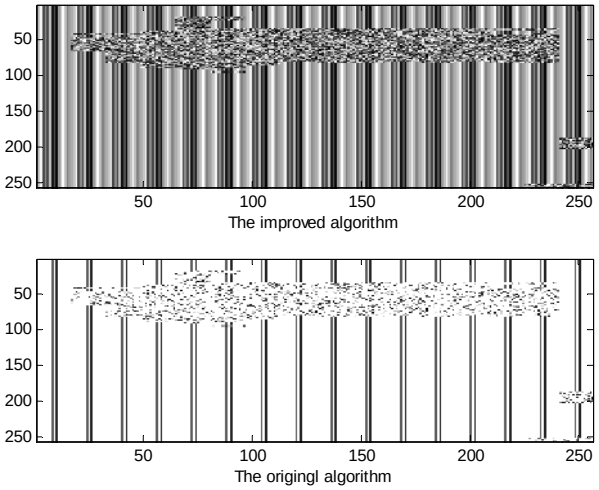

Figure 5. The picture of cipher.

Table 1. Response time.

Time algorithm	First (second)	Second	Third	Fourth
Original	62.79114	62.39147	62.23511	62.46756
Improved	62.34567	62.36778	62.23468	62.87953

The table can be seen, response time of the original algorithm is 62.23511 to 62.79114, response time of the improved algorithm is 62.87953 to 62.67890 (second).

5. Summary and Outlook

It improves sub-key of the original production algorithm through research of the key production algorithm and demand consideration, to strengthen the security of the original algorithm without reducing efficiency. Algorithm improvement extracts from many merits of improvement algorithm when found one method to strengthen the security of the original algorithm without reducing efficiency.

It is unidirectional strategy that the previous round key has only been produced under the emphasis by the next round key. Although this kind of strategy which research in the AES algorithm is put forward, it also can be used with other groups of the production key as a design thought. This algorithm will also be studied further in the future.

REFERENCES

[1] N. Ferguson, J. Kelsey, B. Schneier, *et al.*, "Improved Cryptanalysis of Rijndael, Selected Areas in Cryptography 2008," 2009.

[2] E. Tittel, M. Chapple and James, "The Authentication Information System Security Experts Holographic Tutorial CISSP: Certified Informa," Publishing House of Electronics Industry, Beijing, 2008.

[3] Z. H. Yang, "Testing Efficiency of Encryption Network Security: Theory and Practice," 2008.

[4] J. Daemen and V. Rijmen, "AES Proposal: Rijndael (Version 2)," 2005.

[5] J. Daemen and V. Rijmen, "The Design of Rijndael: AES—The Advanced Encryption Stand," Springer-Verlag, Berlin, 2002.

[6] J.-S. Cui and H.-G. Zhang, "MARS Algorithm—Candidate of Advanced Encryption Standard," *Communication Security*, Vol. 22, No. 2, 2000, pp. 59-66.

[7] B. Yang, "Modern Cryptology," Publishing House of Tsinghua University, Beijing, 2009.

