Asymmetric Cryptography Algorithm with Chinese Remainder Theorem

ZHANG Yun-peng* LIN Xia WANG Qiang

College of Software and Microelectronics Northwestern Polytechnical University

710072 Xi'an, China

poweryp@163.com, rjxyjs@nwpu.edu.cn

Abstract*——*This paper designed a asymmetric algorithm based on Chinese Remainder Theorem and double sequence, which uses the sequence of random numbers generated from the interference of Logistic and Chebychev chaotic mapping to interfere with the backpack sequence, while setting the easy solutions of super-increasing knapsack problem as the limitation of the algorithm, and using Chinese remainder theorem to hide the sequence mentioned above, before making the hidden backpack sequence to be transformed modulus. Through simulation and comparisons with some related algorithms transversely and longitudinally, this algorithm is excellent with a higher efficiency and better security.

Key words: Cryptography, Public-key, Chaotic system, Fast

Ⅰ. INTRODUCTION

The Public-key cryptosystem [1] separates encryption and decryption operations so that both sides are able to establish secure communications without exchanging keys in advance. This, in aspect of transmission and storage of keys, has largely reduced the quantity of the keys which are required in multi-users' communication and saved system resources. Because of its [2] many basic characteristics, such as the ergodicity, miscibility, certainty and the sensitivity to initial conditions, which are all related to the diffusion and confusion of cryptography, chaotic system is of great applied value in cryptography.

At present, the research based on chaotic private-key cryptosystem is more mature than that based on the chaotic Public-key cryptosystem [3], which is rarely done, with some security problems of several existing algorithms waiting for being solved. At the same time, features of the encryption scheme and design in asymmetric encryption system determine that its speed is slower than the speed of private key encryption system and these all impede the development of public-key cryptosystem.

The reference [4] has proposed a high density knapsack public-key cryptosystem algorithm which is quite efficient, but after the author's theoretical analysis and experiments, the aspect of safety is expected to be improved. Therefore the author designed a rapid public-key cryptosystem algorithm through chaotic system generating interference backpack vector, and a chaotic pseudo-random generator which can be applied to the algorithm implementation. Through simulation and comparisons with some related algorithms transversely and longitudinally, this algorithm is excellent with a higher efficiency and better security.

Ⅱ. CHINESE REMAINDER THEOREM

Chinese remainder theorem [5] has been widely used in cryptography, mainly for simplifying some computations, and some public-key cryptosystems proposed recently based on Chinese remainder theorem .The obvious advantage of the algorithm is that it can hide the data and can be designed as a one-way limitation. It can be described as follows: set n_1 n_2, ... n_k are coprime and all positive integers, let $n = n_1n_2n_3...n_k$ so:

978-1-61284-486-2/11/$26.00 ©2011 IEEE

$$\begin{cases} x \equiv x_1 \bmod n_1 \\ x \equiv x_2 \bmod n_2 \\ \quad \cdots \\ x \equiv x_k \bmod n_k \end{cases} \quad (1)$$

The set *{0，1，2...n-1}* has a unique solution, that is, $x = \sum_{i=1}^{k} x_i M_i s_i \bmod n$,with $M_i = n / n_i$,while

$s_i \equiv M_i^{-1} (\bmod n_i)$ （i=0，1，2，...，k）

The corresponding function of Chinese Remainder Theorem in Miracle repository are bool crt_init (big_chinese* c, int r, big* moduli),void crt (big_chinese* c, big* u, big x) and void crt_end* (big_chinese *c).That is, initialize the big_chinese by modulus firstly, then calculate to get the result x and finish the operation in the end.

Ⅲ. DESCRIPTION OF ALGORITHM

This algorithm utilizes the easiness of super-increasing knapsack problem as its limitation and uses double backpack sequence *A* and *B* in the process of constructing, then makes the super increasing sequence S as one of a subset of a backpack, for instance, $S \subset B$, before using Chinese remainder theorem to hide the two sequences to get a new sequence *X*, and apply necessary modulus transformation to *X* to get *X**.Thus, the security is enhanced. Issue *X** as public key while the related parameters and S as private keys. Experiments show that the speed of the algorithm is very fast in both of encryption and decryption. Besides, it is easy to generate a key, and convenient for the software implementation.

The main steps of the generation of keys, encryption and decryption are shown below:

A. The production of the key(shown in Figure 1 below):

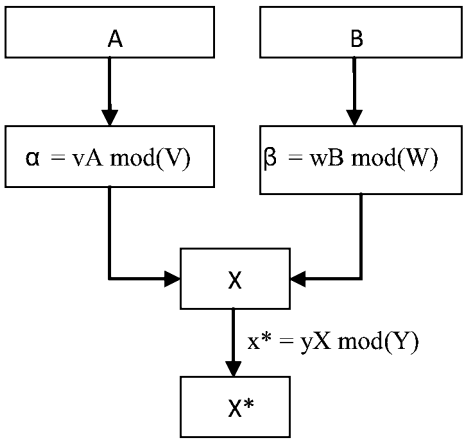

Figure 1. The production of the key

1) Choose two sequences *A* and *B*, *A = (a1,...,an,..., Z1,..., Zu)*, *B = (a1,..., an, s1,..., sw)*, in which, *t = n + u*. Besides, *B* satisfies that vector *S* is super increasing backpack vector.

That is, $s_i > \sum_{j=1}^{u} s_j, (1 < j < u)$; *Z1,... Zu*, satisfy that

Z1 = Z2 = ... Zu , at the same time $Z_i > \sum_{i=1}^{u} a_i$;

2) Choose modulus *V*>|*A*| and *W*>|*B*|, |*A*| and |*B*| respectively are the sum of all the elements in A and B. Generating two random secret parameters v and w to make gcd(*v, V*) = gcd (*w, W*) = 1, let α = vA mod（*V*）, *β=wB mod*（*W*）;

3) Choose two modulus *p* and *q* which are coprime , plus, *p*>|α |, *q*>|β |. |α | *and* |β | respectively represent the sum of all elements in α and β . Let *N = pq*;

4) Use Chinese remainder theorem to calculate *X*, aiming at (in order to) hiding α and β into *X*, and hiding A and B indirectly, that is:

$$\begin{cases} X = \alpha \bmod (p) \\ X = \beta \bmod (q) \end{cases} \quad (2)$$

5) Choose modulus *Y* >|*X*|, |*X*| is the sum of the elements in vector *X*. Select the secret parameter y to make gcd(*y*，*Y*)=1, let *X* = yX mod(Y).*

public key: *(X*,n,u)*

private key:*(A, B, p,q,v,w,V,W,y,Y,Z)*

B. Encryption(shown in Figure 2 below):

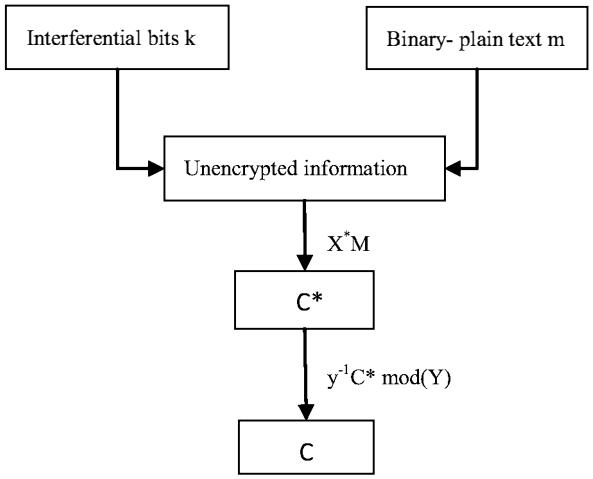

Figure 2. The process of the encryption

The plain text sequence is $m = (m_1, m_2, ..., m_w) \in \{0,1\}U$. We choose the random sequence $k = (k_1, \cdots, k_n) \in \{0,1\}n$, then combine the k and m to be an interfering-plaintext sequence $M = (k_1, ...k_n, m_1, m_2 \cdots, m_w)$which is prepared for encryption .

After encryption, the cipher text is

$$C^*=X^*M=\sum_{i=1}^{t} X_i^* M_i \tag{3}$$

C. Decryption (shown in Figure 3 below):

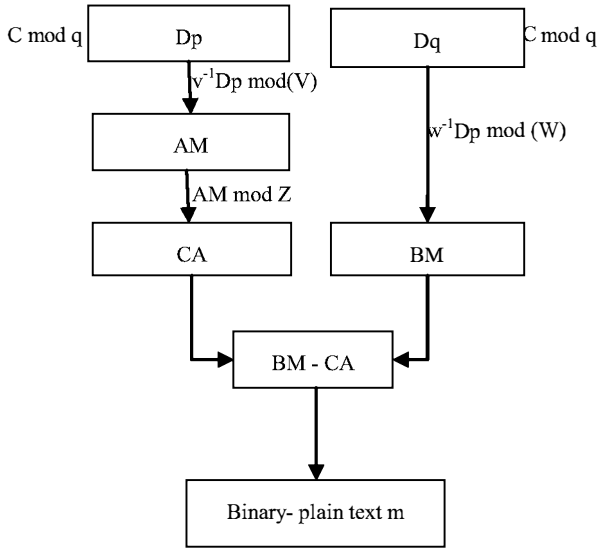

Figure 3. The process of the decryption

1) Calculate the cipher text $C=y^{-1}C^* \bmod (Y)$.

2) Pick modulus p and q with the cipher text C, namely, $Dp = C \bmod p = XM \bmod p = \alpha M$, similarly, $Dq = \beta M$.

3) Applying modulus-reverse transformation to α and β, that is $AM = \mathrm{v}^{-1} Dp \bmod \mathrm{V} = \mathrm{v}^{-1}\alpha M \bmod \mathrm{V}$, similarly we can get $BM = \mathrm{w}^{-1} Dq \bmod \mathrm{W}$

4) Calculate :

$$\mathrm{CA}= \mathrm{AM} \bmod \mathrm{Z} = \sum_{i=1}^{n} \mathrm{a}_i k_i + \sum_{j=1}^{u} Z m_j (\bmod Z) = \sum_{i=1}^{n} a_i k_i$$

5) From the structure of A and B, we can know that

$$(BM\text{-}CA) = \sum_{i=1}^{u} s_i m_i \tag{4}$$

Because s is super increasing backpack vector, that is, $(BM\text{-}CA)$ can get the plaintext via working it out.

D. Algorithm Instructions:

1) The choice of the parameters: The selection of the sequences A and B needs to meet the condition that is mentioned in the steps of the key production in the algorism description above. Elements in A and B can be produced randomly, so they can be generated by the chaotic pseudo-random number generator [6]. Meanwhile, the interfering bit k of the plaintext can be generated totally randomly.

2) We may apply random transformation f (we can make choices freely while implementing) to the subsequence S of sequence B, after which, we can work out the plaintext through the inverse -transformation off.

3)The encipher can add a secret parameter $\mathrm{h} \in \mathrm{Z}^+$, making $B = hB$ and $BM/h - CA$ in decryption. Thus the security of the algorism is strengthened in some degrees, for exhausting h is almost impossible.

Ⅳ. ANALYSIS AND COMPARISON OF THE ALGORITHM

A. *Efficiency analysis*

Suppose that the length of plaintext M is k, actually, the process of encryption is an addition, of which the time complexity is *O (k)*. While in the course of decryption, a inverse modulus operation is carried out firstly; the liner operation of modulus is done(did) twice in the next step; then the liner operation of modulus is carried out once; finally we can figure it out to get the plaintext, namely, execute the comparison operation with super increasing sequences for k times; each of their time complexity is $O(k^2)$, $O(k)$, $2*O(k^2)$, $O(k)$ *and* $O(k)$. So the total time complexity is $3*O(k^2) + 4*O(k)$. After ignoring the lower order, it is $3*O(k^2)$.

The complexities of the traditional public-key algorithms, RSA and ElGamal[7], are both cubic. If the modulus length they use is 1,024 bits in binary , the encryption of RSA will cost the bit operation about 10^9 times, whereas due to the use of operation and two modulus by computing a module, the encryption speed of ElGamal is about a half of that of RSA. This algorithm acquires addition for n-times in the process of encryption. If $n = 1000$, it will only take about 10^3 times bit operation to complete encrytion, which demonstrates the encryption speed is very fast. Besides, in the decryption process it will totally acquire $3*O(t^2) + 4*O(t)$ times calculations, which is about $3*10^6$ times-operation, and *300* times faster than RSA public-key algorithms.

B. *Security analysis*

1) In the aspects of the key, through the modulus Y, the randomness of vector A is able to cover the vector X, which is obtained by Chinese remainder theorem directly. The attacker cannot get X before getting Y and y, in such case he cannot estimate the size of the modulus N, let alone to get p and q by decomposing N, which means that he cannot get the information of the keys. Thus, the security is enhanced. In addition, $k = (k_1, ..., k_n)$ is the random interferential signal that is independent from the plaintext and mixed with the value of plaintext calculation when being calculated. To the attackers who cannot distinguish the message of plaintext from interfering signal, what they can get at most is the encrypted information of interfered plaintext. Never could the attacker find out the corresponding numerical size in the plaintext.

2) This algorithm is also able to resist the attacks of low-density subsets and LDA. According to the *L3–lattice base reduction algorithm*, if the algorithm can always find a basis of the shortest nonzero lattice vector, so if $d = \dfrac{t}{\max \log_2 x_i}$ (note, $t = n + u$), and $d < 0.9408$, it is very likely to be attacked efficiently. Attack may be like this:

$$\begin{pmatrix} 1 & & o & \lambda x_1 \\ & \cdots & & \cdots \\ o & & 1 & \lambda x_2 \\ \frac{1}{2} & \cdots & \frac{1}{2} & \lambda S \end{pmatrix} \tag{5}$$

λ is a proper integer which satisfies:

$$\lambda > \frac{1}{2}\sqrt{t}\ ,\quad S = \sum_{i=1}^{t} x^*_i M_i \ 。$$

The cipher text is worked out by $C = XM$. Assuming that the lengths of the modulus q and p are nearly identical, namely，about W (bit), and the size of the modulus $N = pq$ is about $2\log_2 W$ (from $N = pq$ we can know $\log_2 N = \log_2 (pq)$. That is $d = \dfrac{t}{2\log_2 W}$ .When $d > 1$, it requires $n + u > 2\log_2 W$, that is, $u > 2\log_2 W - n$. When this condition is met, we can get $d > 1$; therefore it can resist L3'attack. Thus, if the plaintext is the random interference of 120 bits-plaintext, $n = 120$, then only if the length of modulus N is less than *70* bits can it resist the attacks of the low-density subsets .

It indicates that the security of this algorithm can be controlled.

There is also a defect in this algorithm that the decryption of the cipher text by vector A and B, thus the strength of the security is weakened. An excellent design of algorithm should make decryption also depend entirely on sequences A and B. Two solutions can be adopted to weaken its influence on the safety of algorithm. One is to add a secret parameter h, making $\boldsymbol{B} = h\boldsymbol{B}$ which is impossible to search h exhaustively for the attackers; Another one is to prevent the leakage of private-key, no longer to store it after using vector, and recover it by using some certain methods.

V. CONCLUSION

In this paper we design a rapid public-key algorithm by making use of chaotic system which produces backpack interfering vector and using the Chinese remainder theorem to hide the double sequences. Through simulation and comparisons with some related algorithms transversely and longitudinally, this algorithm is excellent with a higher efficiency and better, controllable security, thus making up for the shortcoming of security which is put forward in the reference [4].

ACKNOWLEDGEMENTS

This work is supported by Aero-Science Fund of China (2009ZD53045), Science and Technology Development Project of Shaanxi Province Project(2010K06-22g), Basic research fund of Northwestern Polytechnical University (GAKY100101), and R Fund of College of Software and Microelectronics of Northwestern Polytechnical University (2010R001).

REFERENCES

[1] Z. Yunpeng, L. Xia, L. Xi, An improved high-density knapsack-type public key cryptosystem, 5th International Conference on Software and Data Technologies, INSTICC, 2010, pp.127-133

[2] Z. Yunpeng, Z. Fei, Z. Zhengjuni, A Color Image Encryption Algorithm Based on Chaotic Chebychev and Variable-Parameters Logistic Systems, Journal of Nothwestern Polytechnical University, vol.28, no 4 (2010), pp.628-632

[3] S. Xi, The research and implementation of public-key algorithms based on chaos. University of Chongqing, Reading, MA,2006.

[4] W. Bao-cang, H. Yu-pu, Knapsack-Type Public-Key Cryptosystem with High Density. Journal of Electronics & Information Technology, vol.28, no.12 (2006), pp.2390-2393

[5] J. Xue-juan, the origin and the solution of the "Chinese remainder theorem". Journal of jiujiang University (natural sciences), no.3(2004), pp.102-108

[6] Y. Zhen-Biao, F. Jiu-Chao, A method for generating chaotic-spectrum sequences and their optimized selection algorithm, ACTA PHYSICA SINICA,vol.57,no.3(2008), pp.1409-1415

[7] Rivest R L, Gau M J. Adlcman L M. A method for obtaining digital signature and public key cryptosystems [J]. Communications of the ACM, 1978, 21(2): 120-126.