Chaos Based Perturbation Encryption Algorithm

Xiaoyan Sun [1 a*]

[1]Guangxi Key Lab of Multi-source Information Mining & Security, Guangxi Normal University, Guilin 541004, China

[a]jgxysxy@126.com

Keywords: Computer; Cryptosystem; Chaos; Security; system

Abstract. Quantum computers challenge the security of traditional cryptosystems. In 2007, the first quantum computer was designed for practical use in Canada. As a consequence, the world wide used encryption systems such as RSA system, Elliptic Curve Cryptography are both unsecure. In this paper, a novel cryptosystem combining with multivariate cryptosystem and chaotic system is proposed. The plain-texts are encrypted using a traditional multivariate cryptosystem generated by users. A two-dimension chaos system is calculated at the same time and acts as an internal perturbation for multivariate cryptosystem. And then the cipher-texts are derived by adding the outputs of multivariate cryptosystem and chaos system. The analysis shows that the proposed system is able to resist common attacks of multivariate system including linear attack, rank attack and so on because of the non-linear property of chaos system. The proposed system is able to be used in terminal mobile since both the multivariate cryptosystem and chaos system are efficiently calculated.

Introduction

Public Key cryptosystems provide various security services such as confidentiality, credibility (identification), integrity, non-repudiation, usability, access control [2], etc. Currently, the main public key cryptography are RSA code and Elliptic Curve Cryptography (ECC) whose security are based on the complexity of big integer factorization and the difficulty of discrete logarithm respectively[3][4]. As both systems can be transformed to Generalized Discrete Fourier Transform (GDFT), Peter Shor from Bell Laboratories proposed an extension algorithm named Shor algorithm, which can be used to attack public key cryptosystem in polynomial time on quantum computers[5]. A Canadian company named D-Ware successfully manufactured a 28-bit quantum computer in 2007, and continued to bring out a 128-bit quantum computer in 2011 which was purchased by NASA for commercial use. As the speedy development of quantum computer technology, the public key cryptosystems are now facing increasing crucial threat[6]. Multivariate public key cryptosystem(MPKC) is a kind of alternative public cryptosystems which is secure under quantum computers[7]. Moreover, MPKC systems are generally much more computationally efficient than number theoretic-based or discrete logarithm-based schemes[8][9]. Typical multivariate public key cryptography includes cryptosystem developed by Matsumoto and Imai in 1988 (MI scheme)[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], etc. Unfortunately, those cryptosystems were broken out one after another. Combining multivariate public key cryptography and various trap-doors can improve the over-all security of cryptosystem, such as the subtraction mode can apparently improve the anti-attacking of multivariate public key cryptography. In 2004, a multivariate signature scheme named SFlash was accepted by NESSIE(New European Schemes for Signatures, Integrity and Encryption) for European standard of low energy consumption intelligent card[11]. As a matter of fact, SFlash was built on MI scheme with subtraction modification. Since the number of variables was less than equations, SFlash was not an invertible system and as a result, SFlash was acted as a signature scheme rather than cryptosystem. Though it was proved that SFlash was secure in 2004, Dubois forged a signature in one second utilizing the public key in 2007[12]. Although MPKC is theoretically able to resist quantum

computers, there are no practical multivariate cryptosystem so far. Taking advantages of various trap-door modification modes is a feasible solution to improve the security. Though there are many trap-doors are well researched, all the existing trap-doors have potential flaws. And this is why there is no available MPKC for practical applications.

This paper develops a novel MPKC system based on internal chaos trap-door for both encryption and signature. Plaintexts are first transformed through an affine transformation and then encrypted with a central map. The other affine transformation is applied to the outputs of central map. Meanwhile, a two-dimension chaos system is calculated. Adding the outputs of the MPKC and chaos system, the cipher texts are derived

Multivariate Public Key Cryptosystem

The building blocks of Multivariate Public Key Cryptology System are multivariate polynomials over a finite field. The mathematical structure of MPKC is shown in Eq. (1)[13,14].

$$Y=F(X)=T \circ P \circ S, \quad F_q^n \rightarrow F_q^m \tag{1}$$

Where q is a prime number and F_q^k is 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.

MPKC was very much inspired by the knowledge that solving a set of multivariate polynomial equations over a finite field, in general, is proven to be an NP-hard problem[16,17].

Multivariate-Chaos Cryptosystem

Framework of Proposed Algorithm.

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.

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.

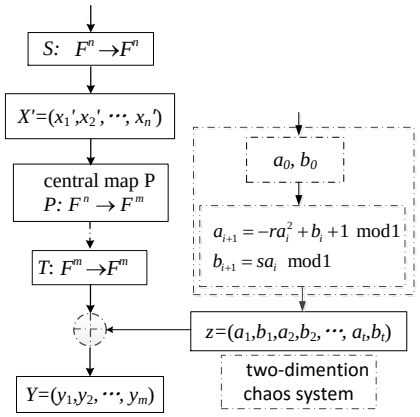

Figure 1. Diagram of multivariate branch chaos encryption system

We first define two invertible affine transformations $S: F^n \rightarrow F^n$ and $T: F^m \rightarrow F^m$. Affine transformations cannot be directly used to develop cryptosystems because of the linearization relationship between inputs and outputs. After applying transformation S, we get X'=(x_1', x_2',…, x_n'):$X'=(x_1', x_2', \ldots, x_n')=S(x_1, x_2, \ldots, x_n)$.

Next, we construct a central map $P: F^n \rightarrow F^m$($m \leqslant n$,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. (2).

$$Y' = (y_1', y_2', \ldots , y_m') = P \circ S(X) \tag{2}$$

Another invertible affine transformation T is applied with input Y' and the traditional MPKC is accomplished.

Taking a_0, b_0 as initial stimulus in chaos system and specifying parameters r and s, the two-dimension chaotic algorithm is then calculated as shown in Eq. (3).

$$\begin{aligned} z &= (z_1, z_2, ..., z_m) = H(a_0, b_0, r, s) \\ &= (a_1, b_1, a_2, b_2, ..., a_t, b_t) \end{aligned} \tag{3}$$
$$\begin{cases} a_{i+1} = -ra_i^2 + b_i + 1 \bmod 1 \\ b_{i+1} = sa_i \bmod 1 \\ i = 0,1,...,t,\ t = m/2 \end{cases}$$

Adding the outputs of T and chaotic system (i.e. z), the cipher texts are finally generated. The generic construction of the new encryption system is shown in Eq. (4).

$$Y=F(X)=z \oplus (T \circ P \circ S(x)) \tag{4}$$

The key of the proposed system is (S,T, p, z).

Encryption and Decryption Process. The encryption and decryption process are the same as symmetric cryptography. If parameters m and n be equal, the encryption process can be implemented efficiently. Let X=(x_1,…,x_n) be the plain texts, we apply eq.(12) to generate cipher texts Y=(y_1,…,y_n). On the other side, Y is easy to be converted to plaintexts. First, we can calculate z by using (a_0,b_0,r,s) through eq.4.

Next, we add z and Y to get U: U= (u_1, …, u_n)= $z \oplus$ Y=$T \circ P \circ S(x)$.

And then, we apply the inverse of T, P and S and finally we can obtain the original plain-texts X:

$$\begin{aligned} W &= (w_1, ..., w_n) = T^{-1}(U) \\ V &= (v_1, ..., v_n) = P^{-1}(W) \\ X &= (x_1, ..., x_n) = S^{-1}(V) \end{aligned} \tag{5}$$

Security Analysis

There are some specific structured-based attacks for MPKC such as bilinear equations attack, differential attack and rank attack[18][19].

Considering function F(x):

$$F(x) = \sum_{1 \le j \le k \le n} u_{jk} x_j x_k + \sum_{1 \le j \le n} b_j x_j + a \tag{6}$$

We generate a bilinear relationship between X and Y:

$$\sum_{0 \le j,k \le n-1} u_{jk} x_j y_k + \sum_{0 \le j \le n-1} \zeta_j x_j + \sum_{0 \le j \le n-1} \xi_j y_j + \eta = 0 \tag{7}$$

We can get a series plain-texts/cipher-texts pairs by using the public key. And thus, we obtain abundance of linear equations from eq.25 As a result, it is possible to estimate the plain-texts from cipher-texts. While in the proposed algorithm, the non-linear property of chaos system leads to the linear relationship doesn't come into existence.

Differential attack was proposed by Fouque, Granboulan and Stern in 2005. This method is a great challenge to MPKCs. The attack only needs the public key and can forge a signature after a one-time training in several minutes[20]. Given arbitrary function $\Im(x): F_q^{\ n} \rightarrow F_q^{\ m}$, the differential function is estimated by:

$$d\Im(x) = \Im(x+k) - \Im(x) \tag{8}$$

According to eq.(8) and eq.(2), the differential function of MPKC is derived:

$$\begin{aligned} &L_{F,k}(x) = dF_k(x) - dF_k(0) \\ &= F_k(x+k) - F_k(x) - F_k(k) + F_k(0) \end{aligned} \tag{9}$$

The signature can be forged because of the linearity of eq.(27). The differential function of the proposed system is given in Eq.(10).

$$\begin{aligned} &L_{\Im,k}(x) = Y(x+k) - Y(x) \\ &= z(x+k) \oplus (T \circ P \circ S(x+k)) \\ &-z(x) \oplus (T \circ P \circ S(x)) \end{aligned} \tag{10}$$

The subtle changes of initial condition and non-linear property can cause great differences to results, which makes the differential function is non-linearity[21]. As a result, differential equations attack doesn't work to the proposed system.

Rank attack was inspired by the knowledge that the minimum rank of linear combination of central map equations[21]. This method becomes a general attack algorithm for MPKCs since it broke HFE system. There are two kinds of rank attacks: low-rank attack and up-rank attack and the time complexity are as shown in eq.(11)(12) respectively.

$$q^{vt}(m^2(nv/2 - m/6) + mn^2v) \tag{11}$$

$$q^{u}(un^2 + n^3/6) \tag{12}$$

where $v = \lceil m/n \rceil$ denotes the minimum rank of linear combination of central map equations. As a matter of fact, the private key in the proposed system is not any more equations because of the perturbation of chaos system. As a consequence, the rank attack doesn't work for the proposed cryptosystem.

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.

Conclusions

This paper proposes a hybrid multivariate cryptosystem. Due to the nonlinearity and unpredictability of chaos theory of two-dimension, the linear relationship between plain-texts and cipher-texts in traditional multivariate cryptosystem is broken and the potential mathematical structural weaknesses are also demolished. However, 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. Though this system is able to resist general attacks, an open question derives from this system is that whether there are new attacks derived based on the novel framework. We will keep on researching on improving the security and efficiency of the proposed system in the near future.

Acknowledgment

This work is Supported by Nature Science Foundation of Guangxi Province (No.2014GXNSFBA118268, 2014GXNSFBA118010), Project of Guangxi Key Lab of Multi-source Information Mining & Security (No.MIMS13-06), Key project of Yulin normal university(No.2013YJZD04).

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.