ATLANTIS PRESS
Advances in Computer Science Research, volume 44
3rd International Conference on Wireless Communication and Sensor Network (WCSN 2016)

CPRS Algorithm for Streaming Media Encryption and Its Functional Analysis for Wi-Fi Security and Rapidity

Dan Cai, Xiao-Yong Ji, Jia-Ming Pan
Nanjing University, China
E-mail: caidan0924@163.com, jxy@nju.edu.cn, panjm@nju.edu.cn

***Abstract*-In order to ensure the security of the wireless network, Wi-Fi Alliance uses stream cipher algorithm RC4 to encrypt data in the security protocol WEP/WPA. RC4 is a fast algorithm but easy to break. To solve the problem, WPA2 is proposed which uses block cipher algorithm to improve the anti-crack ability of wireless system. AES is time consuming because of its complexity even though it is characterized by high security. To respect the safe and real-time requirements at the same time, we propose a new chaotic encryption algorithm CPRS based on Tent chaotic maps. Chaos is pseudo-random and sensitive to initial parameters which improves the safety of algorithm. Besides, Tent chaotic maps used in the crypto-system is a linear equation which reduces the time of encryption. Then, to quantify the rapidity and security level of the CPRS algorithm, we compare it with the AES algorithm.**

Keywords-wireless network;encryption; tent chaotic maps

I. INTRODUCTION

Wireless network refers to the network with wireless communication technology, which allows the users to build data network and global voice communication based on long-distance wireless connection and infrared technology and radio frequency technology relied on short-distance wireless connection. With the development of wireless network, the safety is increasingly important. WEP (Wired Equivalent Privacy) as the first generation Wi-Fi protocol for 802.11 uses the stream cipher RC4 algorithm and integrity check CRC-32 algorithm before transmission. RC4 algorithm consumes a relatively short time but unfortunately, WEP is cracked because simple RC4 algorithm has introduced major flaws [1]. To improve the security, Wi-Fi Alliance put forward WPA (Wi-Fi Privacy Access) and WPA2 successively. TKIP (Temporal Key Integrity Protocol) used in WPA still encrypts data with the RC4 algorithm whose key length increases from 40 bits to 128 bits. Per-shared Key and MIC (Message Integrity Code) as identity verification and integrity check algorithm make package structures more complex, which solves the problem of shorter key length in WEP. However, the encryption system is easily compromised if the user uses the simple weak keys [2]. So AES (Advanced Encryption Standard) was designed in the final security protocol WPA2 to meet the requirements of 802.11i standard which is block cipher with 128 bits, including byte substitution, row shift, column confusion and add round keys. Complex multiple substitution improves the reliability and robustness of the system and consumes a high time and a large amount of memory [3]. To meet the requirements of security and rapidity, we propose a new chaotic encryption algorithm CPRS (chaotic pseudorandom sequences) based on Tent chaotic maps.

II. CPRS ALGORITHM

Chaos is a pseudo-random and seemingly irregular movement appeared in a certain system [4]. A large number of examples show that when the initial value produces small changes, long-term changes are enormous, which is similar with the so-called "butterfly effect" and means that the prediction of long-term state is completely random. So the chaotic system is sensitive to initial parameters and orbital instability, which satisfies the requirements of cryptography. Cryptography with chaos is widely used in information security and other fields. It is impossible to predict the long-term state because the small uncertainty in the initial state quickly expands exponentially in chaotic system. The trajectories either exponentially converge quickly or slowly diverge (the worst case) as they approach each other. The rate of convergence or divergence of this trajectory is called the Lyapunov exponent and the positive Lyapunov exponent means chaotic system. A number of positive Lyapunov exponents imply the hyper chaotic system with high randomness. Tent chaotic map is a piecewise map with good ergodicity and uniformity, but fails the randomness test which needs to apply the stochastic perturbation used in crypto-systems. To improve the randomness and the anti-crack capacity of the Tent chaotic maps, we adopt multi-dimension chaotic systems with multiple positive Lyapunov exponents that is Improved One-way Coupled Ring Map Lattice –IOCRML to build cipher algorithms.

The CPRS algorithm selects m-dimensional OCRML systems.

$$x_i(n+1) = (1-\varepsilon_i)f[x_i(n)] + \varepsilon_i f[x_{i+1}(n)] \quad (1)$$

$$x_{m+1}(n) = x_1(n) \quad i = 1,2,\dots,m \quad (2)$$

This is a very complex system with m-dimensional hyper chaos where n is discrete time, i is the variable of ring lattice, ε_i is coupling coefficient, $f[x_i(n)]$ is an equation, if in a form of the Tent Map:

$$f[x_i(n)] = \begin{cases} x_n/h_i & 0 < x_n \le h_i \\ (1-x_n)/(1-h_i) & h_i < x_n \le 1 \end{cases} \quad (3)$$

h_i takes 0.5 in every node of the IOCRML where three Lyapunov exponents are all greater than zero when m is 3, ε_i is 0.90.

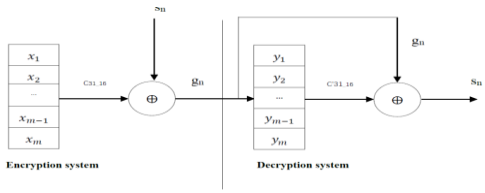


Figure 1. Synchronous CPRS cipher algorithm.

Fig.1 shows the CPRS cipher algorithm based on IOCRML system. Specific steps of encryption and decryption are as follows:

Encryption systems:

$$x_1(n+1) = (1-\varepsilon_1)f[x_1(n)] + \varepsilon_1 g(n)/32768$$
$$x_i(n+1) = (1-\varepsilon_i)f[x_i(n)] + \varepsilon_i f[x_{i+1}(n)]$$
$$x_{m+1}(n) = x_1(n) \quad i = 2,3,\ldots,m \tag{4}$$

g(n) is the cipher text transmitted. The reason of g(n) /32768 is that g(n) can calculate as the iteration variables of 16 bits' binary in chaotic equations. We regard it as a signed integer and its value is fixed in the range of -1 and 1 by multiplying by 1/32768.

The composing process of g(n) is as follows, first,

$$c = f[x_2(n)] \tag{5}$$

$c=f[x_2(n)]$ is seen as steganography information of Tent chaotic maps when the plaintext is encrypted. Here we select i = 2. Chaotic mappings calculate in double form in the digital systems. Double format defined by IEEE shows that the total length of data is 64 bits and 1 bit is sign bit, 11 bits are dedicated to the exponent and 52 bits to the mantissa. So the corresponding value is value= $(-1)^s\left(2^{e-1023}\right)(1.f)$ when omitting the left 1 of decimal point according to normalization. Chaotic values are intercepted 16 bits in the way of c_{m+15_m} that represents 16 bits' binary sequences from the first m bit.

Then, the plaintext is taken as 16 bits' quantization and encoding. c_{m+15_m} which is a chaotic pseudo-random sequence with high randomness is combined with the plaintext s(n) using XOR for the cipher text g(n).

$$g(n) = c_{31\_16} \oplus s(n) \tag{6}$$

Decryption systems:

$$y_1(n+1) = (1-\varepsilon_1)f[y_1(n)] + \varepsilon_1 g(n)/32768$$
$$y_i(n+1) = (1-\varepsilon_i)f[y_i(n)] + \varepsilon_i f[y_{i+1}(n)]$$
$$y_{m+1}(n) = y_1(n) \quad i = 2,3,\ldots,m \tag{7}$$

The decryption systems use the same parameter ε_i as the encryption systems.

The plaintext is as follows, first:

$$c' = f[y_2(n)] \tag{8}$$

$c=c'$ when receiver is in sync with transmitter. Decrypted sequences intercept 16 bits in the way of c'_{m+15_m} the same as the encrypted messages. Then, the plaintext is:

$$s(n) = c'_{31\_16} \oplus g(n) \tag{9}$$

CPRS systems can improve the randomness of Tent chaotic maps and the anti-crack ability of the wireless systems and the rapidity of encryption at the same time.

III. DIFFERENT TEST PARAMETERS

A. Encryption Time

AES and CPRS algorithms' encryption time when encrypting 105bits，106bits，107bits in the same system is shown in Table 1.

TABLE I. ENCRYPTION TIME

Time	Bits of encrypted data		
	10^5bits	10^6bits	10^7bits
AES algorithm(ms)	12.371	114.866	1195.707
CPRS algorithm(ms)	4.256	24.199	224.757

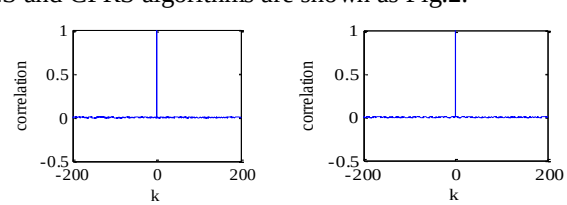
As can be seen in table 1, AES algorithm's encryption time is 2.90 times as much as CPRS's when encrypting 105bits, 4.74 times when encrypting 106bits, and 5.32 times when encrypting 107bits. Thus, AES algorithm's encryption time is greater than CPRS's. CPRS algorithm as the stream cipher algorithm produces random sequences which are combined with the plaintext using XOR operation for cipher. However, AES algorithm as the block cipher is converted into the stream cipher in some way before transmitted which consumes much more time. In a word, CPRS used in wireless system can improve the rapidity for encryption.

B. Correlation

Correlation measures the randomness of sequences. The binary length of chaotic sequences is n, step-size parameters of binary sequences is k. Its correlation coefficient is defined as [5]:

$$\mathrm{corr}(k) = \frac{1}{n}\sum_{i=1}^{n-k} S_i . S_{i+k} \tag{10}$$

We get the sequences S by iterating binary sequences and calculating the correlation coefficient. Correlation coefficients by calculating encrypted sequences produced by AES and CPRS algorithms are shown as Fig.2.



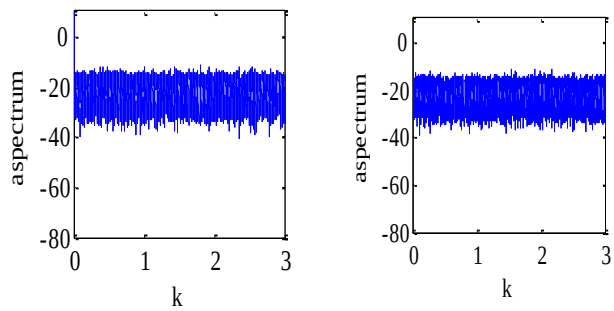
(a) sequences produced by AES (b) sequences produced by CPRS

Figure 2. Correlation.

Results show that the correlation coefficients of binary sequences produced by AES and CPRS algorithms are close to zero whose function curves are with a tapering peak and without high side lobes. The encrypted sequences produced by AES and CPRS have good randomness.

C. Power Spectral Density

Getting the power spectral density by calculating correlation coefficients by formula (10) discrete Fourier transform. Fig.3 shows the power spectral density of sequences obtained by AES and CPRS algorithms.



(a) sequences produced by AES (b) sequences produced by CPRS

Figure 3. Power spectral density.

From Fig.3, we can see that power spectral density curves produced by AES and CPRS sequences are connected apparently. Thus sequences satisfy the requirements of cryptography and anti-attack.

D. NIST Test

Statistical Test Suite put forward by National Institute of Standards and Technology is the most authoritative testing tools for randomness at present. This paper tests the randomness of sequences produced by AES and CPRS by sts2.1.1. There are sixteen kinds of statistical tests in sts2.1.1[6] including Frequency, Block Frequency, FFT, Rank [7], and so on.

Significance level is α and the total length of test sequences is N, so,

$$P = (1-\alpha) \pm 3\sqrt{\alpha.(1-\alpha)} \qquad (11)$$

α is in the range from -1 to 1 in the formula. The initial value of test is 0.4 and total data is 1x107bit which is divided into 100 groups with an array of 100000bit. The results of test are as follows.

If the p-value on behalf of the decision-making rule is less than 0.01, the tested sequences are random. Otherwise the sequences are not random. From Table 2, we can see that p-value of sequences produced by AES and CPRS is greater than 0.01, and therefore both of them are random. PRPPORATION mans that the sequences pass the test.

IV. CONCLUSION

The paper proposes a new CPRS cipher algorithm based on Tent chaotic maps to solve the problem that AES consumes time in the protocol WPA2 in the wireless system. By testing and simulating the performance of CPRS, we can see that CPRS can both improve the security and rapidity of system. In conclusion, CPRS can be used in the field of communication system.

REFERENCE

[1] Yao Yao, jiang Chang, Wang Xingwei "Enhancing RC4 algorithm for WLAN WEP Protocol" Control and Decision Conference, pp 2623-2637, 26-28 may 2010.

[2] Wu Yi-Chen Security Analysis and Improvement of WPA/WPA2-PSK. Computer and Modernization ,2013, (1):153-157.

[3] B. Bakhache, J. Ghazal, S. El Assad, "Enhancement of ZigBee and Wi-Fi security by a robust and fast chaotic algorithm" 5th International Conference on Network and System Security, pages 300 – 304, 2011.

[4] Deng S J, Huang G C, Chen Z J, et al. Research and implement of Self-adaptive image encryption algorithm based on chaos, Journal of Computer Applications, 2011, 31(6): 1502-1504.

[5] Liao Ni H, et al. The chaotic spreading sequences generated by the extended chaotic map and its performance analysis. Journal of Electronics & Information Technology, 2006, 28 (7): 1255-1257. (in Chinese).

[6] Andrew R, Juan S, James N, et al. Statical Test Suit for Random and Pseudorandom Number Generator for Cryptographic Applications. NIST Special Publication, 2001, 1(1): 800-822.

[7] Feng P H, Su G P, Tang M Y. Design and Implementation of a Random Sequence Testing Method of Based Approximate Entropy. Mathematics in Practice and Theory, 2009, 15:149-152.

TABLE II. NIST TEST

STATISTIC TEST	AES		CPRS	
	P-value	PROPORATION(%)	P-value	PROPORATION(%)
Frequency	0.040108	97	0.224821	99
Block Frequency	0.058984	100	0.534146	99
CumulativeSums	0.437274	97	0.465319	100
Runs	0.419021	100	0.474986	100
Longest Run	0.637119	99	0.350485	100
Rank	0.262249	98	0.554420	97
FFT	0.719747	99	0.971699	96
NonOverlapping Template	0.102526	96	0.637119	100
Overlapping Template	0.224821	100	0.401199	99
Approximate Entropy	0.102526	97	0.419021	99
Serial	0.249284	98	0.924076	99
LinearComplexity	0.181557	97	0.213309	99
RandomExcursions	0.162606	100	0.122325	100
RandomExcursionsVariant	0.834308	100	0.739918	100