Hybrid Differential Evolutionary Algorithms for Koblitz Elliptic Curves Generating

Junhua Ku[12]
[1]Department of Information Engineering, Hainan Institute of Science & Technology, Haikou ,China
[2]School of Computer Science China University of Geosciences, Wuhan, China
Email:kujunhua@163.com

Zhihua Cai
School of Computer Science China University of Geosciences, Wuhan, China

Xiuying Yang
Department of Information Engineering, Hainan Institute of Science & Technology, Haikou ,China

Abstract—Elliptic curve cryptography(ECC) is one of the most important public key cryptography. The koblitz curve is a special kind of elliptic curve in ECC. The e1liptic curve cryptosystem (ECC) which is based on elliptic curve discrete logarithm problem. As of today the security of an ECC is determined by the cardinality of $E(\mathrm{F}_q)$ (the set of rational points of E over F_q). Based on the hybrid differential evolutionary algorithms and the evolutionary cryptography theory, we proposed a new a1gorithm to generate secure Koblitz ECC. Traveling Salesman Problems (TSP) is the well-known combinatorial optimization problem. And the optimal solution can not be found in polynomial time. So the approximation algorithm with polynomial algorithm for TSP has been an important topic in this field. PODE was proposed for TSP by incorporating Position-Order Encoding(POE) into DE. PODE is effective for small-size TSP and less effective for middle-size TSP. We deveplp a new hybrid differential evolution algorithm, which improves PODE by using hill-climbing operator as the local search algorithm, is proposed for middle-size TSP. The experimental results show that the generation efficiency of secure curves generated is superior to the parameters recommended by NIST.

Keywords-Koblitz elliptic curve; Differential Evolutionary; Hybrid Differential Evolutionary;Evolutionary Cryptography; Elliptic Curves Generating

I. INTRODUCTION

The e1liptic curve cryptosystem (ECC) which is based on elliptic curve discrete logarithm problem was proposed by Neal Koblilz[l] in 1987. It has advantage of high security, small occupied bandwidth and low computational complexity, so it has gradually been included in standard recommended by IEEE, ANS1, IS0, NIST etc. Especially, 15 curves recommended by NIST have been frequently chosen by the engineering applications.

Cloud-Computing[2] developed rapidly in recent years，The hacker can easily get high-performance computing ability with the cloud-computing open service and powerful computing ability to attack a cryptosystems. So it is necessary to search a new method to easily and quickly generate secure ECC curves. The secure level should be higher than the current secure curves recommended by NIST.

In 2002, Zhang Huanguo et al. proposed the Evolutionary cryptography theory[3]. Evolutionary cryptography theory becomes a principal concept for cryptography design and cryptanalysis. Based on the hybrid differential evolutionary algorithms, we proposed a new a1gorithm to generate secure Koblitz ECC. The experimental results show that the generation efficiency of secure curves generated are superior to the parameters recommended by NIST..

II. KOBLITZ ELLIPTIC CURVES

The Koblitz elliptic curve is a curve defined in domain F_2, its definition is as follows:

$$E_0 : y^2 + xy = x^3 + 1 \tag{1}$$

$$E_1 : y^2 + xy = x^3 + x^2 + 1 \tag{2}$$

That is to say, a=1 or a=0. When l is a factor of m, then $E_a(\mathrm{F}_{2^l})$ is a subgroup of $E_a(\mathrm{F}_{2^m})$, so $\#E_a(\mathrm{F}_{2^m})$ can be divided exactly by $\#E_a(\mathrm{F}_{2^l})$,we know that $\#E_0(\mathrm{F}_2) = 4$ and $\#E_1(\mathrm{F}_2) = 2$, we can easily obtain that $\#E_0(\mathrm{F}_{2^m})$ is the multiple of 4,and $\#E_1(\mathrm{F}_{2^m})$ is the multiple of 2.

In 2000 NIST FIPS 186-2[4] recommended 5 security Koblitz ECs in domain $\mathrm{F}(2^{163})$, $\mathrm{F}(2^{233})$, $\mathrm{F}(2^{283})$, $\mathrm{F}(2^{409})$ and $\mathrm{F}(2^{571})$. At present, secure ECs selecting methods can be divided into two kinds: complex multiplication (CM) method and random curve selection method. The security of EC depends on the size of the EC order. The common methods for computing order include Schoof's algorithm[5], SEA (Schoof-Elkies-Atkin) algorithm[6], Satoh algorithm[7] and so on.

Overall, there is no better method proposed in recent years. The SEA algorithm is still the most secure but time-consuming method and the traditional pure mathematics severely restricts the development of ECC. So we need to search for other new methods. We design an hybrid differential evolutionary model for searching safe general field by referring the application in TSP (Traveling Salesman Problems).

III. THE PROPOSED HYBRID DIFFERENTIAL EVOLUTIONARY ALGORITHMS(HDE)

Differential Evolutionary Algorithm(DE)[8] is a new evolutionary computational method proposed by Storm in 1995.PODE[9]was proposed for TSP by incorporating Position-Order Encoding(POE) into DE. PODE is effective for small-size TSP and less effective for middle-size TSP. A new hybrid differential evolution algorithm, which improves PODE by using hill-climbing operator as the local search algorithm is proposed for middle-size TSP. It is composed of two steps.

Step1. The use of PODE

Firstly, Generate initialize population $\{X_{i,0}|i=1,\ldots,NP\}$.

Secondly, use the operation of mutation, crossover and selection, respectively. The rules of mutation are described by the following equations:

$$V_{i,g} = X_{r_1,g} + F \times \left(X_{r_2,g} - X_{r_3,g} \right) \qquad (3)$$

Where the indices r1,r2 and r3 are uniformly chosen from the set {1, 2,.., *NP*}\{i},are distinct integers. F is mutation factor which is fixed parameter.

The rules of crossover are described by the following equations:

$$u_{j,i,g} = \begin{cases} v_{j,i,g}, & \text{if } rand(0,1) \le \mathrm{CR} \ \text{ or } \ \mathrm{j} = \mathrm{j}_{rand} \\ x_{j,i,g}, & \text{otherwise} \end{cases} \qquad (4)$$

Where rand(0,1) is uniform random number on the interval [0,1], j_{rand} is an random integer chosen from 1 to N and new for each *i* and the crossover probability CR is a fixed parameter.

The rules of selection are described by the following equations:

$$X_{i,g+1} = \begin{cases} U_{i,g}, & \text{if } f(\mathrm{Ord}(U_{i,g})) < f(C_{i,g}) \\ X_{i,g}, & \text{otherwise} \end{cases} \qquad (5)$$

Step 2 the use of Hill-Climbing operator

Before the Hill-Climbing operator, we need the Position-Order Operator: At generation *g*, this operator creates a solution $C_{i,g}$ for TSP based on the current population $\{X_{i,g}|i=1,2,\ldots, NP\}$ in DE. The following is the form of position-order operator.

$$C_{i,g} = Ord(X_{i,g}) = (Ord(x_{1,i,g}), Ord(x_{2,i,g}), \cdots, Ord(x_{N,i,g})) \qquad (6)$$

where, Ord($x_{j,i,g}$) is the index of the element $x_{j,i,g}$ after all the elements in vector $X_{i,g}$=($x_{1,i,g}$, $x_{2,i,g}$,…, $x_{N,i,g}$) are sorted from small to large.

Based on experimental evidence, we believe that DE with Position-Order operator performances poorly when solving middle-size TSP. In view of local search algorithm improving the solutions for TSP[10], a new hill-climbing operator is proposed to improve DE with position-order operator. In the hill-climbing operator, the neighborhood of the current solution is generated and the better of the two solutions is preserved for every iterative. In order to get the neighborhood solution, swap operator, reverse edge operator and insert operator are used in hill-climbing operator.

a)Swap Operator:

The operator generate the neighborhood solution by reversing the cities of two locations in the current solution for TSP.

b) Reverse Edge Operator:

The operator generate the neighborhood solution by swapping the order of two edges in the current solution for TSP. The neighborhood is the solution after reversing edge. Edges is served as the operation object in Reverse Edge operator. So it causes large change of the current solution.

c) Insert Operator:

The operator generate the neighborhood solution by inserting the city with the specified location into another specified location in the current solution for TSP.

Based on the above three operators, the algorithm of hill-climbing is shown as following (Algorithm 1.).

Algorithm 1: The Algorithm of Hill-climbing

1	X= a feasible solution of N cities	12	if f(X_1)<f(X) then
2	j_1= randint(1, 2N/3)	13	X=X_1
3	for j= j_1 to j_1+N/3	14	else
4	for k=1 to N	15	X_1=Insert(X,m_1,m_2); // insert operator
5	X_1=Swap(X,j,k); // swap operator	16	if f(X_1)<f(X) then
6	if f(X_1)<f(X) then	17	X=X_1;

```
X=X_1;
end
m_1=min(j,k);
m_2=max(j,k);
X_1=ReverseEdge(X,m_1,m_2);
end
end
next k
next j
return X;
```

Hybrid differential evolutionary algorithm is composed of two steps: firstly DE with position-order operator is called as a global optimization algorithm; secondly hill-climbing operator is called on the basis of the solution gotten from the first step. The pseudo-code of HDE is shown as following(Algorithm 2.).

Algorithm 2: The Algorithm of HDE

```
//first step:PODE
generate initialize population {$X_{i,0}$|i=1,…,NP}
$C_{i,0}$=Ord($X_{i,0}$)  {$i=1,...,NP$}
for g=0 to max_iterations
for i=1 to NP
Vi,g gotten from {Xi,g|i=1,…,NP}DE mutation
$U_{i,g}$gotten from {$X_{i,g}$,$V_{i,g}$|i=1,…,NP} //DE crossover
if f(Ord(Ui,g))<f($C_{i,g}$) then //DE selection
$X_{i+1,g}$=$U_{i,g}$
$C_{i+1,g}$=Ord(Ui,g)
$X_{i+1,g}$
$C_{i+1,g}$ =$C_{i,g}$
end
next i
next g
//second step: HillClimbing operator
for i=1 to NP
New_$C_i$=HillCliming(Ci,max_iterations)
next i
$C_{best}$=the best from {New_$C_i$ |i=1…NP}
```

IV. THE EXPERIMENTAL RESULT AND ANALYSIS

PC:T5450@1.66GHz 1.67GHz, RAM:3.0G, HDD:500G.

Software platform: Matlab 2013b.

In our experiments, we employ the same selecting standards recommended by the ANSI[27],so it is secure enough for our elliptic curves.

we search secure base fields for both kinds of the Koblitz ECs over [2^{160},2^{600}], and we obtain the secure EC base field exceeding 571 bit.

As the kind of a=0,b=1 Koblitz ECs, we find a total of 15 secure base fields:5,7,13,19,23,41,83,97, 103, 107, 131,239,349,409,571.There are four base fields whose size goes beyond 163. For the kind of a=1,b=1 Koblitz ECs. we find a total of 15 secure base fields:5,7,11,17,19,23,101,107,131, 163,283,311,359.There are 4 base fields whose size goes beyond 163. Here we list the specific parameters of the Koblitz elliptic curve in domain F(2^{163}) , F(2^{233}) , F(2^{409}) and F(2^{571}) in Figure 1.

Figure 1. the specific parameters of the special Koblitz elliptic curve .

a,b,	m	p(t)	n	Gx	Gy
a=0, b=1	233	t233+t74+ 1	3450873173395281893717377138512760570940988862252126328087024741343	0X1CD4147A6FF9F38FD22AA837A7CAA837A7C779FC97BF996D22F9E73E4B0424F66C3	0X16920A80536B1CC4792B1611C0A78D79F7823CFDBAEBF0CBFBC940DF423
	409	t409+t87+	330527984395124299475957654	0X1067E7B22DAB059BD122D	0X4EEE2AB519E518A978E5A35

		1	016385519914202341482140609642324395022807112892491910506732584577774580140963665906177315867	14C49E14A008D3C926ED4DC105F0C2B65985099A11B97C200A43F6F465F7A4A8F6A3A9121BD71B614	E7B72F96C787E15F92FC6AA72D9DE68B3E2A0ED1AEC286D67B3C24AC71494DF34E381D67BDBFE2A
	571	t71+t10+t5+t2+1	19322687615086291723476759454659936721494636648532174993286125725759571144780212268133978522706706711834706712800825351461273674974066617311929682421617092503555733685276673	0X69E202A15A4739E0FEEECDA1B171AB07AC08EC3636977018FCF52D2BF797DFD9E2919EEA9541D832EE8E37DDC92700379F5CBDBF1468B63582FECABDADA8AD94A21EF894D82F454	0X28C3E1D87E305274B9AC6279532E328BE6A607CAB089FC343008E22E46E9ADD451DFCBF8798E765A44340D9195B0DBE98B08B95D7377AF5B0EBDD1CF13DAD6DC8A3D5EA7FF0A71
a=1, b=1	163	t163+t7+t3+1	5846006549323611672814741753598448348329118574063	0X6243C77BD6DACAC2D474C9CF4E30725773B777EB8	0X3E996C6AB516545F86D4B7CEE7633B358C5F793D9

V. CONCLUSIONS

we proposed a secure curve selection algorithm based on Hybrid differential evolutionary algorithm to select secure base field of Koblitz elliptic curves. We have preliminarily completed base field and base point generating experiment for koblitz elliptic curve over[2163,2600]. The experiment results contain the 4 Koblitz elliptic curves recommended by NIST.

VI. ACKNOWLEDGMENT

This work was supported by the Natural Science Foundation of Hainan province under Grant No. 614248, the Young and middle-aged scientific research projects of Hainan Institute of Science and Technology under grant No.HKYZQJ2014-05.

REFERENCES

[1] KOBLITZ N. Elliptic Curve Cryptosystems[J].Mathematics of Computation,1987,48:203-309.

[2] OWENS D. Securing Elasticity in Cloud[J].Communication of the ACM,2010,53:46-51.

[3] Zhang Huanguo et al. Evolutionary Cryptosystems and Evolutionary Design for DES[J]Journal of China Institute of Communication,2002,5(23):57-64.

[4] NIST. Digital Signature Standard[S].Federal Information Processing Standards Publication, January,2000.

[5] SCHOOF R. Elliptic Curves Over Finite Fields and the Computation of Square Roots Mod P[J].Mathematics of Computation,1985,44:483-494.

[6] SATOH T. et.al. Fast Computation of Canonical Lift of Elliptic Curves and its Point Counting[J]. Finite Fields and Their Application,2003,9:98-101.

[7] SATOH T. The Canonical Lift of an Ordinary Elliptic Curves Over Finite Fields and its Point Counting[J].J Ramanuian Math Soc,2000,15,483.

[8] R. Storn and K. Price, "Differential evolution simple and efficient heuristic for global optimization over continuous spaces," Journal of global optimization, vol. 11, pp. 341-359, 1997.

[9] H. Yi-chao, et al., "Differential evolution algorithm with position-order encoding for solving traveling salesman problem,"Journal of Computer Applications, vol. 3, 2007.

[10] Q. Z. Yuan, et al., "Hybrid genetic algorithm for TSP," Jisuanji Gongcheng yu Yingyong(Computer Engineering and Applications), vol. 45, 2009.