Improve the Privacy of AES Encryption Algorithm in Cloud Computing

Heng Wang, Xinrui Chen

School of Electronics and Information Engineering, Jingchu University of Technology, Jingmen 448000, China

wanghengwh@126.com

Keywords: Privacy protection; Encryption algorithm; Inverse confusion operation; Row shift operation

Abstract: This article through to the symmetrical secret key and asymmetric contrast and secret key system requirements analysis identified on the basis of AES encryption mode choice, in describing the AES encryption principle introduced before AES encryption used knowledge of number theory, namely the finite field addition and multiplication algorithm. Through the next round of AES encryption of byte replace operation, line shift operation, columns, confusion and rounds of secret key addition operation phases one by one, mainly around the security of the AES ascension to improve. We through an 8 X 8 involution hadamard matrix column confusion to replace the original AES operation link used in the cycle of 4 * 4 matrix, so that the spread of the original branch number raised from 5 to 9, achieved better diffusion ability, at the same time also reduce the burden of the inverse confused column operation. The experiment proves that the enhancement of diffusion ability does not cause excessive time cost for encryption and decryption performance.

1. Introduction

With the improvement of the current Internet software and hardware performance, cloud storage has become one of the most widely used applications [1]. Using cloud storage technology, users can use different terminals to access data without restriction of space and time. The popularity of cloud storage apps such as DropBox, GoogleDrive, baidu, etc., is huge and growing fast. According to statistics, the number of DropBox users reached 175 million. Cloud storage provides users with convenient data storage functions, and also separates ownership and management rights of data. Cloud Service Provider is Cloud Service Provider (hereinafter referred to as CSP), which can search and use data uploaded to the Cloud by users [2]; At the same time, data in the cloud may be lost due to the data loss of the service provider's system. Some illegal attackers may also attack the cloud server to corrupt the user's data or steal the user's data. All these situations bring hidden trouble to the user's data security. So in order to protect the privacy of user data, before the data upload to encryption processing, the relevant data is in the use of cloud storage applications, the data encryption. There will be more problems to solve [3].

Boneh et al. proposed a searchable Public key encryption with keyword search in 2004, which USES bilinear pairs. However, this method has two known disadvantages: 1. Using public key encryption causes some attackers to guess the Keywords, and then use public key to verify; 2. The complexity of the query is linear with the number of documents, and the larger the document size, the worse the performance. In order to improve the performance and improve the efficiency of the algorithm, Aballa et al. have perfected PEKS [4]. Based on the current research results, a number of researchers have proposed various improvement programs based on PEKS, such as similarity retrieval, keyword retrieval, etc. [5]. However, because the public key is in the retrieval scheme, the computational complexity is too high to play a role in practice.

2. The AES algorithm

AES is a symmetric encryption algorithm for processing a 128-bit data block [6]. The length of the key currently supports three types, namely 128 bits, 192 bits, and 256 bits. Each encryption AES

  DOI: 10.25236/iwmecs.2019.065

algorithm need four steps in a bit of 4 x4 matrix, namely the first byte replacement, then line shift, then the column of confusion, finally add keys. In this step, the last three steps are linear, because the output block of 128 bits is a linear combination of the output bits, so these three steps are lower in the specific implementation difficulty.

And bytes of replacement is a unique nonlinear step, it is the input byte by applying the S box to replace operation, byte replace is 16 bytes of input block inverse operation, bytes of each element is ng Luo Huayu elements. This process is difficult to achieve, and in current circuit design, most use lookup Table method to implement the S box to realize the substitution of bytes.

Look-up Table method in the beginning is regarded as a relatively easy hardware implementation method, however, in the AES algorithm, using look-up Table method to realize the S box, there are some shortcomings, it will cause huge hardware overhead. This is because when using look-up Table method, the arbitrary Tables will need a 256 bytes of storage space, at this point, the bytes of input of 16 bytes are replaced, you need to 16 S box, if carry out 10 would need 160, greatly improving the hardware requirements.

3. Improved AES privacy protection encryption algorithm in cloud computing environment

The AES encryption algorithm is more and more concerned in the current research and application, and has been widely used in various encryption systems. Therefore, a lot of hackers and password interpreter began to attack, although so far have no effective way to crack, but in the choice of algorithm, to the safety performance for further consideration.

AES should meet the following principles of grouping codes in terms of security performance:

Principle of chaos: The secret key of the password should be confused with the clear text and ciphertext, so that the decryption of the password cannot be used to the relationship between them.

Diffusion principle: When making the design of the password, the secret key to affect to all of the bits of cipher text, as far as possible to address the possibility of the attacker to crack the password, and definitely will affect more than the ciphertext, to eliminate clear characteristics.

3.1 Improved AES algorithm diffusion performance.

In the AES encryption algorithm, use the S box instead of the chaos principle, the concrete operation is to use the operation of mixed column operation to realize the chaos. In the current improvement of AES encryption, most of the improvement in principle of diffusion.

For the standard of diffusion ability, in the academic circle, the diffusion branch number is the index, and the diffusion branch number is described as follows:

When setting F is encrypted byte vector linear transformation is expressed as $(F_{2^m})^n \to (F_{2^m})^n$, the number of non zero bytes in a way that is weight said: $W(\alpha)$ is zero bytes, and the number of branch when calculating linear transformation method is as follows:

$B(f) = \min_{\alpha \neq 0}(W(\alpha) + W(f(\alpha)))$, and $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n) \in (F_{2^m})^n$.

The transformation function used by the AES algorithm is $(F_{2^8})^4 / x^4 + 1$, and the reversible polynomial $c(x)$ used in the transformation satisfies $c_i \neq 0 | 0 \leq i \leq 3$, so the value of $W(\alpha)$ can only be taken from the set $\{1,2,3,4\}$.

$\alpha = [\alpha_0, \alpha_1, \alpha_2, \alpha_3]^T \in (F_{2^8})^4$、$f(\alpha) = [b_0, b_1, b_2, b_3]^T$

So $W(f(\alpha))$ =4, $W(\alpha) + W(f(\alpha)) = 5$; $W(\alpha) = i | 2 \leq i \leq 4$, $\alpha \neq 0$ $f(\alpha) \neq 0$, $W(f(\alpha)) \geq 1$, $W(\alpha) + W(f(\alpha)) \geq \mathrm{i} + 1$. The upper bound of the branch number satisfies $B(f) \leq n + 1 = 5$, so the branch interval of $(F_{2^8})^4 / x^4 + 1$ is [3,5]. When using AES, a simple reversible polynomial, $B(f) = 5$ is used to satisfy the maximum requirement of the diffusion layer.

3.2 Requirements for diffusion performance.

When the AES algorithm is in the operation of column confusion, the concept of the maximum

distance of the circulant matrix is used, which is as follows:

The (n,l,d) matrix generated by a linear code G satisfies $d=n-l+1$, (n is code length, d is code dimension). Matrix C in a limited domain for a maximum points on the $GF(2^8)$ code is 4 (6), the linear code generator matrix in $G=[I|C]$ piece on the right, in this linear code generator matrix I is a third-order unit matrix, without considering the left part, in order to card the encryption operation on the linear transformation matrix of the charge, and no to reduce the distance between the code word.Building a maximum distance separable code matrix is sufficient and necessary condition of optimal diffusion layer.

In this paper, the 8×8 size of the hadamard matrix is used to increase the original number of branches from 5 to 9, and its maximum linear separable code is (16,8,9). The following is the definition of the matrix:

In the n element $\alpha_0,\alpha_1,\cdots,\alpha_n$, the structure of each element in the hadamard matrix is $A_{i,j}=\alpha_{i\oplus j}$, in the finite field, it satisfies the condition $A^2=k\cdot I_n$, k is commonly used, when $k=1$, the matrix A is the matrix.

In the suiTable coefficient when the choice, use the following way:

Randomly selected 8 hexadecimal system first, according to the definition of hadamard matrix to the structure of the related, not zero when the input bytes can out of that part of the algorithm.

Using the above steps, output a set of hadammar coefficients {0103, 03, 04, 05, 06, 08,0, B,07}, and its corresponding construction matrix is as follows:

$$H=\begin{bmatrix}01,03,04,05,06,08,0B,07\\03,01,05,04,08,06,07,0B\\04,06,01,03,0B,07,06,08\\05,04,03,01,07,0B,08,06\\06,08,0B,07,01,03,04,05\\08,06,07,0B,03,01,05,04\\0B,07,06,08,04,05,01,03\\07,0B,08,06,05,04,03,01\end{bmatrix}$$

In AES encryption algorithm, the state of 16 bytes can be seen as a matrix, the algorithm of this paper, the confusion will be listed in the state of the information as a byte, and then use the byte and H multiplication, the result of the transformation, got a byte of matrix, and then enter the next step of the algorithm. Because H is a involutory matrix, carries on the reverse, is equal to its own, so in the column of confusion, can effectively reduce the complex circuit declassified filling, in order to reduce the hardware realization of encryption overhead.

3.3 Safety analysis

The improved algorithm improves both the diffusivity and the ability of the original algorithm to decode the code. This article will analyze the current mainstream password attack methods, as follows:

Violent attack: In this way, it needs to be cracked. In this complexity, the supercomputers are unable to complete the task, so the key is generally not available.

The difference attack method: The time consumption of this method and the amount of data is very large. In this way, the wide trajectory strategy used by the AES algorithm may protect it, requiring only sufficient rotation to make the difference trajectory less than.

Linear analysis: It mainly analyzes the S box structure, but the S box of AES is non-linear and the complexity is very high, so the security is better.

For now, the AES encryption mode can resist the current main attack technique. It at the beginning of the design is to consider a variety of means of attack, this consideration can be in every link of the design of operation as you can see, such as the S box makes inverse operation to construct the average distribution of the differential distribution Table, to protect the security of

data.

3.4 Improvement of AES scheme implementation.

If cloud data is encrypted using AES ways, first of all, based on the cloud service identification has been applied to the degree of the API interface, to the user's identifier to get the authorization in the service, the user then build pipeline operation, send the request of the data operation, then the process is as follows:

According to the secret key parameters selected by the user, a random secret key () is generated and the number of rounds is determined.

Use the extension function to extend the generated key and get an extended secret key;

A 16-byte grouping operation for the input data, for non-16-byte multiples, is filled with 0 bytes, then the original key and grouping state are performed;

Use the S box for Table replacement;

Four lines of shift;

The matrix of the obtained matrix is converted into a matrix form, and the obtained matrix is converted into a 4x4 state matrix once again by multiplying the hadamar matrix as described in this paper.

Take a wheel key in the extension key and do it;

When the number of wheels is less than n-1, jump to the fourth step, if equal, enter the next step;

Perform the fourth, fifth, and seventh steps to exit the algorithm.

After the completion of the steps in the algorithm, you can use the service provided by the API interface, the encrypted data will be uploaded to the cloud, to expand the generated secret key stored in the third party's secret key management center.

When the user requests to access data, the third word user management center can be found by the user to access the data storage, and then set up the data access connection channel, then perform the following steps:

The cloud service provider provides the download of the encrypted file, saves the file into the cache, and finds the corresponding secret key from the secret key management center.

A 16-byte grouping of ciphertext and then an operation to extend the key;

Carry out the retrograde shift;

Inverse S box substitution;

Take out the last round key of the key;

Matrix transfer;

When the number of wheels is less than n-1, jump step 3, otherwise enter the next step;

Exit algorithm after step 3, step 4 and step 5.

4. Simulation experiment and result analysis.

Currently, the hardware with AES algorithm is 8 bits or 16 bits. The Cpu has a 16-bit core, a primary frequency of 20MHz, and a 32Kb capacity flash memory. The simulation results of the experiment are as follows:

Table 1. Simulation results of AES encryption.

Operating segment	Cycle time	Number of rounds
Estimated link	2239	1
Make a byte substitution.	123	10
translocation	54	10
Make a list of confusion.	232	9
The total number of keys added.	131	11
A total of	7334	-

Table 2 improved AES encryption simulation results.

Operating segment	Cycle time	Number of rounds
Estimated link	2239	1
Make a byte substitution.	123	10
translocation	54	10
Make a list of confusion.	273	9
The total number of keys added.	131	11
A total of	7434	-

The two Tables above are traditional AES encryption and improved encryption simulation results. A lookup Table is generated before the runtime to eliminate the repetition of the calculation. At the time of the experiment, the average value of the single wheel was 10 times.In the diagram above, can clearly see that two encryption mode only differ among the confusion, the improved encryption into between consumption increase among the confusion, 40 more than the traditional algorithm clock cycles, and improved encryption process will cost about 5% more time on consumption. Their costs are in the same order of magnitude, but they have a better diffusion capability, so the algorithm in this article is desirable.

5. Conclusion

The security of AES is optimized by using symmetric key and asymmetric key as AES encryption mode. By using the hadamard matrix to replace the matrix, the number of branches is increased to 9, which greatly improves the diffusion ability. It also proves that the enhancement of diffusion ability will not bring too much performance cost to the algorithm. This article also explains the current common attack mode and analyzes the security of the encryption mode.

Acknowledgement

Top Innovative Talents Training Program of Jingchu Institute of Technology in 2018 ("Jiuyuan Program").

References

[1] Li J, Liu Z, Chen X, et al. L-EncDB: A lightweight framework for privacy-preserving data queries in cloud computing [J]. Knowledge-Based Systems, 2015, 79:18-26.

[2] Kocabas O, Soyata T, Couderc J P, et al. Assessment of Cloud-based Health Monitoring using Homomorphic Encryption[J]. IEEE, 2013:443-446.

[3] Xhafa F, Feng J, Zhang Y, et al. Privacy-aware attribute-based PHR sharing with user accountability in cloud computing[J]. Journal of Supercomputing, 2015, 71(5):1607-1619.

[4] Ryan M D. Cloud Computing Privacy Concerns on Our Doorstep [J]. Communications of the Acm, 2011, 54(1):36-38.

[5] Mowbray M, Pearson S, Shen Y. Enhancing privacy in cloud computing via policy-based obfuscation[J]. Journal of Supercomputing, 2012, 61(2):267-291.

[6] Khan A N, Kiah M L M, Madani S A, et al. Incremental proxy re-encryption scheme for mobile cloud computing environment[J]. Journal of Supercomputing, 2014, 68(2):624-651.