A Session Key Generator Based on Chaotic Sequence

Chen Zhuo,Zhang zhengwen,Jiang nan
Hubei University of Technology, Wuhan 430068,China
Chenzhuo_hust@163.com

***Abstract*—Key management is a very important part in cryptography. It is related to generation, exchange, storage, safeguarding, use, and replacement of key. This paper focuses on the generation of session key according to the characters of chaotic system. A key generator based on chaotic sequence is proposed in this paper. It has better efficiency compared with the ANSI X9.17 standard.**

Keywords-key management; session key; key generator;chaotic sequence

I. INTRODUCTION

As the foundation of cryptographic technique which supplies confidentiality, integrity, authentication, non-repudiation, etc. Key management acts an important role in cryptology. In modern cryptographic it is required that all encryption arithmetic should be open to the public, so the security of the algorithm resides on the key, not on the secrecy of the arithmetic or encryption of the devices. Once the key is exposed, the attacker can obtain the classified information and the whole encryption system doesn't work any more. Therefore, key management is an important branch of the cryptography, as what the writer of <<<Applied Cryptography>> said in this book: In the real world, key management is the hardest part of cryptography.

Key management concerns the key generation, storage, assignment, using, backup/recovery, updating, cancel and destroy. According to information theory, when the information of cipher runs up to enough, the broken is necessary [2]. So when Alice and Bob communicate each other, they should change the session key regularity. Generally speaking, the session key usually keeps effected only during the current session and when the session is over, the session key should be eliminated immediately, which promise the security. One hand, the more frequently the session key changes, and the less information the attacker can capture, the more secure the communication is. On the other hand, frequent change of the key leads to the more burdens to the system. At present, there are some mechanisms of key generation, such as ANSI X9.17 standard[3].

Now more focuses are on Chaos-based Stream Cryptosystem making use of the iteration unrepeatablity and the property of sensitive dependence on initial conditions of the chaotic sequence[4]. This paper focuses on the generation of session key based on chaotic system and introduces a key generator based on chaotic system which can generate the session key and the initial vectors regularly. Compared with the ANSI X9.17 standard, this mechanism is more simple and more efficient.

II. GENERATION OF KEY

The good way of key generation is very important in a cryptography. It will affect the security of cryptography. Weak key will harm the security of the cryptography terribly, so the core is how to generate a good key which has a good randomicity. Good key should have good randomicity. Meanwhile, the stochastic bits should have good characteristic of cipher (such as excluding weak key, etc).

The familiar ways of key generation are as follows:

1)Using physical Random Noise

Physical Random Noise includes mechanical noise (such as flip a coin or roll a die) and electronics noise(such as vacuum tube noise and diode noise).But it is difficult to put these methods into the application of the network.

2) Linear Congruential Generators

Linear congruential generators are pseudo-random-sequence generators of the form

$X_n = (aX_{n-1} + b) \bmod m$

where X_n is the nth number of the sequence, and X_{n-1} is the previous number of the sequence. The variables a, b, and m are constants: a is the multiplier, b is the increment, and m is the modulus. The key, or seed, is the value of X_0.

The advantage of linear congruential generators is that they are fast, requiring few operations per bit.

Unfortunately, linear congruential generators cannot be used in cryptography; they are predictable. Linear congruential generators were first broken by Jim Reeds [5]and then by Joan Boyar[6]. She also broke quadratic generators: and cubic generators.

3) Using cryptographically secure pseudo-random-bit generator

Pseudorandom bit generator based on cryptography is another way of key generation. For Example, ANSI X9.17 pseudorandom bit generator is a U.S. Federal Information Processing Standard (FIPS) approved method from the ANSI

978-0-7695-3336-0/08 $25.00 © 2008 IEEE
DOI 10.1109/CSSE.2008.833

X9.17 standard for the purpose of pseudorandomly generating keys and initialization vectors for use with DES.

The ANSI X9.17 standard specifies a method of key generation (see Figure 1) This does not generate easy-to-remember keys; It is more suitable for generating session keys or pseudo-random numbers within a system. The cryptographic algorithm used to generate keys is triple-DES.

The process is as follows: K is the special key for this key generator. V_0 is the secret 64-bits seed which is produced by

$$R_i = E_K(E_K(T_i) \oplus V_i)$$

To generate V_{i+1}, calculate:

$$V_{i+1} = E_K(E_K(T_i) \oplus R_i)$$

The output R_i can be used as session key and initialization vector(IV) .The V_{i+1} is the new seed for next calculation.

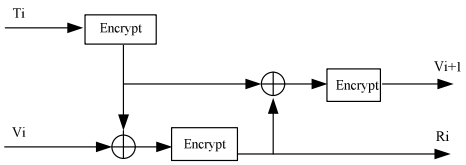

Figure1. Principle of The ANSI X9.17 standard

III. PSEUDORANDOM BIT GENERATOR BASED ON CHAOTIC SEQUENCE

A. The character of chaotic sequence

Since 80s, the idea of building new-style cryptograph via chaotic system has obtained more and more recognition. This idea comes from the natural relationship between the chaotic system and cryptograph. Namely, strong dynamic characteristics in chaotic system roughly corresponds to the highly strong security characteristics in cryptograph and conventional cryptograph with good mixture implicates chaotic phenomenon.

Chaos which is inner random of definite system is seemingly ruleless. A definite system is a dynamic system which can be described by definite ordinary equation, Partial Differential Equations , difference equations or some iterative equations and those coefficients are also definite. Herein, once initial conditions is designated, the system's future behavior is confirmed completely where tiny changes in the starting conditions cannot lead to very large changes over time. However, in 60s people began to know that sensitive dependence on initial conditions resides on some system, namely, tiny changes in the starting conditions will lead to very large changes over time, so the system seems stochastic.

Logistic model is one of the chaotic models, Its equation is as follows:

$$y_{n+1} = \mu y_n(1 - y_n)$$

When μ >3.5699, the equation will enter the chaotic area.

The data in chaotic area has two characteristics. One is the iterative unrepeatablity and the sensitivity to initial conditions. The latter means that only the difference of 10^{-6} will lead to widely divergence in iterative paths of the equation, so the key factor is the initial conditions. The former is that when the iterative equation enters the state of chaos with an appropriate coefficients the equation also enters the infinite non-circular iterative, so repeated iterative values is not available and these values can be adopted to generate random sequence. In theory chaotic sequence is not pseudo-random, but truly stochastic, so key generator with high intension can be constructed using these characteristics.

B. Session key generator based on chaotic sequence

In chaos, tiny changes in the starting conditions cannot lead to very large changes, so the results are unpredictable. Under some circumstances, a mathematics model can easily represent it. Therefore, Not only the method with chaotic theory can generate noises efficiently, but also the noise sequence has good randomicity. Diagram 2 depicts the principle of generating session key via chaotic sequence where session keys of both sides of communication are generated by chaotic sequence and each session adopts different session keys, and chaotic equations plus initial conditions is shared through secret chanel.

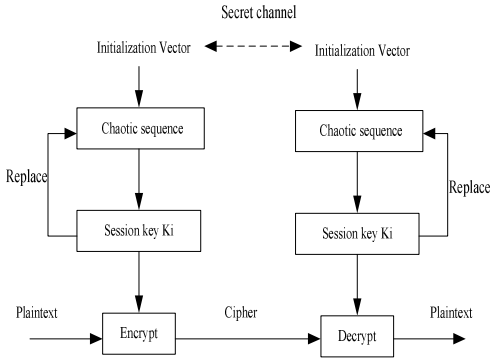

Figure 2. The principle of session key generation from chaos sequence

At first, we should construct a chaos sequence. For example, the following equation can construct chaos sequence.

$$Y_{n+1} = A\sin^2(Y_n - Y_B)$$

A and Y_B is the modulus of equation, along with the change of A and Y_B, the system will enter the state of chaos. For example, A=4, Y_B=2.5, at this point, the equation will enter the state of chaos.

Giving the initial value Y_0 of iterative equation , judge the iterative value. When Y_i>2*A/3, the bit is 1, else it is 0, The sender and receiver should keep the same of the iterative equation modulus and initial value.

The key generator works as follows:

1)According to chaotic sequence generated by the iterative equation, we can obtain a key of 1-bit.

if $Y_i > 2 \times A/3$ then $S_i=1$ else $S_i=0$ (i=1,2,….8), $k=S_i$;

2) according to the need of system ,intercept prescribe length of bits;

3) if current session is over, repeat 1) 2) acquire next session key and IV.

The experiment results show that the efficiency of session key generator based on chaotic sequence is better than the ANSI X9.17 standard, as the ratio of 1：80.

IV. CONCLUSION

Now chaotic cryptography needs further research in many fields. Not only the cryptography system based on chaos has good characteristics of both statistics and topology, but also the system is easy to be designed and implemented. Owing to these characteristics, more and more attention has been paid to the chaotic encryption arithmetic which has become the new resource in cryptograph. This paper explores the application of chaotic sequence in key management.

REFERENCES

[1] Bruce_Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition, Wiley,October 18, 1996

[2] William Stallings, Cryptography and Network Security - principles andpractices,3rd, Prentice Hall, 2003.

[3] ANSI X9.17 -1995 Financial Institution Key Management (Wholesale)Appendix C, American National Standards Institute, 1995.

[4] Murali K. Heterogeneous chaotic systems based cryptography. Phys Lett A,2000,272:184-192

[5] Kocarev L,Jakimoski G.Logistic map as a block encryption algorithm.Phys Lett A,2001,289(4-5);199-206

[6] Ott, Edward. Chaos in dynamical systems. Cambridge University Press, 2002.