Artificial Immune Based Cryptography Optimization Algorithm

Xuanwu Zhou[1, 2], Kaihua Liu[1], Zhigang Jin [1], Shourong Tian[3], Yan Fu[1,3] and Lianmin Qin[3]
[1] School of Electronics and Information Engineering, Tianjin University, Tianjin 300072, China
[2] Command College of the Chinese Armed Police Forces, Tianjin 300250, China
[3] Administrative Centre of Yantai Tax-free Port, Yantai 265400, China
E-mail: schwoodchow@163.com

Keywords: artificial immune, cryptography optimization, blind signcryption, optimization coefficient, ECDSA

Received: November 8, 2012

In the paper, an improved clone selection algorithm for cryptography optimization is proposed, the algorithm integrates genetic algorithm with immune computing and makes use of reproduction and mutation operator to maintain the diversity and optimization of candidate objects. As an experiment of the clone algorithm, a blind signcryption scheme with immune optimized parameter is proposed. In the signcryption scheme, parameters generated with clone selection have relatively higher level of fitness and thus avoids the arbitrary selection of essential parameters. Then we analyze the efficiency and feasibility of immune optimization algorithms with experiment data from the signcryption scheme. The reproduction operator in the algorithm can greatly improve the fitness level of candidate group, while the mutation operator effectively maintains the diversity of candidate individuals. In the experiment, the optimization coefficient (OC) reaches 0.9301 when the clone algorithm is executed just once. Lastly, we make detailed comparison between the optimized signcryption scheme and other typical schemes, including the blind signature of D.Chaum and the ECDSA signature. The data from the experiment and comparison show that the optimization algorithm can effectively improve the efficiency and accuracy of parameter optimization in cryptography systems.

Povzetek: Predstavljen je izviren algoritem za kriptografsko optimizacijo, ki temelji na genetskih imunskih sistemih.

1 Introduction

Artificial immune system is an important branch of computation intelligence; it simulates the architecture and operating pattern of biological immune system and makes full use of the superior bionic mechanisms. In terms of computing ability, biological immune system is a self-adaptive and self-organized system with highly distributed and parallel architecture, and it has prominent capability in learning, recognition, memorizing and property extracting. Artificial immune system is an application-orientated model of biological immune system based on the bionic mechanisms; it also has superb capability in data processing and problem solving. Presently, artificial immune system has been widely applied in pattern recognition, intelligent optimizing, machine learning, data mining and information security, etc [1,2,3].

In traditional cryptography schemes, system parameters are simply generated with pseudo-random generator or the selection process is just overlooked. The arbitrary selection of system parameters makes the cryptography system more vulnerable to malicious attack. In order to reinforce the stability and security of cryptography algorithms, the random parameters can be generated by intelligent optimization algorithm with random selection.

In this paper, we propose an improved clone selection algorithm which integrates genetic algorithm with immune optimization algorithm. Then a signcryption scheme with immune optimized parameter is proposed as an experiment of the clone selection algorithm. Then the optimized signcryption scheme is compared with other typical schemes, including blind signature of D. Chaum and the ECDSA signature scheme. The signcryption scheme and the experiment show that the improved clone algorithm can effectively improve the efficiency and accuracy of parameter optimization in cryptography systems.

2 Artificial immune system and its algorithms

Artificial immune system (AIS) is a series of algorithms and systems based on the superior architecture and operating mechanism in biological immune system. Artificial immune system has a wide application in pattern recognition, intelligent optimizing, machine learning, data mining and information security, etc.

Biological immune system can recognize and clear invading pathogens, toxin, tumour cells from genetic mutation and prostrate cells to achieve immune defending effect and organism homeostasis. One of two immune responses is innate immune response taking rapid defending measures at first, which is fulfilled by skin, mucous membrane, phagocyte cells, natural killer,

compliments etc. The other is adaptive immune response that is mainly executed by T lymphocyte cells and B lymphocyte cells. The hierarchical defence structure of biological immune system is demonstrated in Figure 1[4,5,6].

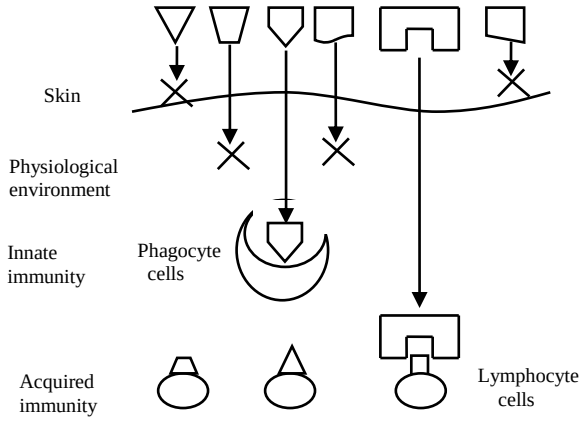

Figure 1: Hierarchical defence structure of biological immune system.

Biological immune system has superior ability to learn, memorize and recognize information, and its operating mechanism is characterized with self-organizing, distribution and diversity. Therefore many researchers have been applying the superior bionic mechanisms of biological immune system to develop corresponding models and algorithms in artificial immune system.

The basic bionic mechanisms of biological immune system can be categorized as: immune learning, immune memorizing, immune recognition, clone selection, diversity, distribution, self-adapting and immune network [7, 8].

Simulating the architecture and operating pattern of biological immune system, artificial immune system has three types of immune algorithms: basic immune algorithm, negative selection algorithm and clone selection algorithm.

Basic immune algorithm: generally, basic immune algorithms have similar searching strategy to genetic algorithms, and they also apply selecting and mutating in optimization.

Negative selection algorithm: this algorithm is based on the principles of negative selection in biological immune system. Negative selection provides protection against mistaken immune response toward normal organisms.

Clone selection algorithm: this algorithm is based on the principles of clone selection in biological immune system. In clone selection algorithms, individual objects will also undergo a process of clone reproduction with the stimulus from corresponding evaluation function (antigen). In the process of clone selection, the objects with higher suitability will be selected for reproduction and the suitability (affinity) and scale of these objects will also be gradually improved [9, 10, 11].

3 Immune optimization in cryptography schemes

In cryptography schemes, the proper selection of certain parameters is essential to the security and feasibility of the whole system. In many schemes, such parameters are simply generated with pseudo-random generator or the selection process is just overlooked. The arbitrary selection of system parameters makes the cryptography system more vulnerable to malicious attack. In the scheme, we introduce clone selection optimization into the design and analyzing of cryptography schemes, and put forward improved cryptography schemes with artificial immune optimization.

3.1 Parameter optimization algorithm

An optimized random parameter is first generated with clone selection algorithm.

(1) Encoding .The candidate parameters should first be encoded as a number string. In our example, we set the length of string as 4 bits.

(2) Initial group generating. The initial group is selected with random. And the number of individuals in the group is set as 5 for the convenience of computing. In our example, they are:

$$x_1= (0, 0, 0, 1),\ x_2= (0, 1, 1, 0),\ x_3= (1, 1, 1, 0),$$
$$x_4= (1, 0, 1, 0),\ x_5= (1, 0, 0, 1).$$

(3) Computing and evaluating of fitness. To evaluate the fitness of parameters, we use an objective function to decide the difference between selected strings. In our example, we use a linear function to compute the maximum function value as the standard of selection.

The objective function is set as:

$$f(x) = -x^2+2x+1. \quad (1)$$

Then we compute the function value of different strings.

$$f(x_1) = f(0001) =2,\ f(x_2) = f(0110) =-23,\ f(x_3) = f(1110) =-167,\ f(x_4) = f(1010) =-79,\ f(x_5) = f(1001) =-62.$$

(4) Reproduction of individuals. Mimicking clone selection of immune system, a certain number of individuals with high level of fitness should be selected for reproduction. In our example, two individuals with the highest level of fitness will be selected for reproduction, and the scale of reproduction is also directly proportional to its level of fitness.

The function value of string x_1, x_2 is the highest, so the two strings should be selected for reproduction to increase their perception in the whole group. In proportion to the level of fitness, string $x_1$will be reproduced twice, and string x_2 once.

Now, the temporary individuals in the group are:

$$x_1= (0, 0, 0, 1),\ x_1= (0, 0, 0, 1),\ x_1= (0, 0, 0, 1),$$
$$x_2= (0, 1, 1, 0),\ x_2= (0, 1, 1, 0),$$
$$x_3= (1, 1, 1, 0),\ x_4= (1, 0, 1, 0),\ x_5= (1, 0, 0, 1).$$

(5) Mutation. There are two mutation operations in the clone selection algorithm: crossover and self-mutation. In crossover mutation, two individuals are selected from the temporary group to develop into two new stings by

exchanging some value of the string. The probability of crossover is connected with the level of fitness in inverse proportion. In our example, string x_3, $x_4$and $x_5$have the lowest level of fitness, so$x_3$and x_5 are selected to exchange the latter two bits. And two new strings are generated [12, 13, 14].

x_6= (1, 1, 0, 1) , x_7= (1, 0, 1, 0) = x_4.

In self-mutation operation, the algorithm will change some bits in some selected strings, that is 0 to 1 or 1 to 0. The probability of mutation is also connected with the level of fitness in inverse proportion. In the example, x_4= (1, 0, 1, 0) has relatively lower level of fitness, and will be selected to change some bits of itself. And the new string is x_8= (0, 0, 1, 0).

(6) Repeating of algorithm. Then we should also compute the function value of the new strings, and make the decision of reproduction, mutation and discarding.

$f(x_1) = f(0001) =2$, $f(x_2) = f(0110) =-23$, $f(x_3) = f(1110) =-167$, $f(x_4) = f(1010) =-79$, $f(x_5) = f(1001) =-62$, $f(x_6) = f(1101) =-142$, $f(x_8) = f(0010) =1$.

Then the above operating algorithm will be repeated for certain times until the requirement is satisfied. In our example, the algorithm will be executed only once, and the final temporary strings in the group are:

x_1= (0, 0, 0, 1), x_1= (0, 0, 0, 1), x_1= (0, 0, 0, 1),
x_2= (0, 1, 1, 0), x_2= (0, 1, 1, 0),
x_3= (1, 1, 1, 0), x_4= (1, 0, 1, 0), x_5= (1, 0, 0, 1),
x_6= (1, 1, 0, 1), x_8= (0, 0, 1, 0).

After comparing the function values of different strings, the strings with the lowest fitness level will be excluded from the group. In this example, five strings with the lowest level of fitness should be excluded from the group to keep the stability of group scale, they are

x_3= (1, 1, 1, 0), x_6= (1, 1, 0, 1), x_4= (1, 0, 1, 0),
x_5= (1, 0, 0, 1) , x_2= (0, 1, 1, 0).

And the final optimized strings of the group are:

x_1= (0, 0, 0, 1), x_1= (0, 0, 0, 1), x_1= (0, 0, 0, 1),
x_2= (0, 1, 1, 0), x_8= (0, 0, 1, 0).

3.2 Immune optimized blind signcryption

In our scheme, the random parameter is generated with the above optimizing algorithm in advance, and other secret parameters of the scheme can also be generated with clone selection algorithm in advance.

Definition 3.2.1 (Elliptic Curve) an elliptic curve $E(F_q)$ over finite field F_q is a sextuple: T = (q , a , b , P , l , h), where P =(x_P , y_P) is the base point of $E(F_q)$, prime l is the order of P . As to $t \in Z_l^*, Q$ and $G \in E(F_q), Q = tG$ denotes multiple double additions on elliptic curve. O is the point at infinity, satisfying $lP = O$ and $G + O = G$ for any point $G \in E(F_q)$ [15,16,17].

Definition 3.2.2 (**ECDLP**, Elliptic Curve Discrete Logarithm Problem). ECDLP is the following computation

$x \leftarrow ECDLP(Q, P)$ (P is a base point and $Q \in \langle P \rangle$, $x \in Z_l^*$, $Q = xP$).

In the scheme, user *A* entrusts signcryption generator *B* to generate a signcryption for message $m \in Z_l^*$ without disclosing any information about it.

Φ = (GC , GK , BSC , USC)

Common parameters generation:

GC (1^k) =“On input (1^k) :

(T , H ,(E , D)) $\leftarrow GC$ (1^k) .”

T = (q , a , b , P , l , h)where P =(x_P , y_P) is the base point of $E(F_q)$, $ord(P) = l$ is a prime, O is the point at infinity. $H : \{0,1\}^* \rightarrow Z_l^*$, (E , D) is secure symmetric encryption/decryption algorithm.

Key pair generation:

GK (A,1^k) =“On input (A,1^k):

$sk_A \xleftarrow{\$} Z_l^*$, $PK_A = sk_A P \neq O$,

(sk_A , PK_A) $\leftarrow$.”

GK (B,1^k) =“On input (B,1^k):

$sk_B \xleftarrow{\$} Z_l^*$, $PK_B = sk_B P \neq O$,

(sk_B , PK_B) $\leftarrow$.”

Signcryption generating:

$BSC(sk_A, PK_B, m)$ =“On input (sk_B , PK_A , C):

$r \leftarrow_R Z_l^*$, $R = rP \neq O$,

$A \xrightarrow{R} Q$.

(u , v , w) $\leftarrow_R Z_l^*$, $U = uPK_B \neq O$,

$k = (U)_x \bmod(|E(\cdot)|)$,

$c = E_k(m)$, $h \leftarrow H(m \| ID_Q)$,

$F = (h + w)R - vP$, $e = (h + w) \bmod l$,

$A \xleftarrow{e} Q$.”

$t = (sk_A + er) \bmod l$, $i \leftarrow_R Z_l^*$, $I = iP \neq O$.

$A \xrightarrow{t} Q$.”

$s = u^{-1}(t - v - h) \bmod l$,

$A \xleftarrow{(c,h)} Q$.

$h' \leftarrow H(c \| (I)_x)$, $s' = (i - sk_A h') \bmod l$,

$A \xrightarrow{(h',s')} Q$.

$s'P + h'PK_A = iP = I$, $h' \stackrel{?}{=} H(c \| (I)_x)$,

C =(c , h , h' , s , s' , F).”

Unsigncryption algorithm:

USC (sk_B , PK_A , C)=“On input (sk_B , PK_A , C):

If $sk_B \notin Z_l^*$ or $PK_A \notin < P >$ return $\perp$,

Parse C into (c, h, s, F, h', s'),

If $s, s' \notin Z_l^*$ or $c \notin SP_E$ or $F \notin < P >$ return $\perp$, else

$$s^{-1} sk_B (PK_A + F - hP) = U,$$

$$k = (U)_x \bmod (|E(\cdot)|),\ m = D_k(c),$$

$$h\ ? = H(m \| ID_Q),$$

If the equation holds return m, else return $\perp$."

4 Analysis of the optimization scheme

Artificial immune optimization is the simulation of biological immune system and it is also an improved genetic algorithm with biological inheritance and natural selection mechanism. Clone selection algorithm in artificial immune system is an iteration algorithm. While searching for optimized group, clone selection generates a new improved individual from the original one; and from the improved one to another further improved one. Therefore, clone selection algorithm has much superiority in efficiency and stability compared with other optimization algorithm.

In our scheme, the optimization of random parameters is executed only once, but the fitness level of the strings has been greatly improved. The comparison can be made in the following table.

Initial group	Fitness level	Temporary group	Fitness level	Optimized group	Fitness level
x_1= (0, 0, 0, 1)	2	x_1= (0, 0, 0, 1)	2	x_1= (0, 0, 0, 1)	2
		x_1= (0, 0, 0, 1)	2		
x_2= (0, 1, 1, 0)	-23	x_1= (0, 0, 0, 1)	2	x_1= (0, 0, 0, 1)	2
		x_2= (0, 1, 1, 0)	-23		
x_3= (1, 1, 1, 0)	-167	x_2= (0, 1, 1, 0)	-23	x_1= (0, 0, 0, 1)	2
		x_3= (1, 1, 1, 0)	-167		
x_4= (1, 0, 1, 0)	-79	x_4= (1, 0, 1, 0)	-79	x_2= (0, 1, 1, 0)	-23
		x_5= (1, 0, 0, 1)	-62		
x_5= (1, 0, 0, 1)	-62	x_6= (1, 1, 0, 1)	-142	x_8= (0, 0, 1, 0)	1
		x_8= (0, 0, 1, 0)	1		
Sum of fitness	-229	Sum of fitness	-489	Sum of fitness	-16
Average level	-45.8	Average level	-48.9	Average level	-3.2

Table 1: Comparison of fitness level.

Definition: Let α is the average fitness level of the initial group, and β is the average fitness level of the temporary group or the optimized group, $\delta = \beta - \alpha$ is the difference between α and β, then optimization coefficient(OC) γ can be defined as the following formula.

$$\gamma = \frac{\delta}{|\alpha|} = \frac{\beta - \alpha}{|\alpha|}. \quad (2)$$

According to the definition of optimization coefficient, the smaller the value of γ, the weaker the optimization effect of clone selection algorithm on initial group. The larger the value of γ, the stronger the optimization effect of clone selection algorithm on initial group. When $\gamma > 0$, the algorithm has positive optimization effect on the group, when $\gamma < 0$, the algorithm has negative optimization effect on the group, When $\gamma = 0$, the algorithm has no optimization effect on the average level of the group.

In the above table, the average fitness level of the initial group is -45.8, after clone selection operation, the average fitness level of the optimized group is -3.2. The optimization coefficient γ between the initial group and the optimized group is 0.930131, the average fitness level of the initial group has been greatly improved by93.01%, and thus the optimization effect of clone selection algorithm proves to be remarkable.

Different immune operations render different optimization effect on the group. In reproduction operation, individuals with higher level of fitness will be reproduced to obtain their majority in the group, and thus the scale of the whole group will be improved. The average level of fitness will also be improved with the increase of ideal individuals. In mutation operation, new individuals can not necessarily be those with relatively higher level of fitness, therefore, the average level of fitness can not necessarily be improved. On the contrary, the fitness level will most probably be reduced. Yet, mutation operation in the immune optimization algorithm maintains the diversity of the candidate group.

The comparison of different clone operations can be made in the following table.

	Initial group	Temporary group with reproduction	Temporary group with mutation	Optimized group
Sum of fitness	-229	-348	-489	-16
Average level	-45.8	-43.5	-48.9	-3.2
OC γ		0.0502	-0.1241	0.9346

Table 2: Comparison of different optimization effect.

In the above table, the average fitness level of the initial group is -45.8, after reproduction operation, the fitness level is -43.5, and the optimization coefficient γ is 0.0502, the fitness level is improved by 5.02%. Yet, after mutation operation, the average fitness level is -48.9, the optimization coefficient γ is -0.1241, the average fitness level is reduced by 12.41%.With the discarding process, the scale of the group keeps stable, and the

fitness level is also improved with the discarding of improper individuals with low level of fitness. The average fitness level increases from -48.9 to -3.2 with a prominent optimization coefficient γ 0.9346, and the average fitness level is improved by 93.46%.

5 Comparison with other typical schemes

In this section, the proposed artificial immune based optimization algorithm and the optimized signcryption scheme will be compared with other typical schemes, including the famous blind signature put forward by D.Chaum and the ECDSA signature algorithm, which has been accepted as standard elliptic curve algorithm in many international standardization organizations, such as ISO14888-3, ANSI X9.62, IEEE1363-2000, etc.

5.1 Comparison with blind signature of D.Chaum

The signature algorithm for comparison in our scheme is based the original scheme put forward by D.Chaum and the security of the blind signature is based on elliptic curves cryptosystem.

(1)System parameter

F_q is a finite field (q is a prime number of n bits, $n \geq 190$), an elliptic curve on this finite field is defined as the following.

$$E: y^2 = x^3 + ax + b \ (a, b \in F_q, \ 4a^3 + 27b^2 (\mathrm{mod}\, q) \neq 0). \quad (3)$$

$P \in E(F_q)$ is a base point whose order is a large prime number l . $\#E(F_q)$ denotes the order of the elliptic curve which has a factor of large prime number larger than 160 bits [18, 19, 20].

$(P)_x$ is a function which makes the conversion from a point $P = (x, y)$ on elliptic curve to x . In the blind signature scheme, user A requires B to generate a blind signature of his message $m \in Z_l^*$ for him. ($K_A = k_A P$, k_A), ($K_B = k_B P$, k_B) are the public/private key pairs of A and B. In our scheme, the Hash function in signing algorithm is eliminated for simplicity, which can be easily added without loss of generality.

(2)Message blinding

Before generating signatures, the original user should blind the secret message with blinding parameters.

Step1: As to message $m \in Z_l^*$, User A randomly selects parameter $v \in Z_l^*$ and computes

$$m' = vm (\mathrm{mod}\, l) \quad (4)$$

$$V = v^{-1} P \quad (5)$$

Then he sends m' and V to B.

Step2: The blind signature generator B randomly selects $r \in Z_l^*$ and then computes

$$R = rV \neq 0 \quad (6)$$

$$t = m'(R)_x (\mathrm{mod}\, l) \quad (7)$$

$$s = r - k_B t (\mathrm{mod}\, l) \quad (8)$$

Then he sends (t , s) to user A.

(3)Signature generating

After getting the partial signature (t , s), user A computes the following to get the blind signature.

$$s' = v^{-1} s (\mathrm{mod}\, l) \quad (9)$$

$$t' = v^{-1} t (\mathrm{mod}\, l) \quad (10)$$

Then (s' , t') is the blind signature for message $m \in Z_l^*$ generated by entrusted signer B.

(4)Blind signature verifying

After getting blind signature (s' , t'), the signature verifier can testify the signature with the public key of the entrusted signer B.

$$R = s'P + t'K_B \quad (11)$$

$$t' ? = m(R)_x (\mathrm{mod}\, l) \quad (12)$$

If the formula holds, the verifier will accept (s' , t') as a valid blind signature of message $m \in Z_l^*$ [21, 22].

Remark 1. As a comparison, in the traditional schemes with random parameter selection, the parameters are selected without any optimization, such as in the step of message blind protocol (4) - (8). In these steps, parameters r and v are generated randomly without any optimization or selection standards. Many insecure parameters or weak keys will be selected to insure the security of the scheme, which will make the cryptography system more vulnerable to malicious attack. While with the proposed signcryption optimized algorithm, many insecure parameters or weak keys will be discarded or undergo the mutation process because of their low level of fitness.

5.2 Comparison with ECDSA signature

ECDSA signature scheme is as the following:

(1)System parameter

System parameters are the same as the above scheme, $k_A \in Z_l^*$ is the private key, $K_A = k_A P$ is the corresponding public key, $H: \{0,1\}^* \to Z_l^*$ is a secure one-way hash function.

(2) Signing algorithm

As to message $m \in Z_l^*$, the signer randomly selects parameter $u \in Z_l^*$ and computes

$$U = uP \neq 0, \quad (13)$$

$$e = H(m), \quad (14)$$

$$s = u^{-1}(e + k(U)_x)(\mathrm{mod}\, l). \quad (15)$$

$\sigma = (U, s)$ is the signature text.

(3)Verifying algorithm

After getting signature $\sigma = (U, s)$, the verifier can testify the signature with the public key of the signer.

$$w = s^{-1}, \quad (16)$$

$$u_1 = ew(\mathrm{mod}\, l), \quad (17)$$

$$u_2 = (U)_x w(\mathrm{mod}\, l), \quad (18)$$

$$(u_1 P + u_2 K)_x ?= (U)_x. \quad (19)$$

If the above formula is correct, the signature verifier will accept $\sigma = (U, s)$ as a valid signature of message $m \in Z_l^*$ [23, 24, 25].

Remark 2. Although ECDSA signature has been accepted as standard signature algorithm in elliptic curves, parameter $u \in Z_l^*$ in signature generating is still generated randomly without any optimization or selection to avoid weak keys and insecure parameters. Compared with the proposed scheme with immune optimization in the paper, ECDSA is more vulnerable to malicious attack, such as signature forgery and attack on the secret key for signing.

5.3 Comparison of performance

In this section, we will make a performance comparison between our immune optimized signcryption scheme and other traditional techniques, including the blind signature of D.Chaum and the ECDSA signature. To fulfil both the functions of encryption and signature as the proposed immune based blind signcryption, the above signature schemes must be improved with a secure symmetric encryption/decryption algorithm, for which the typical ElGamal encryption algorithm is selected with its simplicity and security. ElGamal public key encryption algorithm is as follows.

(1)System parameter

p is a large prime with binary length no less than 1024 such that $p-1$ has a large prime factor. $G = Z_p^*$ is a cyclic group under multiplication modulo p in which the discrete exponentiation function is conjectured to be one-way (meaning the discrete logarithm function is computationally hard) . g is the generator of group G ,meaning $G = \{g^0, g^1, \cdots, g^{l-1}\}$, where $l = |G|$ is the order (size) of G .

Then, as to any $x \in Z_l^*$, the computation of $y = g^x$ via x and g is called discrete exponentiation function, which is computationally feasible; but the computation of x via y and g is called discrete logarithm problem (DLP), which is computationally infeasible. $k \in Z_p^*$ is the private key, and $K = g^k$ is the public key.

(2)Encryption algorithm

As to message $m \in Z_p^*$, the sender randomly selects $r \in Z_p^*$, and computes

$$c_1 = g^r \ (\mathrm{mod}\ p), \quad (20)$$

$$c_2 = mK^r \ (\mathrm{mod}\ p). \quad (21)$$

Then (c_1 , c_2) is the cipher text.

(3)Decryption algorithm

$$c_2 \ (c^k{}_1)^{-1} = mK^r (g^{rk})^{-1}$$
$$= mg^{rk}(g^{rk})^{-1} \equiv m(\mathrm{mod}\ p). \quad (22)$$

In these schemes, such computing as modular exponential, modular inverse and elliptic curve addition ,elliptic curve scalar multiplication should be taken into comparison for computing complexity, while computing cost of modular addition, modular multiplication, hash, symmetric encryption/decryption are negligible. To ensure the security of basic cryptographic primitives, the minimum security parameters recommended for current practice are as follows: for DLP, |*p*|=1024bits, |*q*|=160bits. For RSA, |*N*|=1024bits; for ECC, |*q*|=131bits (79, 109 may also be chosen), |*l*|=160bits. The block length of the block cipher is 64bits. The length of secure hash function is 128bits.

Scheme	*GC+ GK*	*Sign*	*VF*	*Sum cost*	*IO*	*Length of C*
Blind signature	1*kP*	2*kP* +3*I*	2*kP*	5*kP* +3*I*	/	2 |*l*|
ECDSA	1*kP*	1*kP* +1*I*	2*kP*+ 1*I*	4*kP*+2*I*	/	|*l*|+ |*q*|
	GC+ GK	*EC*	*DC*			
Elgamal encryption	1*E*	2*E*	1*E*+1 *I*	4*E*+1*I*	/	2 |*p*|
	GC+ GK	*Sign and EC*	*VF and DC*			
Compound scheme 1	1*kP*+ 1*E*	2*kP* +2*E*+ 3*I*	2*kP*+ 1*E*+1 *I*	5*kP*+4 *E*+4*I*	/	2 |*l*|+ 2 |*p*|
Compound scheme 2	1*kP*+ 1*E*	1*kP* +2*E*+ 1*I*	2*kP*+ 1*E*+2 *I*	4*kP* +4*E*+ 3*I*	/	|*l*|+ |*q*|+ 2 |*p*|
	GC+ GK	*SC*	*USC*			
Immune based blind signcryption	2*kP*	4*kP* +1*I*	1*kP*+ 1 *I*	7*kP* +2*I*	*N*	|*E* (·) |+2|*h*|+ 2|*l*|

Table 3: Comparison of computing and communication cost.

Notes of notations: 1. *GC+GK* denotes the common parameters and key generation algorithms; *Sign/VF* denotes the signature/verification algorithms; *IO* denotes immune optimization algorithm; *EC/DC* denotes encryption/decryption algorithm; *SC* denotes the signcryption algorithm; *USC* denotes the unsigncryption algorithm; *Length of C* denotes the length of signcryption text /cipher-text/signature. *Compound scheme 1* is the scheme of blind signature+ Elgamal encryption;

Compound scheme 2 is the scheme of ECDSA+ Elgamal encryption. 2. *E* denotes modular exponential; *I* denotes modular inverse; *kP* denotes scalar multiplication on elliptic curves. / denotes there is no relevant computation. 3. |*E* (·) |denotes the block length of block cipher. 4. *N* denotes negligible.

In the above ECC and Elgamal based schemes, elliptic curve scalar multiplication *kP* and modular exponential $\alpha^k \bmod p$ are the most complex computations, so we will compare these two typical computations with the currently recommended security parameters:

(1) Elliptic curve scalar multiplication *kP*, where $P \in E(F_{2^l})$, *E* is a non-supersingular curve, $l \approx 160$， *k* is a random160-bit integer.

(2) Modular exponential $\alpha^k \bmod p$, where *p* is a 1024-bit prime and *k* is a random160-bit integer.

A field multiplication in F_q takes l^2 ($q= 2^l$) bit operations, then a modular multiplication in (2) takes $(1024/160)^2 \approx 41$times longer than a field multiplication in (1). Computation of *kP* by repeated doubling and adding on the average requires 160 elliptic curve doublings and 80 elliptic curve additions. From the addition formula for non-supersingular elliptic curves, an elliptic curve addition or doubling requires 1 field inversion and 2 field multiplications. The time to perform a field inversion is equivalent to that of 3 field multiplications. Hence, computing *kP* requires the equivalent of 1200 field multiplications, or $1024/41 \approx 29$ 1024-bit modular multiplications. On the other hand, computing $\alpha^k \bmod p$ by repeated squaring and multiplying requires an average of 240 1024-bit modular multiplications. Thus, the operation in (1) can be expected to be about $240/29 \approx 8$ times faster than the operation in (2) [26].

In the following table, the computation costs of the schemes are compared by the equivalence of $kP, \alpha^k \bmod p$ and field inversion to field multiplication in F_q ($q= 2^l$,$|q| \approx 160$bits).

Scheme	*GC+GK*	*Sign*	*VF*	*Sum cost*	*IO*	*Length of C*
Blind signature	1200	2409	2400	6009	/	320bits
ECDSA	1200	1203	2403	4806	/	291bits
	GC+GK	*EC*	*DC*			
Elgamal encryption	9840	19680	9881	39401	/	2048bits
	GC+GK	*Sign and EC*	*VF and DC*			
Compound scheme 1	11040	22089	12281	45410	/	2368bits
Compound scheme 2	11040	20883	12284	44207	/	2339bits
	GC+GK	*SC*	*USC*			
Immune based blind signcryption	2400	4803	2403	9606	*N*	640bits

Table 4: Comparison of computing and communication data.

Remark 1. (Comparison with compound scheme 1). Based on the result of Koblitz and Menezes [26], the computing cost in parameter and key generation in our scheme is 2400/11040 ≈ 1/5of that in compound scheme1; signcryption operation in ours is about $4803/22089 \approx 1/5$ of that in scheme1, and unsigncryption is about $2403/12281 \approx 1/5$ of that in scheme1. To sum up, our scheme reduces about 1-9606/45410 ≈ 78.9% commutating cost compared with compound scheme1.

Remark 2. (Comparison with compound scheme 2). As per the result of [26], the computing cost in parameter and key generation in our scheme is $2400/11040 \approx 1/5$of that in compound scheme2; signcryption operation in ours is about $4803/20883 \approx 1/5$ of that in scheme2, and unsigncryption is about 2403/12284 ≈ 1/5 of that in scheme2. To sum up, our scheme reduces about 1-9606/44207 ≈ 78.3% commutating cost compared with compound scheme2.

Remark 3. (Comparison of communication efficiency). The length of signcryption text in our scheme is 640/2368 ≈ 1/4of that in compound scheme1 and $640/2339 \approx 1/4$of that in compound scheme2; our scheme reduces about 1-640/2368 ≈ 73% communication cost compared with compound scheme1and reduces about 1-640/2339 ≈ 72.6% communication cost compared with compound scheme2.

Remark 4. Furthermore, the immune based optimization algorithm in our blind signcryption scheme is an algorithm of polynomial time complexity which can be neglected in the comparison of computation and communication efficiency. For specific application systems, the optimization algorithm can be executed in advance without any influence to the efficiency and designed as a separate computing unite which provide optimization service to other function units, such as encryption, signature, authentication, etc.

Therefore, the proposed cryptography optimization algorithm and the blind signcryption scheme prove to be more efficient and applicable to many security schemes in resource-restricted environment.

6 Conclusions

This paper studies the unique properties of biological immune system and optimization application in cryptography system. In the scheme, we introduce clone selection optimization into the design and analyzing of cryptography schemes, and put forward an improved signcryption scheme with artificial immune optimization. In the scheme, parameters with high level of security and fitness are selected as candidate individuals, and those with security problem or low level of fitness are rejected. On this basis, the final selection of parameters can be made with random mode. Thus the scheme avoids the security problems of other cryptography scheme and reinforces its stability, adaptability and robustness.

Acknowledgement

The authors should thank the anonymous reviewers for their constructive advice and comments to the paper,

with which we can improve our work clerically and academically.

References

[1] Han K H, Park K H. Parallel Quantum-inspired Genetic Algorithm for Combinatorial Optimization Problems, Proceedings of the CEC. Piscataway: IEEE Press, 2001:1442-1429.

[2] Xuanwu Zhou, Ping Wei,etc. Study on Proxy Signature Schemes with Bionic Optimization[C]. Proceedings of FITME'2009, IEEE Press. 2009, (Vol.3)365-368.

[3] D.W. Matolak, and B. Wang. Efficient Statistical Parallel Interference Cancellation for DS-CDMA in Rayleigh Fading Channels. IEEE Transactions On Wireless Communications, vol. 6, no. 2, pp.566-574, February 2007.

[4] Alexandra Boldyreva,Adriana Palacio,Bogdan Warinschi. Secure Proxy Signature Schemes for Delegation of Signing Rights [J]. Journal of Cryptology. 2012, 25(1): 57-115.

[5] Yong Yu,Yi Mu,Willy Susilo,ect. Provably secure proxy signature scheme from factorization[J]. Mathematical and Computer Modelling. 2012, 55(3-4): 1160-1168.

[6] Emura Keita,Miyaji Atsuko,Rahman Mohammad Shahriar. Dynamic attribute-based signcryption without random oracles[J]. International Journal of Applied Cryptography. 2012, 2(32): 199-211.

[7] Seung Hyun Seo;Kyu Young Choi;Jung Yeon Hwang;Seungjoo Kim. Efficient certificateless proxy signature scheme with provable security [J]. Information Sciences. 2012, 188: 322-337.

[8] Degabriele Paul,Paterson Kenny,Watson Gaven. Provable Security in the Real World[J]. IEEE Security & Privacy. 2011, 9(3): 33-41.

[9] Harendra Singh,Girraj Kumar Verma. ID-based proxy signature scheme with message recovery[J].Journal of Systems and Software. 2012, 85(1): 209-214.

[10] Xuanwu Zhou, Zhigang Jin, etc. Short Signcryption Scheme for the Internet of Things [J]. Informatica. Vol.35 (4) 521-530, 2011.

[11] Han Yu Lin;Chien Lung Hsu;Shih Kun Huang. Improved convertible authenticated encryption scheme with provable security[J]. Information Processing Letters. 2011, 111(13): 661-666.

[12] Tzong-Sun Wu;Han-Yu Lin;Pei-Yih Ting. A publicly verifiable PCAE scheme for confidential applications with proxydelegation[J].European Transactions on Telecommunications. 2012, 23(2): 172-185.

[13] Zhang Chuanrong. Zhang Yuqing . Li Fageng and Xiao Hong.: New Signcryption Algorithm for Secure Communication of ad hoc Networks. Journal of Communications, 2010, 31(3): 19-24.

[14] Han K H,Kim J H.Quantum-inspired Evolutionary Algorithms with a New Termination Criterion, Hε Gate, and two-phase Scheme. IEEE Transactions on Evolutionary Computation, 2004, 8(2):156-169.

[15] Gu Jingjing,Chen Songcan,Zhuang Yi. Wireless Sensor Networks-Based Topology Structure for the Internet of Things Location [J].Chinese Journal of Computer . 2010, 33(9): 1548-1556.

[16] Zhu Hongbo,Yang Longxiang,Yu Quan.Investigation of Technical Thought and Application Strategy for the Internet of Things [J]. Journal of Communication. 2010,31(11):2-9.

[17] Haipeng Zhang, Mitsuo Gen. Effective Genetic Approach for Optimizing Advanced Planning and Scheduling in Flexible Manufacturing System.GECCO'06, July 8-12, 2006, Seattle, Washington, USA.

[18] Z Luo, M Zhao, S Liu,ect. Generalized Parallel Interference Cancellation With Near-Optimal Detection Performance[J].IEEE Transactions On Signal Processing. 2008, 56(1): 304-312.

[19] Xuanwu Zhou. Elliptic Curves Cryptosystem Based Electronic Cash Scheme with Parameter Optimization [C]. Proceedings of KESE'2009, IEEE Press. 2009, 182-185.

[20] S Manohar, V Tikiya, R Annavajjala,etc. BER Optimal Linear Parallel Interference Cancellation for Multicarrier DSCDMA in Rayleigh Fading [J]. IEEE Transactions On Communications. 2007, 55(6): 1253-1265.

[21] Blundo C, Desantis A. Perfectly Secure Key Distribution for Dynamic Conferences. Advances in Cryptology-Crypto'92. New York: Springer-Verlag, 1993, 471-486.

[22] Keita Emura,Atsuko Miyaji,Mohammad Shahriar Rahman. Dynamic Attribute–based Signcryption without Random Oracles[J].International Journal of Applied Cryptography,2012,2(3):199-211.

[23] Xu Peng,Cui Guohua,Lei Fengfu, Tang Xueming, Chen Jing. An Efficient and Provably Secure IBE Scheme Under the Standard Model[J].Chinese Journal of Computer . 2010, 33(2): 335-1556.

[24] Xuanwu Zhou. Elliptic Curves Cryptosystem Based Electronic Cash Scheme with Parameter Optimization[C]. Proceedings of KESE'2009, IEEE Press. 2009, 182-185.

[25] Kim Y K,Park K,Ko J.A symbiotic evolutionary algorithm for the integration of process planning and job shop scheduling. Computers and Operations Research.2003, 30:1151- 1171.

[26] Koblitz N, Menezes A and Vanstone S. The State of Elliptic Curve Cryptography [J]. Designs, Codes and Cryptography, 2000, 30(19): 173-193.