Research Paper

Volume : 2 | Issue : 10 | October 2013 • ISSN No 2277 - 8179

Proposed Approach for Elliptic Curve Cryptography Based on Metaheuristic Algorithms

Computer Science

KEYWORDS : Elliptic curve, Key exchange, Cryptography protocols, metaheuristic algorithms

Hala Bahjat Abdul Wahab	Computer Sciences Department, University of Technology, Baghdad, Iraq
Suhad Malallah Kadhem	Computer Sciences Department, University of Technology, Baghdad, Iraq.
Estabraq Abdul Redaa Kadhim	Computer Sciences Department, University of Technology, Baghdad, Iraq

ABSTRACT

Elliptic Curve Cryptography (ECC) has attracted the attention of researchers and product developers due to its robust mathematical structure and highest security compared to other existing algorithms. This paper produced a new approach for elliptic curve cryptosystem take behavioral symmetric cryptographic system instead of asymmetric cryptographic system by investigate from Metaheuristic algorithms (Greedy Randomized Adaptive Search Procedure (GRASP) and Variable Neighborhood Search(VNS)) in order generate symmetric mask key (i.e. produced symmetric key consist of more the one ECC points). The proposed approach aim to combine between the features of Elliptic Curve Discrete logarithm, mathematics and Metaheuristic algorithms (GRASP and VNS) to produce robust symmetric mask key. The most important feature of this mask key it must have a minimum correlation among points . (i.e. Minimum correlation provide randomness on the mask key) . The proposed approach tested using visual prolog language by performs the encryption and decryption processes using text and gives efficient results.

INTRODUCTION

Elliptic curve cryptography (ECC) provide a faster alternative for public key cryptography .Much smaller key lengths are required with ECC to provide a desired level of security, which means faster key exchange, user authentication, signature generation and verification, in addition to smaller key storage needs. The security of ECC has not been proven but it is based on the difficulty of computing elliptic curve discrete logarithm in the elliptic curve group [1]. Metaheuristics are designed and play important role with complex optimization problems .The applicability of metaheuristics as a preferred method over other optimization methods is primarily to find good heuristic solutions to complex optimization problems with many local optima. The metaheuristic approach aim to solving such problem started by obtaining an initial solution or an initial set of solutions, and then initiating an improving search guided by certain principles [2].

Greedy Randomized Adaptive Search Procedure (GRASP) is a simple Metaheuristic that combines constructive heuristics and local search,[3]. It's a multi-start iterative process, in which each iteration consists of two phases: *construction of a solution and local search. The construction phase builds a feasible solution, whose neighborhood is investigated by the local search until a local minimum is found. The best overall solution is kept as the result [4].*

Variable Neighborhood Search (VNS) based on dynamically changing neighborhood structures [3]. VNS explores increasingly distant neighborhoods of the current incumbent solution and jumps from this solution to a new one if and only if an improvement is attained [5].

In this paper the proposed method has been combined between hybrid metaheuristic algorithms (GRASP and VNS) and Elliptic Curve discrete logarithm to generate symmetric mask key with minimum as possible of correlation between ECC points. And then using ECC algebra to implement the encryption and decryption process. We descript the complete approach stages in subsequence sections.

THE PROPOSED APPROACH

This section illustrate the proposed approach and descript each stage with details. Figure (1) show the general structure of this approach.

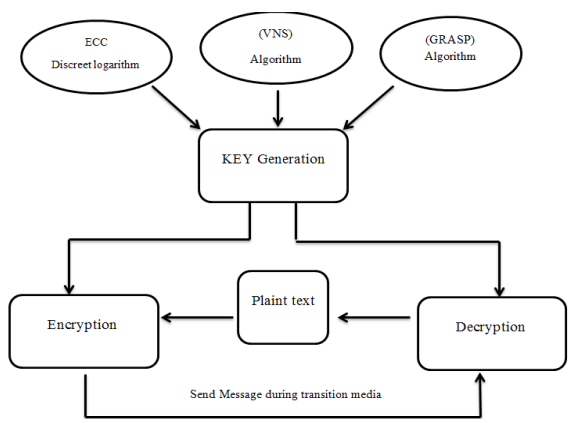


Figure1: general structure of the proposed approach

Preprocessing the plain text(secret massage) stage

There are many methods for coding or translate the characters for secret massage to binary code such as Unicode and ASCII code. In this work ASCII code is selected because it's more suitable when matching with ECC points and flexible with ECC algebra computations.

Generate symmetric key cryptography (Mask Key) stage

The key generation stages consist of two parts. First, is represented by generating all possible ECC points and second is represented by metaheuristic algorithms in order to obtain a robust symmetric cryptograph key. In the following illustrated the process with details:-

PHASE ONE :: ECC Processing Steps

Step1: Generate ECC points (Q) according the following equation

$$y^2 = x^3 + ax + b \quad \text{.....(1)}$$

Step 2: Select base point (secret point) P from ECC points (Q)

Step 3: While (Mask Key length is not met)

Step 4: Remove P from Q

Step 5: Compute Discrete Logarithm (k) between base point P and ECC points Q

Step 6: Q_Q= Eliminate all Q points that have k =0

Note1:: ECC Discreet Logarithm (k) is calculated by this equation

kP = Q .....(2)

Where: P is the base point and k is discreet logarithm of Q point.

Note2:: k=0, only if the base point does not have discrete logarithm with ECC point Q

PHASE TWO: Apply Metaheuristic algorithms GRASP + (VNS)
Basic GRASP Algorithm (Construction Phase)

Step 7 : Build Candidate list

C = Q_Q ..... (3)

Step 8 : Apply the following equation for getting feasible solution

$\mu = MAX_{cost}(C) - \alpha\ (\ MAX_{cost}(C) - MIN_{cost}(C)\ )$ **....(4)**

Step 9 : Constuct RCL according to this range

[*μ , MAXcost(C)]*

Step 10: Insert RCL into RCL_Database (RCL_DB)

Step 11: Select New point randomly from RCL

Step 12: Evaluate new point for objective function as following:

If (New point ∈ RCL_DB) **Then**

Base point = New point

Mask key= Mask key+New point

Else
(Return to Step 11)

Step 13: until (stopping condition)

Note3:: The eq-4- represent the modifying on original greedy function in GRASP to be more suitable for the proposed approach to find the maximum feasible solution instead of the minimum feasible solution as in original equation.

Note4:: All candidate elements C_i whose have incremental cost between MAX element and the threshold μ value are inserted into the RCL,(i.e. RCL have a feasible solution for each base point at each iteration and storing in the database to investigated from it in the next iterations).

Improvement Phase or Local using Variable Neighborhood Search (VNS) as in the following algorithm:

Step 12: Apply VNS algorithm:

Procedure VNS: Given $\{N_k, (k=1,\ldots,k_{max})\}$ and some x∈X

```
Begin
   Repeat
        K=1;
   Repeat
        Generate at random x' ∈ Nk(x);
      X''  ⟵  apply local search wit x' as starting point;

            If  (f(x'') < f(x)) then

                X  ⟵  x''
                K  ⟵  1;
          else
                K  ⟵  k+1
     Until k=kmax
 Until (some stop condition is satisfied);
 End
```

Initial solution S = {(3, 28), (0,250), (1,76), (4,123), (30,26)} with total cost =685

Note :: Set neighbor Structures N_k={k=1,……..,k3}. Mask key has been treated with only special type of neighborhood structures as in the following :

transpose neighborhood: in which two jobs occupying adjacent positions in the sequence are interchanged:

S=P1,P2,P3,P4,P5→N1(S)= P2,P1 ,P3,P4,P5

swap neighborhood: in which two arbitrary jobs are interchanged:

S=P1,P2,P3,P4,P5→N2(S)=P1,P5,P3,P4,P2

insert neighborhood: in which one job is removed from its current position and inserted elsewhere:

S=P1,P2,P3,P4,P5→N2(S)= P1,P3,P4,P2, P5

All above neighborhood structures are working on change the tracking of solution elements within the incumbent solution for fulfill mask key requirement.

According to these structures , there are several solutions are generating after applying local search on neighbor structures (S'') , Quality of these new solutions may consist of into four cases :

- Worst solution : Occur when the elements of new solution don't have connection with each other (i.e one or more points are out of the scope).
- Not good solution: Occur when new solution has fully connection among elements solution with total heuristic cost that less than in initial solution (i.e. F(S')<F(S)) .
- Good solution : Occur when new solution reaches to local minimum F(S')>F(S).
- Optimal solution : Occur when new solution reaches to local optima

Step 13: End.

Note 6:: Fitness (Objective function) in VNS is evaluated by that all elements within solution (points within Mask Key) must connect with each other in minimum correlation for getting to best solution with high randomness.

Encryption and Decryption processes Stage
Elliptic Curve addition algebra is used according to following equation:

R=P+Q .....(5)

Where:

P= plaint text point, Q = Mask Key, R=Cipher point.

And the decryption process is done by using the equation:
P=R-Q→P=R+ (-Q) …….. (6)

Implementation
The proposed approach has been implemented using Visual Prolog (v.5.1) Personal Edition. The following stages illustrate the main steps of the proposed approach:

Secret message is :" COMPUTER SCIENC" , Convert it to ASCII code:

{67,81,77,80,85,84,69,82,32,83,67,73, 69, 78,67}
And then treated these code as pair of number (point) {(67,81),(77,80),(85,84),(69,82),(32,83),(67,73),(69,78),(67,69)}

At 1st Iteration

Let solution = {(3,28),}

Step 3: While (length of Mask key < =4)

Step 4 : ECC points Q = (0,1) ,(0,250) ,(1,76), (1,175), (3,28), (3,223), (4,123), (4,128), (5,70), (5,181),(7,10),(7,241), (9,57), (9,194), (10,42), (10,209),(11,29),(11,222),(14,91),(14,160) ,(20,95),(20,156),(25,66),(25,185),(28,12),(28,239),(30,26) , (30,225), (31,74),(31,177), (35,50),….., (246,97), (246,154), (248,67), (248,184)

Step 5: Compute Discreet logarithm

When P(3,28),Q1=(248,67)
2P=P+P=(3,28)+(3,28)=(57,196)
214 P=(174,100) + (3,28)= (248,67)

Discrete logarithm k between (3,28) and (248,67) = 214

Table (1) illustrates some computation of discreet logarithm between base point and other ECC points :

Table(1) Compute the discrete logarithm k of all possible Q points to the base point P = (3,28)		
base point (P)	Discreet Logarithm (k) / Incremental cost	$ECC_{251}(1,1)$ (Q)
(3,28)	214	(248,67)
	198	(0,250)
	204	(1,67)
	182	(4,123)
	98	(4,128)
	102	(5,70)
	178	(5,181)
	193	(7,10)
	87 . .	(7,241) . .

Step 7: C= {(248, 67), 214 ,(0,250), 198 ,(1,67), 204 ,…… }

Step 8: Let α =0.7

$\mu = MAX_{cost}(C) - \alpha (Max_{cost}(C) - Min_{cost}(C))$
μ =279-0.7*(279-1)
μ =84
RCL range [279,84]

Step 9: RCL={(1,76),204,(4,123),182,(4,128),98, (0,250),198,..., (11,29),241,(14,160),216,(20,95),132, (20,156),148,……}

Step 10: Insert RCL into RCL database as in the following table (2) :

Step 11: Let new point = (0,250)

Step 12: Evaluate this point by fitness

(0,250) ∈ RCL database // (True)

Table 2: RCL Database	
1st iteration	RCL={(1,76),204,(4,123),182,(4,128),98 , (0,250),198, (11,29),241 ,(14,160), 216, (20,95),132, (20,156), 148}

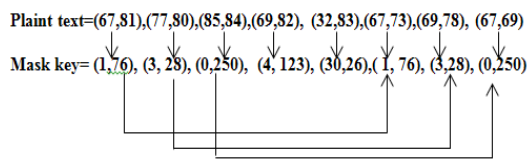
Step 13: Mask key (solution)= { (3,28),(0,250), } After repeated construction phase for four iteration, mask key will be:

{(3,28),(0,250),(1,76),(4,123),(30,26),(60,47)}

Step 14: After apply Local search on mask key using (VNS) Best solution=

{(1,76),(3, 28),(0,250),(4,123),(30,26)}

Encryption/Decryption processes
Encryption process:



Mask is replication according to plaint text length

Example:- Let P= point in plaint text such as (67,81) and Q= point in key mask such as (1,76)

R=P+Q→R= (67,81)+ (1,76)

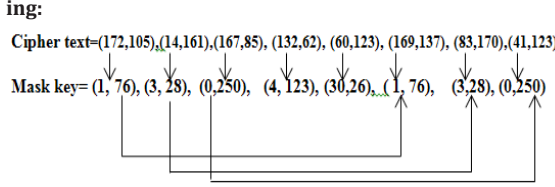
λ = (yQ - yP) / (xQ - xP) mod 251→λ =156

$X_R = (\lambda^2 - x_P - x_Q) \bmod 251 = 172$

$Y_R = (\lambda (xP - xR) - yP) \bmod 251 = 105$ R→(172,105)

Cipher text = { (172,105), (14,161),(167,85), (132,62), (60,123) ,(169,137),(83,170),(41,123)}

Decryption process performs the reverse process as following:



Mask is replication according to plaint text length

P=R-Q→P=R+ (-Q)

P= (172,105)+(1, -76)

.

.

P= (67,81)

Plaint text = (67,81),(77,80), (85,84),(69,82),(32,83),(67,73),(69,78),(67,69)

RESULT AND DISCUSSION
The proposed cryptographic was generated new method for generation mask key for ECC with symmetric behavior using hybrid of metaheuristic algorithms and ECC .

Table(3) illustrates that how the length of mask key was effected by t (α) value that was explained in eq (4).

Table(3) Effect of α on mask key ,When a=1, b=1, p=251,point=(3,28)			
(α)	RCL size	RCL range[MAX,μ]	Maximum length of mask key
0.0	1 point	[279]	1
0.1	28 points	[279-252]	3
0.3	84 points	[279-196]	4
0.5	140 points	[279-190]	5
0.7	195 points	[279-85]	8
1.0	279 points	[279-1]	26

When (α) is increased then RCL size, RCL range and mask key length is also increased to some extent according to prime number value (i.e. prime number determines the state space of solution table (4) is illustrated this case).

Table(4) Generate the state space of prime number	
Prime number	State space
251	281 points
457	441 points
593	578 points
929	909 points

Length of mask key also is depended on the random selection of point from RCL because each point has different number of points that connected with it) for example When a=1,b=1,p=457 and secret point =(0,1) There are two masks may be generating according to select random point from RCL

First mask : {(0,1) , (8,8), (12,85) ,(12,85) , (15,211) ,(19,107), (20,131) , (48,31), (54,35)}

Second mask : {(0,1) , (8,8), (12,85) , (12,85) , (15,211) , (19,107), (20,131),(48,31), (66,32), (179,13) , (64,207), (243,149) , (255,79), (322,117)}

Local search phase was effected on some solutions when compared them with initial solution such as in table (5-a), (5-b).

Table (5-a) Initial solution with cases					
Initial solution (S)	Fitness	Worst	Not good	Good	Optimal
{(3, 28), (0,250), (1,76),(4,123), (30,26)}	685			Yes	

Table (5-b) Improvement solution with cases					
New solution (S'')	Fitness	Worst Sol	Not good Sol	Good Sol	Optimal Sol
{(0,250),(3, 28), (1,76), (4,123), (30,26)}	755			Yes	
{(1,76),(3, 28),(0,250),(4,123),(30,26)}	805			Yes	yes
{(3,28),(1,76),(0,250),(4,123),(30,26)}	None	Yes			
{(4,123),(1,76),(3,28),(0,250),(30,26)}	None	yes			
{(3,28),(1,76),(0,250),(4,123),(30,26)}	607		yes		
{(0,250),(1,76),(3,28),(4,123),(30,26)}	697			Yes	
{(30,26),(1,76),(3,28),(0,250),(4,123)}	None	yes			
{(1,76),(0,250),(3,28),(4,123),(30,26)}	577		yes		
{(4,123),(0,250),(3,28),(1,76),(30,26)}	None	yes			

But in another hand, local search doesn't improve the solution such as in tables (6-a),(6-b).

Table (6-a) Initial solution with cases					
Initial solution (S)	Fitness	Worst	Not good	Good	Optimal
{(1,76),(0,1),(7,10),(11,29),(28,239)}	611			yes	

Table (6-b) Improvement solution with cases					
New solution (S'')	Fitness	Worst Sol	Not good Sol	Good Sol	Optimal Sol
{{(0,1),(1,76),(7,10),(11,29),(28,239)}	423		yes		
{(1,76),(0,1),(7,11),(10,29),(28,239)}	None	yes			
{(28,239),(7,10),(1,76),(0,1),(11,29)}	None				
{(11,29),(7,10),(1,76),(0,1),(28,239)}	None				

Conclusion

- **Using mask key length that depend on** *α value help to produce more flexible mask key (i.e. RCL length is variable according to α), when α is increased from [0 to 1] the RCL length is increased ,so the probability of mask key length is also increased .*
- Local search phase have a great effect on some solutions but in another cases it have low or not effect to solution (i.e. constructed solution remain as the same).
- The proposed approach produce robust secure randomness key based on some robust factor as following:

- ECC factors:(Prime number, a , b values)
- **GRASP metaheuristic factors :**(selection of α value [0,1] , random selection of base point form RCL)
- **VNS local search factor: (Random selection in the** *k-th neighborhood in shaking phase)*

Volume : 2 | Issue : 10 | October 2013 • ISSN No 2277 - 8179

REFERENCE

Erik De Win, Bart Preneel , "Elliptic curve public-key cryptosystems – an introduction. State of the Art in Applied Cryptography", LNCS 1528, pp: 131-1411, 1998. | [2] Sigurdur Olafsson ,"Metaheuristics in Nelson and Henderson (eds.)Handbook on Simulation" , Handbooks in Operations Research and Management Science ",VII Elsevier, 2006. | [3] Joao Paulo Queiroz dos Santos, Francisco Chagas de Lima Junior, Rafael Marrocos Magalhaes,"A Parallel Hybrid Implementation Using Genetic Algorithm, GRASP and Reinforcement Learning" ,pp: 2-3, 2009. | [4] Francisco Chagas de Lima J´unior, Jorge D. de Melo, Adrı˜ao Duarte D. Neto, "Proposal for Improvement of GRASP Metaheuristic and Genetic Algorithm Using the Q-Learning Algorithm",2007. | [5] Leonardo Gomes, Viviane Diniz Carlos Martinhon , "An Hybrid GRASP+VNS Metaheuristic for the Prize-Collecting Traveling Salesman Problem",pp: 2,3, 2009. |