Two-Dimension Chaotic-Multivariate Signature System

Xiaoyan Sun[1], Maosheng Zhang[2*] , Huanguo Zhang[3], Xiaoshu Zhu[1]

[1] School of computer science and engineering, Yulin normal University, Yulin 537000, China

[2*] School of Mathematics and Information Science, Yulin normal University, Yulin, 537000, China

[3]School of Computer, Wuhan University, Wuhan 430079, China

Abstract

A novel hybrid cryptosystem which is resistant to quantum algorithm is developed. The system is combined with multivariate cryptosystem and chaotic system, two systems which are both secure under quantum attacks. The plaintexts are displaced by an affine transformation and encrypted by central map in multivariable cryptosystem. And then, the outputs of central map act as initial values in a two-dimension chaos system and are transformed by another affine transformation. Finally, the cipher texts are derived by adding the outputs of chaos system and the second affine transformation. Due to the chaos system, the shortcomings of traditional multivariate cryptosystems are offset and therefore the security is enhanced. The analysis shows that the proposed signature system is able to resist common attacks.

Keywords: *quantum computer; cryptosystem; chaotic; security*

1. Introduction

Public Key Cryptology was developed by Diffe and Hellman in 1976[1], which can provide various security services such as confidentiality, credibility (identification), integrity, non-repudiation, usability, access control[2], etc. There are some excellent Public Key Cryptosystems, such as RSA Public Key Cryptosystem which was based on big integer factoring and developed by Rivest in 1978[3]; ElGamal Public Key Cryptosystem which was based on discrete logarithm and developed by ElGamal in 1985[4]; Elliptic Curve Public Key Cryptosystem(ECC) which was developed by Koblitz and Miller in 1987[5]. These systems are widely used in all trades and professions. In 1994, a scientist named Peter Shor working in Bell laboratory proposed a famous algorithm to attack all cryptosystems which can be converted to discrete Fourier transform, including RSA, Elgma and ECC [6]. Shor algorithm and its extended algorithm are efficient with polynomial time in quantum computers. Meanwhile, 28 bit quantum computer was successfully created by D-Wave Company in 2007. NASA bought the first 128 bit quantum computer in 2011. Consequently, the widely used public cryptosystems are not secure under quantum computers. In recent years, Anti Quantum Computation Public Key Cryptology or Post Quantum Computation Public Key Cryptosystem has been received widespread attention and intensive studied all over the world [7, 8]. Multivariate Public Key Cryptology (MPKC) and chaotic cryptosystem are two cryptosystems which can resist quantum computers.

The security of MPKC is based on the difficulty of solving multivariate quadratic equations on finite fields. There is no evidence that multivariate quadratic equations can be solved efficiently on quantum computers [7, 9]. And the calculation resource consuming is much less than traditional public cryptosystems. In recent decades, scholars designed a few famous quadratic multivariate public algorithms, such as MI Cryptosystem developed by Matsumoto and Imai in 1988[10], Hidden Field Equation (HFE) system proposed by Patarin in 1995[11], Unbalanced Oil and Vinegar (UOV) Schemes designed by Patarin in 1997[12], Tame Transformation system originated by T.T.Moh in 1999[13]. Professor Boyin Yang and Minjun Chen proposed a well-known signature system named tame transformation signatures (TTS) in the first International Workshop for Applied PKI (IWAP2002). And then, there were many modification versions based on this signature system for different situations. In 2004, multivariate signature scheme SFlash was accepted as European safety standard for low consumption smart card by European New European Schemes for Signatures, Integrity and Encryption (NESSIE) [14]. Wuhan University developed a kind of new noise factor and noise-operation perturbed mode in order to strength the safety of Sflash in 2011[15]. Though MPKC is well researched by scholars and the great importance is attached by governments, the proposed MPKC above are proved to be unsafe one after another [16-19]. The ways of combining the Multivariate Public Key Cryptosystem with various modification modes can improve the security of cryptosystems, for example, minus mode can strength anti-attack property of Multivariate Public Key Cryptosystem obviously, branch mode can improve computing efficiency [13].

This paper designs a high security hybrid public key cryptosystem, in which two affine transformations, a central map and a chaotic system are combined. Plain texts are first transformed through an affine transformation and then encrypted with a central map. The first two elements of outputs of central map act as initial values in a two-dimension chaotic system. After applying another affine transformation, the outputs are added to the outputs of chaotic system and the cipher texts are derived.

The next section introduces some fundamental theory about MPKC and chaotic algorithm. Section 3 develops our proposed system and section 4 analyzes the security of our crypto scheme. Finally, conclusions are presented in section 5.

2. Multivariate public key cryptosystem and chaos theory

2.1 Multivariate Public Key Cryptosystem

Multivariate Public Key Cryptology System (MPKC) is established on a finite domain in a polynomial ring [20]. Mathematical structure of Multivariate Public Key Cryptology System is shown in Eq. (1).

$$Y=F(X)=T\circ P\circ S,\ F_q^n \to F_q^m \qquad (1)$$

Among this formula, q is a prime number and F_q^k means the k-dimension vector space on finite domain F_q. T and S are invertible affine transformations on F_q^m and F_q^n respectively. P denotes polynomial equations with n variables and m equations, which is known as central map. The maximum degree of each equation is 2 and the coefficients belong to F_q. The central map is from F_q^n to F_q^m. Non-linear central map P is the core of Multivariate Public Key Cryptology System. The main function of T and S is to hide central map. The calculated result Y is public key. Expression form of its equivalent equation set is shown in Eq. (2).

$$y_i = \sum_{1\le j\le k\le n} c_{ijk}x_jx_k + \sum_{1\le j\le n} b_{ij}x_j + a_i,\ i=1,2,...,n \qquad (2)$$

where $c_{ijk}, b_{ij}, a_i \in F_q$.

(S, P, T) are private keys of MPKC. MQ problem is usually expressed as given public key Y=F(X) but x needs to be worked out. IP problem is that Y is divided into S, P and T. Patarin proved that MQ problem on arbitrary domain is a NP complete problem and IP problem is a NP difficult problem on Eurocrypt conference. Multivariate Public Key Cryptology System is designed based on these two mathematic problems [8, 20].

2.2 Chaos Theory

Lorenz, Father of Chaos, defined chaos as “random behavior of deterministic system”. Professor Shuisheng Qiu in South China University of Technology considered that if one movement includes the following three characteristics, namely, being sensitive to initial values, having random-like property and unpredictability, then it can be called chaos [21]. According to the number of variables in an equation, chaos equations can be categorized into one-dimension, two-dimension and three-dimension equations which are shown in Eq. (3), (4), (5) respectively.

$$x_{n+1} = \lambda x_n(1-x_n) \qquad (3)$$

$$\begin{cases} x_{n+1} = 1 + y_n - C_n^2 \\ y_{n+1} = Bx_n \end{cases} \qquad (4)$$

$$\begin{cases} \dfrac{dx}{dt} = \sigma(y-x) \\ \dfrac{dy}{dt} = \rho x - y - xz \\ \dfrac{dz}{dt} = xy - \beta z \end{cases} \qquad (5)$$

Where (x, y, z) represent some meaningful variables and act as system trajectory. And also system parameters δ, ρ, β are participating in calculation.

There are many technologies to generate chaos sequence, such as Logistic Mapping, Kent Mapping, Chebyshev Mapping, etc. The expression form of one-dimension Logistic Mapping is shown in Eq.(6).

$$x_{n+1} = 1-\mu x_n^2, x\in(-1,1), \mu\in[0,2] \qquad (6)$$

Whereby x_n are called state variables. μx_n is named driving factor which drives state variable to change from x_n to x_n+1. μ is a bifurcation parameter. When the value of μ satisfies 3.5699456<μ≤4, Logistic Mapping conducts chaotic state [22].

The subtle changes of parameters and initial condition in chaos system will cause avalanche phenomenon to the output of chaos sequence. Meanwhile, the output of chaos system has strong non-linear property as well as strong anti-attack ability against regular cryptanalysis method. So due to its usability, uniqueness, reliability, random-like property and unpredictability, chaos sequence is extraordinary suitable for structuring secure cryptology systems [23].

3. Multivariate-chaos crypto-algorithm

The structure of center map has great influences security performance and so plays a key role in MPKC system. Though it has property to resist quantum calculation, it doesn't receive wide application at present because the mathematical structural properties of center map cannot resist bilinear attack, rank attack, etc. Chaos system is of good random-like property and unpredictability, but many chaos system make use of same initial values and control parameters to start chaos system, meanwhile, the iterative process of chaos system isn't influenced by other factors (i.e. initial state is not given) and doesn't accord with safety criterion of "One-way Pad". As a result, it has potential security flaws. In order to resist quantum algorithm, we can combine the two systems together to make the two systems complement each other. The key idea of two-dimension chaos-multivariate is to add the outputs of multivariate cryptosystem and two-dimension system to demolish the potential mathematical properties of MPKCs. Thus, the hybrid system is secure under common attacks by using the center map of multivariate to change the initial state of chaos system and utilizing chaos system to generate the cipher texts.

3.1 Framework of proposed algorithm

Let X=(x_1, x_2,… x_n) denotes plaintexts and Y= (y_1, y_2,…, y_m) denotes the output of the cryptosystem. S and T are affine transformations. The diagram of proposed multivariate-chaos cryptosystem is depicted in Fig.1.

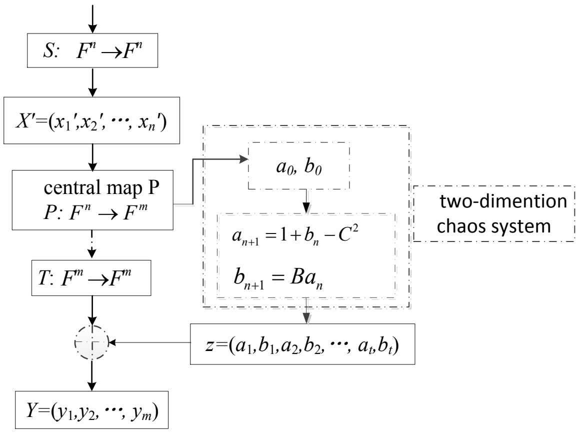

Fig.1. Diagram of multivariate branch chaos signature system

We first define an invertible affine transformation S: $F^n \to F^n$. Affine transformations cannot be directly used to develop cryptosystems because of the linearization relationship between inputs and outputs. We denote X'=(x_1', x_2',…, x_n') which are calculated using S-affine transformation with input parameter X.

Next, we construct a central map P: $F^n \to F^m$(m, n are integers and m is even). The central map consists of m equations with n variables in each equation. There are some existed central maps which can be utilized here, such as the central map of HFE, MI, UOV, TTS, etc. Though they are not secure, the disadvantages will be demolished in the following steps. The mathematic expression of above processes can be shown as Eq. (7).

$$Y' = (y_1', y_2', \dots, y_m') = P \circ S(X) \qquad (7)$$

Taken y'_1, y'_2 as initial stimulus in chaos system, the two-dimension chaotic algorithm is then calculated. After specifying parameters B and C, a two-dimension chaotic system is estimated as shown in Eq. (8).

$$z=(z_1,z_2,...,z_m)=H(a_0,b_0,B,C)=(a_1,b_1,a_2,b_2,...,a_t,b_t)$$

$$\begin{cases} a_0 = y'_1 \\ b_0 = y'_2 \\ a_{i+1} = 1+b_i-C^2 \\ b_{i+1} = Ba_i \\ i=0,1,...,t,\ t=m/2 \end{cases} \qquad (8)$$

Another invertible affine transformation T is applied with input Y'. Adding the outputs of T and chaotic system (i.e. z), the cipher texts are finally generated. The generic construction of the new public key signature system is shown in Eq. (9).

$$Y=F(X)=z \oplus (T \circ P \circ S(x)) \qquad (9)$$

The public key, i.e. polynomials of degree 2 over finite fields, is shown as Eq. (10).

$$Y=(y_1,...,y_m)=F(x_1,...,x_n)$$
$$=\begin{cases} y_1 = \sum_{j,k=1}^{n} \gamma_{1,j,k}x_jx_k + \sum_{j=1}^{n} \beta_{1,j}x_j + \alpha_1 \\ y_2 = \sum_{j,k=1}^{n} \gamma_{2,j,k}x_jx_k + \sum_{j=1}^{n} \beta_{2,j}x_j + \alpha_2 \\ \quad \dots\ \dots \\ y_m = \sum_{j,k=1}^{n} \gamma_{m,j,k}x_jx_k + \sum_{j=1}^{n} \beta_{m,j}x_j + \alpha_m \end{cases} \qquad (10)$$

And the private key consists of maps S,T, p and z.

3.2 Signature process

To sign a document, which is an element Y=(y_1,…,y_m), we need to solve the equation

$$Y=F(X)=T \circ P \circ S(x) \qquad (11)$$

We must apply the inverse of S, P and T. First, we have Y':

$$Y'=T^{-1}(Y) = P \circ S(x_1,…,x_n) \qquad (12)$$

Next, we need to calculate the inversion of central map P. In this case, we must solve the equation

$$P(x_1,\ldots,x_n)= Y' \qquad (13)$$

It should be pointed out that the central map P is not an invertible map. To overcome this problem, we can calculate the parity-check of $(y'_1,\ldots,y'_m)$, which can be presented as $(o_1,\ldots, o_{n-m})$, and plug them into Y'. As a result, the new equation is shown in Eq. (14).

$$P(x_1,...,x_n)=\overline{Y}=(\overline{y}_1,....,\overline{y}_n)$$
$$where \begin{cases} \overline{y}_i = y'_i, i=1,...,m \\ \overline{y}_i = o_{i-m}, i=m+1,...,n \end{cases} \qquad (14)$$

Thus, we can solve these invertible equations shown above and have all values of $(x'_1,\ldots,x'_n)$. Then we apply the inverse of S and estimate $X=(x_1,\ldots, x_n)=T^{-1}(X')$. In the next step, we will calculate chaos sequence. By taking y'_1, y'_2 as initial stimulus and specify parameters B and C, we can generate chaos sequence, which we denote by $z=(z_1,z_2,\ldots, z_n)$. We add the plain message Y and z and a new value $\overline{\overline{Y}}$ is calculated.

$$\overline{\overline{Y}} = Y \oplus z \qquad (15)$$

Again, taking $\overline{\overline{Y}}$ as plain messages and applying the inverse of affine transformation T, central map p and affine transformation S, we obtain a totally different values $X=(x_1,\ldots, x_n)$. Finally, the signature $s= (s_1, \ldots, s_{2n})$ is derived.

$$s = X \,\|\, z \qquad (16)$$

3.3 Verifying the signature

To verify the signature, one needs to decompose s to X and z first. And then, one must calculate

$$\overline{\overline{Y}} = F(X) \qquad (17)$$

Finally, one checks if indeed

$$Y = \overline{\overline{Y}} \oplus z \qquad (18)$$

4. Security Analysis

There is still no convincing, strict and scientific demonstration for the security of chaotic cryptography system [24-27]. At the same time, any effective solution isn't found too. The subtle changes of initial condition and non-linear property can cause great differences to results, which makes huge amounts of analytical methods for classical cryptography doesn't work on Chaos system. Common attacks which aim at Multivariate Public Key Cryptology System include bilinear attack, rank attack and differential attack, etc. The fundamental principle of bilinear attack is to establish bilinear relationship of plaintext/cipher-text pairs by using the characteristic that both sides of center map equations are linear transformations. Rank attack uses the smallest rank of linear combinations equations in center map and the number of occurrences of the variable which appears least to attack. Differential attack works by using the feature that differential function of center map is a linear relationship of differences. Algorithm proposed in this paper adds center map and chaos sequence together. Hence, it makes full use of the nonlinearity of chaos to prevent the above-mentioned various attacks based on linearity. As a result, signature generated by proposed system cannot be forged.

5. Conclusion

This paper proposes a hybrid signature algorithm combining multivariate public key cryptology system and chaos theory. Taking advantages of nonlinearity and unpredictability of chaos theory, the system is able to offset the matrix relationship between plain-texts and cipher-texts and demolish its potential mathematical structural weaknesses of multivariate public key cryptology system, and improve the security of signature algorithm. But the computing efficiency of proposed algorithm is probably slightly less than traditional MPKC. In conclusion, the proposed system can be applied to any kind of mobile devices whose computing power is not very high.

Acknowledgments

This work is supported by the established Project of Educational Office of Guangxi(Grant Nos:201106LX513;201106LX516) and Key Project of Yulin normal university(Grant No: 2012YJZD17)

References

[1] W. Diffie, M. Hellman, "New directions in cryptography", Information Theory, IEEE Transactions on, vol. 22, no. 6, 1976, pp.644-654.

[2] S. CX, Z. HG, F. DG, C. ZF, H. JW, "REVIEW ON INFORMATION SECURITY", SCIENCE CHINA, vol. 37, no. 2, 2007,pp.129-150.

[3] Gupta, Kamlesh, Silakari, Sanjay. ECC over RSA for Asymmetric Encryption: A review. International Journal of Computer Science Issues,vol.8, no.3-2, 2012, pp. 370-375.

[4] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory - TIT, vol. 31, no. 4, 1985,pp.469-472.

[5] N. Koblitz, "Elliptic curve cryptosystems", Mathematics of computation, vol. 48, no. 177, 1987,pp.203-209.

[6] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on, 1994, pp.124-134.

[7] W. W. Cao, L. Hu, Cryptanalysis of a Multivariate Public Key Encryption Scheme with Internal Perturbation Structure, Berlin: Springer-Verlag , 2009.

[8] H. Z. Wang, H. G. Zhang, Z. Y. Wang, M. Tang, "Extended multivariate public key cryptosystems with secure encryption function", Science China-Information Sciences, vol. 54, no. 6, 2011,pp.1161-1171.

[9] Y. Hashimoto, T. Takagi, K. Sakurai, General Fault Attacks on Multivariate Public Key Cryptosystems, Berlin: Springer-Verlag, 2011.

[10] T. Matsumoto, H. Imai, "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption", In Advances Cryptology -EUROCRYPT, 1988, pp.419-453.

[11] J. Patarin, "Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms", Advances in Cryptology-EUROCRYPT ’96, 1996, pp.33-48.

[12] A. Kipnis, J. Patarin, L. Goubin, "Unbalanced Oil and Vinegar signature schemes", Theory and Application of Cryptographic Techniques-EUROCRYPT'99, 1999, pp.206-222.

[13] J. Ding, J. E. Gower, D. Schmidt, Multivariate public key cryptosystems, New York: Springer, 2006.

[14] J. Patarin, N. Courtois, L. Goubin, "FLASH, a Fast Multivariate Signature Algorithm Topics in Cryptology—CT-RSA 2001", Cryptographers' Track at RSA, 2001, pp.298-307.

[15] H. Z. Wang, H. G. Zhang, H. M. Guan, H. Q. Han, "A new perturbation algorithm and enhancing security of SFLASH signature scheme", Science China-Information Sciences, vol. 53, no. 4, 2010, pp.760-768.

[16] V. Dubois, P. A. Fouque, A. Shamir, J. Stern, "Practical cryptanalysis of SFLASH", International Crytology Conference-CRYPTO 2007, 2007, pp.1-12.

[17] X. Y. Nie, Z. H. Xu, L. Lu, Y. J. Liao, Security Analysis of an Improved MFE Public Key Cryptosystem, Berlin: Springer-Verlag, 2011.

[18] J. C. Faugere, L. Perret, High Order Derivatives and Decomposition of Multivariate Polynomials, New York: Assoc Computing Machinery, 2009.

[19] D. Smith-Tone, On the Differential Security of Multivariate Public Key Cryptosystems, Berlin: Springer , 2011.

[20] C. Wolf, Multivariate quadratic polynomials in public key cryptography, Mierlo: Leuven, 2005.

[21] S.S. Qiu, Y.F. Chen, M. Wu, Z. Ma, "Discussion on Chaotic Secure Communication and New Schemes of Chaotic Encryption", Journal of South China University of Technology(Natural Science Edition), vol. 30, no. 11, 2002, pp.75-80.

[22] Y. Jing, G.J. shall, S.B. Yu, "An Improved Approach of Logistic Chaotic Series Encryption", Journal of Automatic Technology and Application, vol. 23, no. 2, 2004, pp.58-61.

[23]Ahadpour, Sodeif; Sadra, Yaser; ArastehFard, Zahra. “A Novel Chaotic Encryption Scheme based on Pseudorandom Bit Padding”, International Journal of Computer Science Issues,vol.9, no.11-2, 2012, pp. 449-456.

[24] L. Kocarev, "Chaos-based cryptography: a brief overview", Circuits and Systems Magazine, IEEE, vol. 1, no. 3, 2001, pp.6-21.

[25] Akhavan, A, Samsudin, A, Akhshani. “On the speed of ‘Image encryption with chaotically coupled chaotic maps’ ”, International Journal of Computer Science Issues,vol.9, no.3-3, 2012, pp. 452-454

[26] J. Amigó, Chaos-Based Cryptography Intelligent Computing Based on Chaos, Berlin : Springer /Heidelberg, 2009

[27] C. Pellicer-Lostao, R. Lopez-Ruiz, Notions of Chaotic Cryptography: Sketch of a Chaos based Cryptosystem, USA: arXiv, ,2012.

First Author Biographies

Xiaoyan Sun received the bachelor degree from Guangxi Normal University in 2004 and master degree in computer science from the school of mathematics & computing science in Guilin University of Electronic Technology. Currently, she is a lecturer at Yulin normal University, China. Her research interests include software protection and watermarking. She has published over 10 papers and 2 books on journals and/or international conferences. Her research has been supported by 8 provincial-level research projects.

Second Author Biographies

Maosheng Zhang received the bachelor degree from Hubei University in 2004 and master degree in mathematics from Dalian university of technology in 2009. He is a Ph.D. candidate of Wuhan University. Currently he is a lecturer at Yulin normal university. His research interests are in cryptography, watermarking and multimedia coding. He has published over 10 papers and 2 books on journals and/or international conferences and proposed 1 national standard and 2 national patent. He is an ACM member and his research has been supported by 6 provincial-level research projects.