An Improved AES Key Expansion Algorithm

Junjie Yan* and Feng Chen
School of Information Science and Technology, University of Science and Technology of China, Hefei, Anhui, 230027, China
*Corresponding author

***Abstract*—Advanced Encryption Standard (AES) has been widely used in wireless communications with advantage of the small amount of computation and fast speed. In order to overcome the drawback of typical expansion algorithm whose key is easily attacked by Square, an improved AES algorithm is proposed. In this algorithm, the double S-box model, the only non-linear structure, is employed to increase the diffusivity of data. Experimental results indicate that this AES algorithm can improve the security of the key in the same condition of algorithm efficiency.**

Keywords-advanced encryption standard; key expansion; square; double S-box

I. INTRODUCTION

With the development of information technology and increasing demands for information security, the encryption methods have been attracted more and more attention in recent years. Existing encryption systems are divided into three types such as symmetric encryption, asymmetric encryption, and Hash algorithms.

DES and AES are the most popular symmetric encryption method [1]. And they are high effective and suitable for large chunks of data transmission. AES was accepted as a new generation of encryption standard in 2000, and it has been widely used in the world.

AES key expansion algorithm can get the round key by the initial key for the encryption and decryption processes. The fast algorithm has advantage that the generated extended key can be used in encryption in time. However, its main drawback is that one can deduce all the keys with any round key. In allusion with this problem, Wang et .al.[2] proposed a double key algorithm. In this algorithm, a new key, irrelevant to the initial key, is used to fill the first round key, and then carries out key expansion. This algorithm is equivalent to these schemes that increase the length of the key. The algorithm proposed by Wang can improve data security, but it increases the difficulty of key management.

In Literature [3] method, a round key is obtained by adding two adjacent round keys. It ensures that two adjacent round keys cannot be deduced by one round key. But data security has not been improved. An improved algorithm is proposed in Literature [4]. One round key as the random function seed is used to generate the next round key. The data security is guaranteed. However, this method is inefficient and difficult to realize simultaneously implementation in both ends of the encryption.

Difference to these schemes as above, this paper presents an improved AES key expansion algorithm. This algorithm calculates the extending key by introducing a double S-box. It enhances both the diffusibility of data and data security.

II. AES ALGORITHM DESCRIPTION

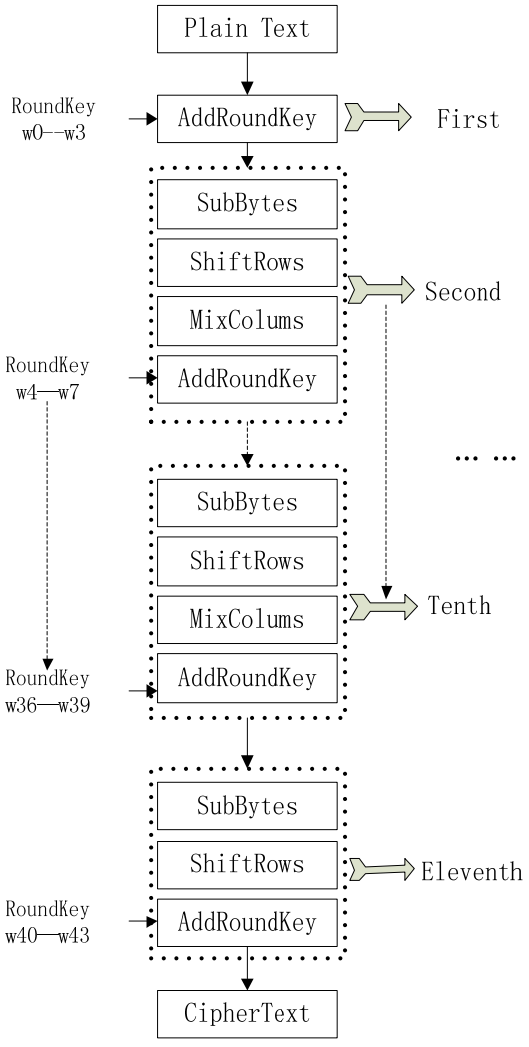

FIGURE I. AES ENCRYPTION ALGORITHM

Rijndael algorithm is based on an iterative block cipher principle, which has a variable block of data and key length. Packet length and key length can be specified as 128 bits, 192 bits, and 256 bits respectively. In the AES specification, the length of the key may be one of the three, but the packet length

only is 128. In this work, we focus on the AES-128 bit. A brief introduction to the encryption structure is given in the following.

AES is an iterative encryption algorithm with data bock and a variable key. Data block need multiple rounds of transformation and the intermediate results are called states. Various transformations are based on states. The initial input of the text is called the initial state [6]. The key seed is the initial key of AES, which is used to generate the desired key. In equation (1), N_b is the number of words in plain text, N_k is the number of words in secret key, and N_r denotes represents the number in rounds of the algorithm. N_r is determined by both N_b and N_k in equation(1).

$$N_r = \max\{\frac{N_b}{32}, \frac{N_k}{32}\} + 6 \tag{1}$$

AES algorithm encryption process is shown as Figure I. It is mainly composed of 4 transformations including Sub Byte (BS), Shift Row (SR), Mix Column (MC) and Add Round Key (AK)[6]. The main composition is round transformation. The last round has no MC which operates each column in the state independently.

The BS transformation is to replace each byte in a state by checking the S-box. It consists of two processes: 1) calculating the multiplicative inverse of each byte of state in finite field $GF(2^8)$; 2) taking affine transformation pair $(F1, 63)$ for example, affine transformation is carried out in finite field $GF(2^8)$ of multiplicative inverse in the following:

$$\begin{aligned} y_i = {} & x_i \oplus x_{(i+4) \bmod 8} \oplus x_{(i+5) \bmod 8} \oplus \\ & x_{(i+6) \bmod 8} \oplus x_{(i+7) \bmod 8} \oplus c_i \end{aligned} \tag{2}$$

This operation is equivalent to the matrix transformation, in equation (3) follows:

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \\ X_5 \\ X_6 \\ X_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \tag{3}$$

Where, c_i is the I bit in number of c(0x63),and its binary form is $(c_7 c_6 c_5 c_4 c_3 c_2 c_1 c_0) = (01100011)$.

The SR transformation is to transpose the bytes in the state. It is that one byte is moved from one column to another with multiple of four byte linear distance, which ensures that the four bytes of a column can be extended to different columns. The first line remains the same, the second row moves to left one byte, the third row moves to left two bytes, and the fourth rows move to left three bytes. The reverse transformation is that the first line remains unchanged and the other three rows move to right.

The MC transform is that a unit with 32 bytes in a column multiplies by a polynomial $c(x)$, and then performs modulus by $(x^4 + 1)$.

$$c(x) = 03x^3 + 01x^2 + 01x^1 + 02 \tag{4}$$

Each byte associates with other 4 bytes in current column for states. This is transformation can be also represented by matrix multiplication in equation (5). Decryption process uses the inverse matrix of $c(x)$.

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} \tag{5}$$

The AK transformation XOR the round keys with a state: $s_{i,j} \oplus k_{i,j} = s'_{i,j}$. The key expansion algorithm is the core of AES.

We can get four 32bits w_0, w_1, w_2, w_3 words from the initial key in the column.

$$w_i = w_{i-4} \oplus g(w_{i-1}) \text{ For } i = 4, 8, \ldots, 40$$

$$w_i = w_{i-4} \oplus w_{i-1} \text{ For } i = 5, 6, 7, 9, \ldots, 43$$

In turns, we can get 44 extended keys. g is one of the most important parts of the key expansion. First, w moves to left one byte and performs BS transformation. Then it performs XOR with RCON constant. The cipher text has the same length as the plain text.

III. KEY EXTENSION ALGORITHM IMPROVEMENT

Square Attack proposed in the literature [7] is the process of Speculation and determining sub-key. When the round key expansion algorithms are relatively simple, they may be attacked easily. The attacking processes of different Squares are similar. Because the attack on AES of five rounds and six rounds is based on attack on AES of four rounds, an introduction to the attack on AES of four rounds is given as follows. (These attack process are described in detail in the literature [8].)

Λ set is a group of plain text which has fifteen same data and 256 possible values in the last byte. State produces another set after BS and AD with active byte position unchanged, and produces another after SR, and may produce another after MC. We analyze the state according to the AES by round transformation. The SR transformation makes no effect, and the MC make the only active byte spread to an active byte column in first round. The SR make the only active column spread to four column, and the MC make the one active byte spread to sixteen bytes in second round. So after the SR and MC of third round transformation, the relationship between input a and output b is as follows:

$$\begin{aligned}
&\bigoplus_{b=MC(a),a\in\Lambda} b_{i,j} \\
&= \bigoplus_{a\in\Lambda}(02a_{i,j} \oplus 03a_{i+1,j} \oplus a_{i+2,j} \oplus a_{i+3,j}) \\
&= 02 \bigoplus_{a\in\Lambda} a_{i,j} \oplus 03 \bigoplus_{a\in\Lambda} a_{i+1,j} \oplus \bigoplus_{a\in\Lambda} a_{i+2,j} \oplus \bigoplus_{a\in\Lambda} a_{i+3,j} \\
&= 0 \oplus 0 \oplus 0 \oplus 0 \\
&= 0
\end{aligned} \tag{6}$$

All bytes are balanced at this time. In the fourth round, the value of the key suspected is verified by the above formula, and then the initial key can be derived by the extended key algorithm. So the key expansion algorithm is important to safety, then we analyze the typical algorithms and propose an improved algorithm.

The scheme proposed by literature [2] can indeed enhance the security of the encryption algorithm, but it increase the length of the key and has no improvement in the process of encryption. The scheme proposed by literature [3] ensures that adjacent two round keys cannot be deduced by one round key. But it is problematic if one gets adjacent two round keys. The scheme in literature [4] can guarantee the security but it is difficult to synchronous implementation in the ends of the encryption.

Difference to the algorithms as above, we propose an improved key expansion algorithm. It can increase the diffusivity of data with double S-box that is the only nonlinear structures. The new key expansion is shown in Figure 2.

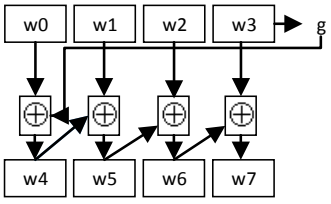

FIGURE II. KEY EXPANSION ALGORITHM

The formula is as follows:

$$\begin{aligned}
W_i &= W_{i-4} \oplus g(W_{i-1}) \\
W_{i+1} &= W_{i-3} \oplus W_i \\
W_{i+2} &= W_{i-2} \oplus W_{i+1} \\
W_{i+3} &= W_{i-1} \oplus W_{i+2}
\end{aligned} \tag{7}$$

In the equation (7), we can compute one element with another two elements and deduce adjacent two round keys by AK process. In view of simple structure, we put forward a new Key expansion algorithm.

$$\begin{aligned}
W_i &= W_{i-4} \oplus W_{i-3} \oplus W_{i-2} \oplus g(W_{i-1}) \\
W_{i+1} &= g'(W_i) \oplus g(W_{i-1}) \\
W_{i+2} &= W_{i+1} \oplus W_i \\
W_{i+3} &= W_{i+2} \oplus W_{i+1}
\end{aligned} \tag{8}$$

When we get a sub key and deduce the last round key, only w_i, w_{i+1} are available. But we still can't get the w_{i-1}, which is dependent on the nonlinear of S-box. In function g', we selected the improved S-box that is more close to the strict avalanche criterion. It is similar to classical S-box in balance, uniform, nonlinear structure, nonlinearity and algebraic attack against resistance etc. Cracking g' and g need the same cost. Brute forcing is the only way to deduce the $w_{i-2}, w_{i-3}, w_{i-4}$.The difficulty to get the last round key is 2^{128} and to get the next round key is 2^{64}. It has the same computation difficulty with the brute force after two round processing, and improves the safety with no obviously increase of computation.

Compared with the related methods in literature [2], [3] and [4], our scheme can ensure each round key has consistent security. Meanwhile, it does not increase the key length. Even if one knows two adjacent round keys, he still can't get the next or the last round key. The improved key expansion algorithm maintains the same property that the round key depends on last round only, and round seed key and key have the same security. The improved algorithm still has high efficiency due to just adding a function mapping process and two XORs. Square attack is the process of Speculation and determining sub-key. So when the key expansion algorithm is relatively simple, the resistance on square attack is quite weak.

IV. EXPERIMENTAL ANALYSIS

Diffusion and confusion are two basic methods for the design of cryptographic system, whose purpose is to resist the opponent's statistical analysis of cryptosystem. The so-called diffusion is that each bit in plain text can impact on a number of bits in cipher text, which can conceal statistical properties of the plain text. We select a 128 bit string to encrypt, and ensure that the key is constant, and change the bits in plain text increasingly to obtain number of change in cipher text. Table 1 shows the experimental result generated by three random groups of data, which indicates that the improved algorithm has more stable diffusivity.

TABLE I DIFFUSION EXPERIMENT

Plain changed / Cipher changed	One	Two	Three	Four
AES	64	63.5	60.5	61
Improved AES	64.5	62	64	65

In order to get the corresponding operation effects，we encrypt and decrypt 1024-bit string and record the running time on the test platform whose main frequency is 220Mhz and memory is 128M. From table 2, we can see that the improved algorithm meets the safety requirement without decreasing efficiency at the same time.

TABLE II RUNNING TIME

Time (Ms)	AES		Improved AES	
	encrypt	*decrypt*	*encrypt*	*decrypt*
First	588	611	588	615
Second	585	620	591	614
Third	582	613	586	621
Forth	584	618	585	614
Fifth	583	620	589	615
Average	584	616	587	615

V. CONCLUSION

In this paper, we discuss the classical AES encryption algorithm and its extended versions. An improved Key extension algorithm is proposed to improve the process of generating the sub-key with introducing a double S-box. This algorithm enhances data diffusion and security in condition of almost the same processing efficiency.

REFERENCE

[1] Yixian Yang, Xinxin Niu. Applied cryptography [M]. BeiJing : Beijing University of Posts and Telecommunications Press, 2005:44-46.

[2] Xinggang Wang. Design of encryption chip based on RSA and AES hybrid algorithm [D]. JiNan: University of Jinan, 2011.

[3] Shao rong Yuan, Min Xie, Weibin Li, Jianchao Du.A Beidou navigation and positioning information system based on improved AES key expansion algorithm. 2015.

[4] Xiaodong Yang, Yi Wang. New method of AES key expansion[J]. Microelectronics and computer, 2012, 29(1): 102-104,108.

[5] Nechvatal J, Bassham E, Bassham L. Report on the Development of the Advanced Encryption Standard [J]. Res National Institute of Standards and Technology, 2000, 106(3):511-577

[6] National Institute of Standards and Technology(NIST). FIPS PUB 197 Advanced Encryption Standard [S]. US: Federal Information Processing Standards Publications, 2012

[7] Daemen J. and Rijmen V.AES Proposal:Rijndael.

[8] Joan Daemen, Vincent Rijmen. The Design of Rijndael AES: The Advanced Encryption Stand [M]. Berlin: Springer-Verlag, 2002:48-54

[9] Lianhao Liu, Jie Cui, Shangli Liu, Hongbo Ma. An improved scheme design for AES S-box [J]. Journal of Central South University: Natural science edition, 2007,38(2): 339-344.