Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **3**, May **2016**

A New Method of Encryption Algorithm Based on Chaos and ECC

Nan Jia, Songyan Liu*, Qun Ding, Shangru Wu, Xuming Pan

Electronic Engineering College
Heilongjiang University, Harbin 150076, China
313191115@qq.com, liusongyan@hlju.edu.cn, ding-qun@263.net,
shangruwu@foxmail.com, 1160639404@qq.com
*Corresponding author

Received January, 2016; revised March, 2016

Abstract. *Chaotic encryption algorithm represents a new encryption way with less memory consumption and operation time. However, the chaotic sequences will cause the phenomenon of short period due to the computational accuracy of hardware processing, which brings the security problem. The Elliptic Curve Cryptography (ECC), which is famous for its high efficiency, has been proved as one of the most safe and effective public key cryptosystems. But it is inefficient to improve the security from increasing the length of key. This paper aims to improve its security through combining the chaotic encryption algorithm and the ellipse encryption algorithm. In this paper, we design a encryption method that processes the plaintext using the one-dimension Logistic sequence before encrypting it to provide the first level of security, and encrypts it using ECC encryption algorithm which had been optimized to provide the second level of security. It does not only improve the security comparing with the individual algorithm, but also avoid the resource consumption caused by increasing the length of the key in ECC encryption system.*
Keywords: Encryption Scheme, Logistic sequence, ECC

1. **Introduction.** Chaos encryption [1, 2] is a random process in the deterministic algorithm. Its characteristic mainly represents in the sensitivity of initial value and in the impossibility of a long-term forecast and in the possibility of a short-term forecast. Due to the chaos encryption is sensitive to initial value, every small change will lead to exponentially growth in the iteration.

The security of the ECC is based on the intractability of the elliptic curve discrete logarithm problem. The elliptic curve discrete logarithm problem is much more difficult than the integer factorization problem [3] and discrete logarithm problem for finite field [4, 5] in computation. So, in terms of safety, elliptic curve cryptosystem has great advantages than others.

However, there are some limitations exist in the two method above. The limited precision problem of the hardware processer will bring a short period phenomenon of the binary sequences in the process of converting chaotic signal into binary sequences. Although ECC seems an efficient cryptography, the security is closely linked to the length of key. But, to increase the key length will increase computing time that gives a big challenge to ECC which has large numbers of complex operation.

In the past, researchers had accomplished a series of optimization researches in improving the security and reducing computing time of ECC using the Chaos. Liu et al.[6]

presented the pseudo random number produced by Chebyshev polynomial applied to knapsack cryptosystem. They combined the knapsack cryptosystem with elliptic curve cryptosystem to make the new elliptic curve cryptosystem more security. Sowmya, S. et al.[7] proposed a novel approach of generating pseudo random sequence based on cuclic elliptic curve. The resultant sequence of elliptic curve points was used as key sequence in an additive stream cipher system to encrypt images. Baheti, A. et al.[8] introduced an efficient symmetric encryption scheme based on a cyclic elliptic curve and chaotic system. The scheme generated pseudorandom bit sequences for round keys based on a piecewise nonlinear chaotic map. Then, the generated sequences are mixed with the key sequences derived from the cyclic elliptic curve points. The algorithms above are all using the chaotic method to generate pseudo random sequences and aiming at good encryption effect, large key space, high sensitivity and high processing speed.

This paper focuses on a new method that to improve the security from increasing the key space and enhancing the randomicity of the plaintext and ciphertext. We create an available pseudo random sequence to pre-process the plaintext before encrypting. In the method, we use the one-dimension Logistic map to pre-process the plaintext to make it random, and then use ECC to encrypt the message.

2. Proposed Algorithm.

This algorithm consists of two part: preprocessing and ECC encryption. Plaintext will be pre-processed by chaotic sequences before it enters into the ECC encryption system.

2.1. Preprocessing.

In this part, the plaintext will be encrypted by the Logistic sequence to make the plaintext from a readable message to a chaotic and unreadable sequence as the preprocessing of this algorithm. The one-dimensional Logistic map model is given as follow:

$$x_i + 1 = ux_i(1 - x_i)x_i, x_i \in [0, 1], u \in [0, 4]$$

(1) $u \in (0, 1)$, the system is stability in $x = 0$

(2) $u \in [1, 3]$, it has two stable points: $x = 0$ or $x = 1 - 1\frac{1}{\lambda}$

(3) $u \in (3, 1 + \sqrt{6})$, it has four stable points.

(4) $u \in (3.5699.., 4)$, the system enters to the chaotic state.

Preprocessing process:

(1) The initial parameters will be selected following the standard above by sender which will lead to the chaotic state: $x_0 \in [0, 1]$, $u \in [0, 4]$.

(2) Input plaintext m (the length of m is $klen$ bits).

(3) The number of iteration: $n = klen$. And get $w = w_0w_1w_2...w_n$ from quantizing the n-dimension iteration sequence [10] with the one-dimension Logistic model as:

$$w_n = \begin{cases} 0 & x_i > c \\ 1 & x_i \leq c \end{cases}, \quad \text{and } c = 0.5$$

(4) XOR w_n and the binary plaintext.

2.2. Key management.

Due to the different type of chaotic encryption scheme and ECC, it is difficult to manage the key. So we propose a method that embed the initial parameters of Logistic sequence into the message after preprocessing:

$$M = x_0||u||m \oplus w$$

In the step, x_0 and u will be expressed as two 32 bits binary number, and embedded into message as a certain order.

2.3. **The ECC encryption.** The message M will be encrypted as the follow steps which based on the SM2 [9].

(1) Select the system parameters of ECC $T(p, a, b, G, n)$, and the public key P_A of receiver's is available.

(2) The sender B select a random number as a private key k, and then figure out the public key :$C_1 = [k]G = (x_1, y_1)$.

(3) Obtain the points of Elliptic Curve after calculating by the formula $[k]P_A = (x_2, y_2)$, but the private key k of sender must be changed if x_2 =0.

(4) Key derivation function: $t = KDF(x_2||y_2, klen + 64)$.

(5) Get C_2 and C_3 by the function as follow:

$$C_2 = M \oplus t$$

$$C_3 = Hash(x_2 \| M \| y_2)$$

(6) Output the ciphertext $C = C_1||C_2||C_3$.

The flow chart of the encryption process as follow:

2.4. **Decryption process.** The receiver should do the steps as follow when he get the ciphertext.

(1)Get C_1 from C and calculate $[d_A]C_1 = (x_2, y_2)$.

(2) Key derivation function $t = KDF(x_2||y_2, klen64)$ is same as the step of encryption.

(3) Get C_2 from C, and then calculate $M' = C_2 \oplus t$.

(4) Calculate v=*Hash* $(x_2||M'||y_2)$.

(5) Get C_3 from C. Report error and output if $v \neq C_3$.

(6) Get x_0 and u from M', and get the quantitative n-dimension iteration sequence w' with the one-dimension Logistic model($n = klen$).

(7) Calculate $m' = M' \oplus w'$.

The decryption process presents in Fig.2:

3. Result and discussion.

3.1. **Processing time.** MATLAB simulation tool was used to simulate the proposed cryptographic scheme for different key size. The parameter setting is shown on table.1.

In Fig.3, the horizontal axis represents as different key size and vertical axis represents as the process time. It shows the simulation result by comparing key size and processing time for ECC and ECC based Chaos(L-ECC). From the results, we can infer that the method we proposed just takes a little more time than ECC.

3.2. **Safety analysis.** Based on the character of the Chaos and ECC, the new method will have a higher security than before.

3.2.1. *Ciphertext-only attack:* Ciphertext-only attack assume that the attacker has got the algorithm of the encryption and be able to intercept the ciphertext. The attackers must find the using key and the corresponding plaintext. The most common methods of ciphertext-only attack are brute-force attack and statistical attack and pattern attack. Brute-force attack requests the attacker knowing all the algorithms and key space and try them to make the plaintext seems meaningful. Statistical attack is to analysis the intrinsic attributes of the plaintext language. To resist this kind of attack should hide the statistic characteristic of the plaintext language. Pattern attack analyse the pattern of the ciphertext to get plaintext. Making the ciphertext looks like random as far as possible is an effective way to resist attacking.

In our method, we combine the randomicity of chaos and the high security of ECC to design a safer algorithm. For brute-force attack, because of the independence of the two

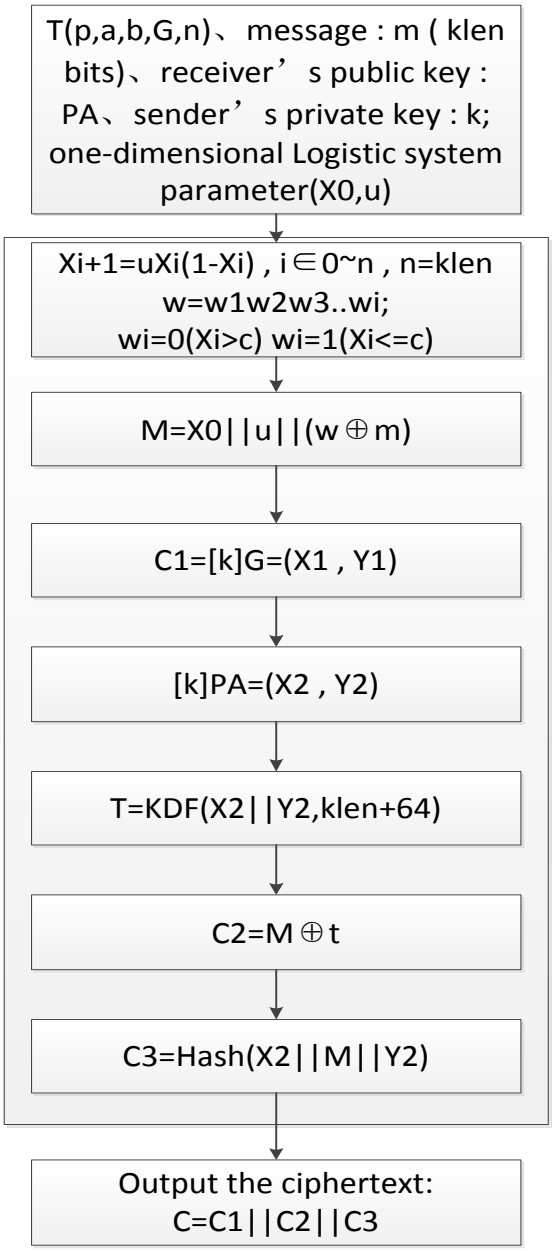

FIGURE 1. Encryption process

processes, attackers must get the right combination of the initial parameters of chaotic sequences and key of ECC to decrypt the ciphertext. The combination of chaotic and ECC will definitely increase the key space and make the brute-force attack more difficult.

we preprocess the plaintext with chaos to make it random. This process eliminats the statistical characteristics of the human language before the ECC encryption. These characters of our method can effectively resist the statistical attack and pattern attack.

3.2.2. *Known-plaintext attack:* Known-plaintext attack request for a pair of plaintext-ciphertext and the whole ciphertext. Attackers will decrypt the ciphertext by analyzing the relation of the pair of plaintext-ciphertext to decrypt the ciphertext.

Because of the randomness of the chaos, a little change will bring big deviation to the chaotic sequences. The different initial parameters of chaos will make the plaintext

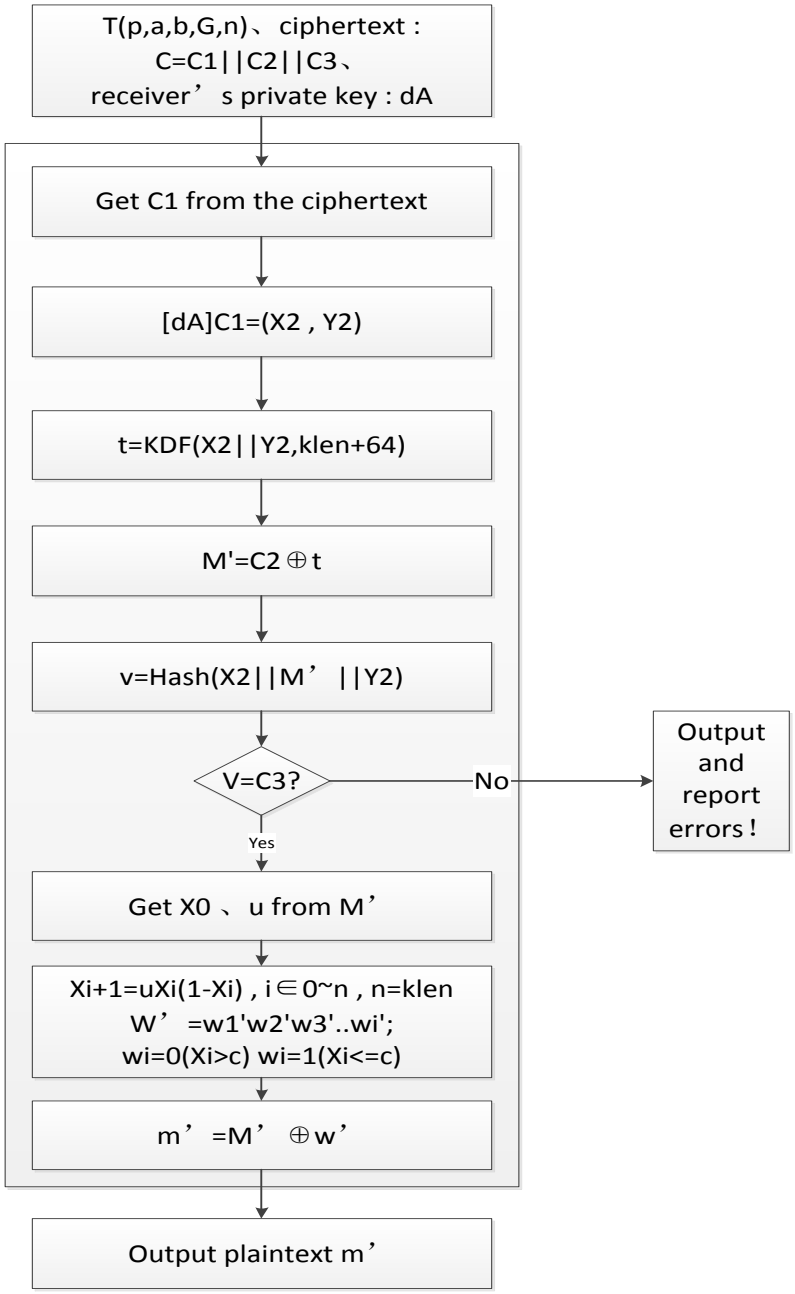

FIGURE 2. Decryption process

completely different after preprocessing. So it is impossible for attackers to infer the relation between the plaintext and ciphertext as a matter of experience.

In this method, we choose ECC to be the first level security. The main advantage of the elliptic curve encryption system is to use the smaller key length to reach higher security due to the intractability of the elliptic curve discrete logarithm problem. The character of ECC provide necessary security for the algorithm to resist the brute-force attack. The second level security is provided by chaos. It can not only make the plaintext random to resist the statistical attack and pattern attack, but also increase the key space to improve the ability to resist the brute-force attack.

If we use ECC individually, we have to increase the key length like other encryption algorithms to improve its security. It exactly brings some obstacles to the realization of

TABLE 1. Parameter setting

Processing of proposed algorithm	Parameter setting
Preprocessing	u= 0.75; x_0= 3.58; c=0.5;

ECC	P=8542D69E 4C044F18 E8B92435 BF6FF7DE 45728391 5C45517D 722EDB8B 08F1DFC3;
	a=787968B4 FA32C3FD 2417842E 73BBFEFF 2F3C848B 6831D7E0 EC65228B 3937E498;
	b=63E4C6D3 B23B0C84 9CF84241 484BFE48 F61D59A5 B16BA06E 6E12D1DA 27C5249A;
	G_x:421DEBD6 1B62EAB6 746434EB C3CC315E 32220B3B ADD50BDC 4C4E6C14 7FEDD43D;
	G_y:0680512B CBB42C07 D47349D2 153B70C4 E5D7FDFC BFA36EA1 A85841B9 E46E09A2;
	Plaintext: encryption algorithm;

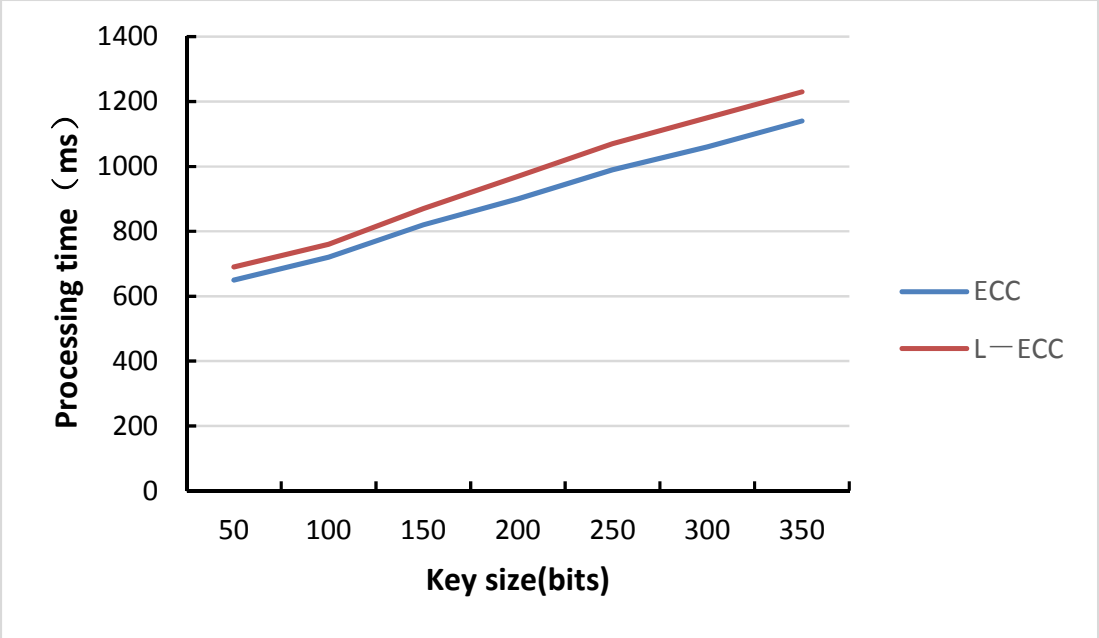

FIGURE 3. Processing time

the algorithm in computing time and resource usage. This algorithm on the basis of the original key length unchanged, pre-processing the plaintext before encrypting with the one-dimensional Logistic sequence and embed the parameter of chaotic into the result of preprocessor as the input plaintext post to the ECC encryption system. It is impossible to infer the plaintext M without the chaos initial value. The combination of chaotic encryption algorithm and elliptic curve encryption system not only solves the problem of that the elliptic curve encryption system must increases the length of the key to improve

the security, but also can solves the problem of the security of chaotic encryption algorithm itself and greatly improving the security.

4. **Conclusion.** This method is a new attempt of resisting the risk caused by the short period of the chaotic sequences. It improves the security of the single encryption, and also solves the pressure of operational of the complex ECC without increasing the length of the key only by adding two inputs (parameter u and initial value x_0). The experiment can show that the encryption/decryption system is attainable, and the message is completely same to input after the decryption process, without bias. It can ensure the integrity of the data, and proves that the algorithm is feasible. In terms of processing speed, the method we proposed just take little more time than the single ECC, but it provide a higher security at the same key size. It avoids the consumption of resource due to increasing the key size. So we consider it saves time at the same security compare with the single ECC.

Acknowledgment. This study is supported by the National Science of China under Grant No. 61471158. We tribute to Qun Ding, Professor of the key laboratory of electronic engineering college, who gave much help in the design and conduct of this study.

REFERENCES

[1] M. S. Baptista, Cryptography with chaos [J]. *Physics Letters A*, vol. 240, no.(s 1-2), pp. 50-54, 1998.
[2] T. Yang, C. W. Wu, L. O. Chua, Cryptography based on chaotic systems[J]. *IEEE Transactions on Circuits & Systems I Fundamental theory & Applications*, vol.44, no. 5, pp. 469-472, 1997.
[3] J. W. Bos, M. E. Kaihara, T. Kleinjung, A. K. Lenstra, P. L. Montgomery, On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography[J]. *Suite B Cryptography*, 2009.
[4] J. H. Silverman, J. Suzuki, Elliptic Curve Discrete Logarithms and the Index Calculus[A]. *ASIACRYPT'* 98[C]. Berlin: Springer-Verlag, vol. 1514, pp. 110-125, 1999.
[5] E. Teske, Speeding Up Pollard's Rho Method For Computing Discrete Logarithms[A]. *Algorithmic Number Theory*[C]. Berlin: Springer-verlag, vol. 1423, pp. 541–554, 1998.
[6] M. L. Liu, G. Z. Wei, G. Zhao, S. P. Zhang, Research on Elliptic Curve Cryptographic Algorithms Based on Chaotic System[C]. *Computer Sciences and Applications* (CSA), 2013 International Conference on, pp. 77-81, Dec. 2013.
[7] S. Sowmya, S. V. Sathyanarayana, Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points over GF(p)[C]. *Contemporary Computing and Informatics* (IC3I), 2014 International Conference on, pp. 1345-1350, Nov. 2014.
[8] A. Baheti, L. Singh, A. U. Khan, Proposed Method for Multimedia Data Security Using Cyclic Elliptic Curve, Chaotic System, and Authentication Using Neural Network[C]. *Communication Systems and Network Technologies* (CSNT), 2014 Fourth International Conference on, pp. 664-668, April 2014.
[9] Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves[S]. 2010.
[10] Y. B. Zheng, J. Pan, Y. Song, H. Cheng, Q. Ding, Research on the quantifications of chaotic random number generator[J]. *International Journal of Sensor Networks*, vol. 15, no. 1, pp. 139-143, 2014.
[11] L. P. Lee, K. W. Wong, A random number generator based on elliptic curve operations[J]. *Computers & Mathematics with Application*, vol.47, no. 2, pp. 217–226, 2004.
[12] E Wenger, P Wolfger. Harder, better, faster, stronger: elliptic curve discrete logarithm computations on FPGAs [J]. *Journal of Cryptographic Engineering*. pp. 1–11, 2015.
[13] S. P. Zhang, Y. Y. Chen, G. Zhao, K. Guo, A new elliptic curve cryptosystem algorithm based on the system of chebyshev polynomial[C]. *Information Technology and Artificial Intelligence Conference* (ITAIC), 2014 IEEE 7th Joint International, pp. 350-353, Dec. 2014.
[14] J. Pan, N. Qi, B. B. Xue, Qun Ding, Design and hardware implementation of FPGA & chaotic encryption-based wireless transmission system[A]. First International Conference on Instrumentation, Measurement, Computer, Communication and Control[C], vol. 10, pp. 691-695, 2011.
[15] J. Pan, Q. Ding, B. X. Du, A NEW IMPROVED SCHEME OF CHAOTIC MASKING SE SECURE COMMUNICATION BASED ON LORENZ SYSTEM[J]. *International Journal of Bifurcation & Chaos*, vol. 22, no. 5, pp. 56-64, 2012.

[16] Hongjun Wang, Bingbing Song, Qiang Liu, Jing Pan, Qun Ding. FPGA Design and Applicable Analysis of Discrete Chaotic Maps[J]. *International Journal of Bifurcation & Chaos*, vol. 24, no. 4, 2014.
[17] IEEE Std 1363-2000, Standard specifications for public-key cryptography [S].
[18] KOBLITZ N. Elliptic curve cryptosystem [J]. *Math Comput*, vol. 48, pp. 203-209, 1987.
[19] Tim Güneysu . Utilizing hard cores of modern FPGA devices for high-performance cryptography[J]. *Journal of Cryptographic Engineering*, vol. 1, no. 1, pp. 37-55, 2011.
[20] S. H. Islam, M. S. Farash, G. P. Biswas, M. K. Khan, M. S. Obaidat, A pairing-free certificateless digital multisig nature scheme using elliptic curve cryptography [J]. *International Journal of Computer Mathematics*, vol. 25, August, 2015.
[21] M. Bluhm, S. Gueron, Fast software implementation of binary elliptic curve cryptography[J]. *Journal of Cryptographic Engineering*, vol 5, no. 2, pp. 1-1, 2015.
[22] P. C. Realpe-Muñoz, J. Velasco-Medina. High-performance elliptic curve crypto processors over GF(2m) on Koblitz curves[J]. *Analog Integrated Circuits and Signal Processing*, vol. 85, no. 1, pp.129-138, 2015.
[23] ISO/IEC 15946, Information Technology: Security Techniques-Cryptographic Techniques based on elliptic curves [S]. *Committee Draft*, 1999.
[24] T. Y. Wu, T. T. Tsai, Y. M. Tseng, Efficient searchable ID-based encryption with a designated server[J]. *Annals of telecommunications*, vol. 69, no. 7, pp. 391-402, 2014.
[25] T.T. Tsai, Y.M. Tseng*, T.Y. Wu, Efficient revocable multi-receiver ID-based encryption[J]. *Information Technology and Control*, vol. 42, no. 2, pp. 159-169, 2013.