Proposed Approach for Key Generation Based on Elliptic Curve (EC) Algebra and Metaheuristic Algorithms

Dr. Hala Bahjat Abdul Wahab
Computer Science Depart, University of Technology/ Baghdad
Email:hala_bahjat@yahoo.comsuhad_mallala@yahoo.com
Dr.Suhad Malallah Kadhem
Computer Science Depart, University of Technology/ Baghdad
Estabraq Abdul Redaa Kadhim
Computer Science Depart, University of Technology/ Baghdad

Received on: 12/6/2013 & Accepted on: 26/11/2013

ABSTRACT

The key management is an important area of research in internet applications, because protecting secret messages during transmission becomes an essential issue for the Internet. 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 produces a new cryptographic key generation approach that investigate from metaheuristic algorithms (Greedy Randomized Adaptive Search Procedure (GRASP) and Variable Neighborhood Search(VNS)) in order generate symmetric mask key that consist of more the one EC points with minimum correlation among points. The proposed approach aims to combine between the features of elliptic curve arithmetic, Discrete Logarithm and metaheuristic algorithms (GRASP and VNS) to produce robust symmetric cryptography key (mask key). The proposed approach tested and gives efficient results when compared with other previous approach in term of secrecy and privacy .

Key words: Elliptic Curve, Key Exchange, Cryptography Protocols, Met heuristic Algorithms**.**

اقتراح طريقة لتوليد المفاتيح بالاعتماد على رياضيات المنحني الاهليجي والخوارزميات الفوق توجيهة

الخلاصة

تعتبر ادارة المفاتيح من اهم المجالات البحثية الموجودة على تطبيقات الانترنت وذلك لأنه حماية الرسائل السرية خلال ارسالها اصبحت مسألة اساسية في الانترنت . التشفير باستخدام المنحني الاهليجي قد لفت الانظار بالنسبة للباحيثين ومطوري المنتجات نظرا لقوة الهيكلية الرياضية والامنية العالية الخاصة به عندما يتم مقارنته مع بقية الطرق الموجودة. هذا البحث يقدم طريقة جديدة لتوليد مفتاح وذلك من خلال الاستفادة من خوارزميات الفوق توجيهية الذكية وهي GRASP و VNS من اجل توليد مفتاح تشفير

متماثل يتألف من مجموعة من نقاط المنحني الاهليجي ذات ترابط قليل بين نقاط المنحني الاهليجي . الطريقة المقترحة تهدف الى الدمج بين رياضيات واللوغارتمات المنفصلة للمنحني الاهليجي مع الخوارزميات الفوق توجيهية الذكية من اجل الحصول على مفتاح تشفير متماثل قوي وامن . الطريقة المقترحة تم اختبارها اعتمادا على الفحوصات الشائعهوقد أعطت نتائج كفؤه ومشجعة وذلك عندما تمت مقارنتها مع اعمال السابقة من ناحية الامنية والسرية .

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 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 ellipticcurve group [1]. Metaheuristics are designed and play important role with complex optimization problems .The practical advantage of metaheuristics lies in both their effectiveness and general applicability. 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 metaheuristicapproachaimto 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]. Previous work based on EC algebra and they select random mask or random point directly from EC point space and used for encryption decryption purpose. This paper will be produced a novel approach that aim to combine between the robust features from Elliptic Curve arithmetic, Discrete Logarithm problem and Metaheuristic algorithms (GRASP and VNS) to produce robust symmetric key (mask key) that have minimum correlation among EC mask points. The proposed approach tested and gives efficient results when compared with other previous approach in term of secrecy and privacy.

RELATED WORK

HalaBahjet Abdul Wahab›Rafal Ali Sameer, " Partial Cryptography in Digital Media Environment based on ECC Algebra ",2013, [3].

Hala and Rafal proposea new approach for encrypting digital image using the arithmetic of elliptic curve algebra. That proposed approach produces a new mask for encrypting the digital image by using a new convolution process basedon ECC algebra operations and work as symmetric cryptographic system.

ELLIPTIC CURVE CRYPTOGRAPHY (ECC)[4]

Comprised; computational brute-force has broken the keys. The defense is "simple" keeps the size of the integer to be In general, public-key cryptography systems use hard-to-solve problems as the basis of the algorithm. The most predominant algorithm today for public-key cryptography is RSA, based on the prime factors of very large

integers. While RSA can be successfully attacked, the mathematics of the algorithm has not been factored ahead of the computational curve!

In 1985, Elliptic Curve Cryptography (ECC) was proposed independently by cryptographers Victor Miller (IBM) and Neal Koblitz (University of Washington). ECC is based on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). Like the prime factorization problem, ECDLP is another "hard" problem that is deceptively simple to state: Given two points, P and Q, on an elliptic curve, find the integer *n*, if it exists, such that P = nQ.

Elliptic curves combine number theory and algebraic geometry. These curves can be defined over any field of numbers (i.e., real, integer, complex) although we generally see them used over finite fields for applications in cryptography. An elliptic curve consists of the set of real numbers (x,y) that satisfies the equation:

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

The set of all of the solutions to the equation forms the elliptic curve. Changing *a* and *b* changes the shape of the curve, and small changes in these parameters can result in major changes in the set of (x,y) solutions.Refered as $E_p(a,b)$.Figure (1) shows the addition of two points on an elliptic curve. Elliptic curves have the interesting property that adding two points on the elliptic curve yields a third point on the curve. Therefore, adding two points, P and Q, gets us to point R, also on the curve. Small changes in P or Q can cause a large change in the position of R.So let's go back to the original problem statement from above. The point Q is calculated as a multiple of the starting point, P, *or,* Q = nP. An attacker might know P and Q but finding the integer, *n*, is a difficult problem tosolve. Q (i.e., nP) is the public key and *n* is the private key.

ELLIPTIC CURVES OVER Z_P [4]

Elliptic curve cryptography makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field. Two families of elliptic curves are used in cryptographic applications: prime curves over Z_p and binary curves over $GF(2^m)$. For a prime curve over Z_p, we use a cubic equation in which the variables and coefficients all take on values in the set of integers from 0 through p -1 and in which calculations are performed modulo p. For a binary curve defined over $GF(2^m)$, the variables and coefficients all take on values in $GF(2^n)$ and in calculations are performed over $GF(2^n)$. Points out that prime curves are best for software applications, because the extended bit-fiddling operations needed by binary curves are not required; and that binary curves are best for hardware applications, where it takes remarkably few logic gates to create a powerful, fast cryptosystem.

GREEDY RANDOMIZED ADAPTIVE SEARCH PROCEDURE (GRASP) ALGORITHM

A metaheuristic is formally defined as an iterative generation process which guides a subordinate heuristic by combining intelligently different concepts for exploring and exploiting the search space, learning strategies are used to structure information in

order to find efficiently near-optimal solution [5].Greedy Randomized Adaptive Search Procedure is a simple metaheuristic that combines constructive heuristics and local search,[6]. 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 [7].

CONSTRUCTION PHASE [8]

Construction phase start from an empty solution, a complete solution is iteratively constructed by one element at a time. At each construction iteration, the choice of the next element to be added is determined by ordering all candidate elements in a candidate list *C* with respect to a greedy function $g: C \rightarrow R$. This function measures the benefit of selecting each element. The heuristic is adaptive because the benefits associated with every element are updated at each iteration of the construction phase to reflect the changes brought on by the selection of the previous element. The probabilistic component of a GRASP is characterized by randomly choosing one of the best candidates in the list, but not necessarily the top candidate. The list of best candidates is called the restricted candidate list (RCL).There are two main mechanisms to build this list: a cardinality-based (CB) and a value-based (VB) mechanism. In the CB case, the RCL is made up of the k elements with the best incremental costs, where *k* is a parameter. In the VB case, the RCL is associated with a parameter $\alpha \in [0, 1]$ and a threshold value according the following equation:

$$\mu = gmin + \alpha(gmax - gmin) \quad \ldots(2)$$

In fact all candidate elements *i* whose incremental cost *g(i)* is no greater than the threshold value are inserted into the RCL, i.e. $g(i) \in [gmin, \mu]$. Note that, the case $\alpha = 0$ corresponds to a pure greedy algorithm, while $\alpha = 1$ is equivalent to a random construction. With maximization problem, the purely greedy construction corresponds to $\alpha = 1$, whereas the random construction occurs with $\alpha = 0$. Note that, when the value of α increases from 0 to 1, the mean solution value increases towards the purely greedy solution value, while the variance approaches zero

IMPROVEMENT PHASE

The improvement phase consists typically of a local search procedure aimed at enhancing the solution obtained in the construction phase, given that the construction phase solution may not represent an overall optimum. In GRASP metaheuristic it is always beneficial to use a local search to improve the solutions obtained in the constructive phase [5] .The efficiency of the local search procedure basically depends of the suitable choice of a neighborhood structure and the starting point generated at the construction phase.[9]

The neighborhood structure N for a given problem relates a solution *s* of the problemto a subset of solutions *N(s).* A solution *s* is said to be locally optimal if in N(s) there is no better solution in terms of objective function value [8]

VARIABLE NEIGHBORHOOD SEARCH (VNS) ALGORITHM

Variable Neighborhood Search (VNS) is a metaheuristic, which explicitly applies a strategy based on dynamically changing neighborhood structures .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. To rapidly expose the main steps of VNS, consider a finite set of pre-selected neighborhood structures with N_k, (k=1,.., kmax), and with N x k ( ) the set of solutions in the k thneighborhood of (x)[5]:

The stopping condition used, the maximum number of iterations, maximum CPU time allowed and maximum number of iterations between two improvements [9].VNS' main cycle is composed of three phases: shaking, local search and move. In the shaking phase a solution **X'** in the k-th neighborhood of the current solution**X**' is randomly selected. Then, **X'** becomes the local search starting point. The local search can use any neighborhood structure and is not restricted to the set of neighborhood structures N_k, k =1,…..,k_{max}. At the end of the local search process (terminated as soon as a predefined termination condition is verified) the new solution X'' is compared with s and, if it is better, it replaces s and the algorithm starts again with k =1. Otherwise, k is incremented and a new shaking phase starts using a different neighborhood [5].

THE PROPOSED APPROACH

This section will explain the proposed approach and describe each stage with details .Mask key generation

Consists of two phases. First one EC algebra and discreet logarithm problem and second is metaheuristic algorithms. Figure (2) illustrates the main stages of mask key generation with the secure information that related with each stage.

(i) First Phase: EC algebra and discreet logarithm problem

This phase is providing a suitable key space based on the feature from discreet logarithm problem as follows:

- **Generate Elliptic Curve:**

This process needs agreement on prime number p and a, b values as in following Equations.

$$(4a^3 + 27b^2) \bmod p \neq 0 \quad \dots (3)$$

$$y^2 = (x^3 + ax + b) \bmod p \quad \dots (4)$$

Note: Choosing another a and b will changethe shape of the curve, this feature increases the flexibility of the mask.

- **Select Secret Point (Base point (P)) from EC points:**

One of EC point is selected and considered as Base point. Base point is a root which through the mask key will be constructed and there must be agreement on it.

- **Discreet Logarithm (k):**

Discreet logarithm (k) represents the distance between one point and another that is explained in section (2.4.3). Providing suitable Key Space mainly depends on discreet logarithm (k) feature on ECC.

Note: Discreet logarithm (k) values can consist of two sets. First, when k>0, that means there is a correlation between base point (P) and particular EC point (Q). Second when k=0, that means there is no correlation between P and Q (i.e. number of addition times of (P) reaches infinity (O) before reaching Q point).

In this work, key space will consist of EC points (Q_n) that have discreet logarithm k > 0. Figure (3) will illustrate the process of how key space is generated and Algorithm (1) will illustrate the main steps of key space generation process using EC Arithmetic and Discreet Logarithm.

Algorithm (1): Generate Key Space
Input: Prime number (p), (a) value, (b) value .
Output: Key Space.
Process:
Begin
Step1: Generate EC points (Q_n) according the following equations:

$$(4a^3 + 27b^2) \bmod p \neq 0 \quad \text{... (3)}$$

$$y^2=(x^3 + ax + b) \bmod p \quad \text{... (4)}$$

Step 2: Select Base point (secret point) P from EC points (Q_n)
Step 3: While (Mask key length is not met)
Step 4: Remove P from Q_n
Step 5: Compute Discrete Logarithm (k) between base point P and EC points (Q_n)
Step 6: Key Space=Q_n with k>0
Step7: End.

(ii)Second Phase: Metaheuristic Algorithms

This phase will produce new method to construct a robust and efficient mask key that consists of EC points and then is improved using metaheuristic algorithms (Greedy Randomized Adaptive Search Procedure (GRASP) and Variable Neighborhood Search (VNS)).

(a) Basic GRASP (Construction phase)

Mask key will construct based on greedy function for maximize problem. GRASP algorithm is utilized because the building of solution starts from an empty solution and complete solution is iteratively constructed in the next iterations .This feature gives several benefits in terms of accuracy and time as well as the constructed solution is always a good solution. The mask key consists of a set of EC points. These points must have as minimum of correlation among them as possible. This leads to dependence on two conditions that must be considered when mask key is constructed.

1. First, each point must have fully correlation with other mask key points.
2. Second, the total of incremental costs (k_n) among Mask key points are to be large as possible to guarantee the minimum correlation.

According to the above conditions some modifications may be intervene on Basic GRASP algorithm to be more suitable for this proposed requirement such as building database (RCL-database) for storing the feasible solution that is generated at each iteration and investigated from it in the next iteration to verify the first condition. Number of GRASP iteration represents the length of mask key. The following steps will illustrate the main steps of basic GRASP construction:

- **Build Candidate List** :

Key Space will be considered as a Candidate List (*C*) in GRASP construction phase with respect to their incremental costs (Discreet Logarithm (k) that will be considered as incremental cost) given by evaluating a greedy function $g : C \rightarrow R$.

- **Construct Feasible Solution (RCL):**

Construct Feasible Solution (RCL) will be applied by using value-based (VB) mechanism by applying greedy function for maximum problem on candidate list (*C*) and then getting range from max incremental cost to threshold (μ) as in the following equation :

$$\mu = \mathbf{Min}_{cost}(C) + \alpha(\mathbf{Max}_{cost}(C) - \mathbf{Min}_{cost}(C)) \quad \ldots(2)$$

where

$MAX_{cost}(C)$: maximum point in *C* with incremental cost respect

$MIN_{cost}(C)$: minimum point in *C* with incremental cost respect

μ: responsible for determining less maximum value in equation (2) .

α: purely greedy construction corresponding to α = 1, whereas the random construction occurs with α = 0.

Note: When value of (α) increases from 0 to 1, this means solution value increases towards the purely greedy solution value

- **Select One Point Randomly From RCL**

The technique of Random selection from RCL must agree with two parties such as (select 5th element from RCL) If selected point is unrealized to the conditions then another point will be selected randomly from RCL. The selected point will be new base point for the next iteration. Algorithm (2) illustrates the main steps of mask key construction.

Algorithm (2): Construction of mask key

Input: Key Space (α) value, No. GRASP iterations (Mask key length)

Output: Mask key.

Process:

Begin

Step 1: Build Candidate list: (**C** = Key Space)

Step 2: Apply the following equation to getting feasible solution

$$\mu = MIN_{cost}(C) + \alpha(MAX_{cost}(C) - MIN_{cost}(C)) \quad \ldots.(2)$$

Step 3: Construct RCL according to this range $[MAX_{cost}(C), \mu]$

Step 4: Insert RCL into RCL-database

Step 5: Select new point randomly from RCL

Step 6: Evaluate new point as following:
If (New point ∈ RCL_database) **Then**
Base point = New point
Mask key= Mask key+ New point
Else
Return to step 5
Step 7: Return to Step 3 in Algorithm (1))
Step 8 : End While (in Algorithm 1)
Step8: End.

(b) Basic GRASP /Improvement Phase (using VNS)

VNS metaheuristic search will be used in this work as local search phase. because it is based on dynamically changing neighborhood structures and 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 .This feature gives more flexibility and diversity when improving the solution, Whenever the number of neighborhood structures is increased then probability of getting best solution is also increased. In local search phase, solution will be improved by getting the highest total of incremental cost for entire solution without manipulation in correlation condition. Algorithm (3) illustrates the applying of VNS algorithm on the mask key.

Algorithm (3): Improving mask key
Input: Mask key (x), No. neighborhood structure N_k(k=1,…..k_{max}), No. iterations,
Output: Improved/Non improved Mask key.
Process:
Begin
Step 1: Repeat
Step 2: K=1
Step 3: Repeat
Step 4: Generate at random x' ∈N_k(X);
Step 5: X'' ß apply local search with x' as starting point;
If (f(X'') <f(X)) **Then**
X ß X''
K ß 1
Else
K ß k+1
Step 6: Until k=k_{max}
Step 7: Until (some stop condition is satisfied);
Step 8: End

Experimental Results

This section illustrates the results that obtained according the implementation the proposed approach which that explained in the previous sections

1. Key space**:** This section discusses the results of EC arithmetic and discreet logarithm (k) on generated key space and the effect of metaheuristic on constructed and improvement of the mask key. Figure (3) illustrates the size of key space

when discreet logarithm (k) is greater than zero and Figure (4) illustrates size of key space when discreet logarithm (k) is equal to zero. In the two Figures, row represents difference prime numbers and column represents size average of points according to (k) value.

Figures (3) and (4) clarify that key space with k>0 is provided with larger search space than k=0 and there is difficulty of expecting attackers. For this reason, the proposed approach relied on key space with k>0 as space for generation of cryptographic mask key.

2. Table (1) illustrates the result of effect of (α) value on determining the size of feasible solution (RCL) and mask key length.
   From Table (1), there are several results which can be extracted in the following way:
   i. Decrees in (α) value increases feasible solution (RCL) size by getting more points with low k; this leads to increase the maximum length of cryptographic mask key.
   ii. When prime number is increased, mask key length also increases with regard to (α) value.
   iii. It's not suitable to select (α) value that is close to one, because this makes key become easy to break.
   iv. Prime number (p) has a big effect on length of mask key
   v. Mask key length also depends on the random selection from RCL. Sometimes, the random point may not have enoughkey space, this leads to restrict the flexibility of the length of mask key.
3. Table (2) illustrates the results of effect of local search algorithm (VNS) on improving the initial solution. When initial (constructed) solution ={(3,28),(0,250),(1,76),(4,123),(30,26)} and fitness = 685 ,it is classified as good solution .New solutions have been improved three times.
   Table (3) illustrates the results of effect of local search algorithm (VNS) on improving the initial solution.When initial (constructed) solution {(1,76),(0,1),(7,10),(11,29),(28,239)}and fitness = 611 ,it is classified as good solution , new solutions never improve , and initial (constructed) solution has been considered as an optimal solution.
   From these tables, some results have been observed as in following:

(i) Tables(2) and (3) show four vocabularies that describe the case of each new solution based on initial (constructed) solution :

- **Worst solution:** is a solution that doesn't have correlations with each other (i.e. one point has k=0), so fitness isn't calculated for it.
- **Not good solution:** is a solution that has full correlation with each other, but fitness is less than in initial solution.
- **Good solution:** is a solution that has full correlations with each other and fitness is equal or greater than in initial solution
- **Optimal solution:** is a solution that has full correlations with each other and highest fitness from new solutions (one of good solution).

(ii) Local search has great effects on some solutions through reaching an excellent improvement ,but in other cases such as that in Table (3) , local search does not improve the solution. This means that solution reaches local optimum in construction phase of GRASP algorithm.

(iii) Increased number of neighborhood structures and number of iterations according to length of solution may give chance to getting local optimum. for example when initial (constructed) solution {(513),(959,0),(1,4),(821),(9,204), (59,516),(86,516), (116,254), (155,460), (269,867),(742,865),(767,963)}and fitness =1314 ,it's classify as good solution After four iterations later .

(iv) Solutionwillbe{(59,516),(513,959),(0,1),(4,821),(9,204),(86,516),(116,254),(155,460),(269,867),(742,865),(767,963) and fitness =1370, but after 80 iterations later solutionis improving to reach optimal {(513,959) ,(155,460) ,(9,204), (269,867), (0,1) ,(742,865),(59,516),(4,821),(86,516),(116,254),(767,963)} and fitness =1555 .

CONCLUSIONS

This paper described a novel approach of key generation using ECarithmetic and metaheuristic algorithms .It was succeed to construct robust and secure mask key using intelligent way from EC points when compared with the previous approaches that depend on three secure constant when generation key (Prime (p) a, b, values) but this proposed approach have more secure constant that make mask key more robust and secure as following:

- ECC factors **:** Prime number and a , b values
- GRASP metaheuristic factors**:** selection of α value [0,1], random selection of Base point form RCL with more robust according the results.
- VNS local search factor**:** Random selection in the *k*-th neighborhood in *shaking phase* The proposed approach succeed to produce an efficient mask key consist of multiple EC points with minimum correlation according the experimental results and tests.

REFRENCES

[1]. DeWinand B. Preneel,"Elliptic curve public-key cryptosystems – anintroduction. State of theArt in Applied Cryptography", LNCS 1528, pp: 131-1411, 1998.

[2].SigurdurOlafsson, "Metaheuristics," in Nelson and Henderson (eds.). Handbook on Simulation, "Handbooks in Operations Research and Management Science "VII, Elsevier", 2006.

[3].HalaBahjat,RafalAli ," Partial Cryptography in Digital Media Environment Based on ECC Algebra",2012.

[4]. Aydos, Savas and C.K. KoV, "Implementing network security protocols based on elliptic curve cryptography". Proc. fourth Symp. Computer Networks, pp: 130-139,1999.

[5].Christian Blum, Andrea Roli, "Metaheuristics in Combinatorial Optimization: Overview andConceptual Comparison", pp: 9,10,2003.

[6].Joao Paulo Queiroz dos Santos, Francisco Chagas de Lima Junior, Rafael MarrocosMagalhaes,"A Parallel Hybrid Implementation Using Genetic Algorithm, GRASP and Reinforcement Learning" ,pp: 2-3, 2009.

[7].Francisco Chagas de Lima J´unior, Jorge D. de Melo, Adri˜ao Duarte D. Neto,"Proposal for Improvement of GRASP Metaheuristic and Genetic Algorithm Using the Q-Learning Algorithm",2007.

[8]. FestaResende,"GRASP: basic components and enhancements", pp: 2-5, 2010.

[9]. Leonardo M. Gomes, Viviane B. Diniz, Carlos A. Martinhon, "An Hybrid GRASP+VNS Metaheuristic for the PrizeCollecting Traveling Salesman Problem",pp: 2,3,2009.

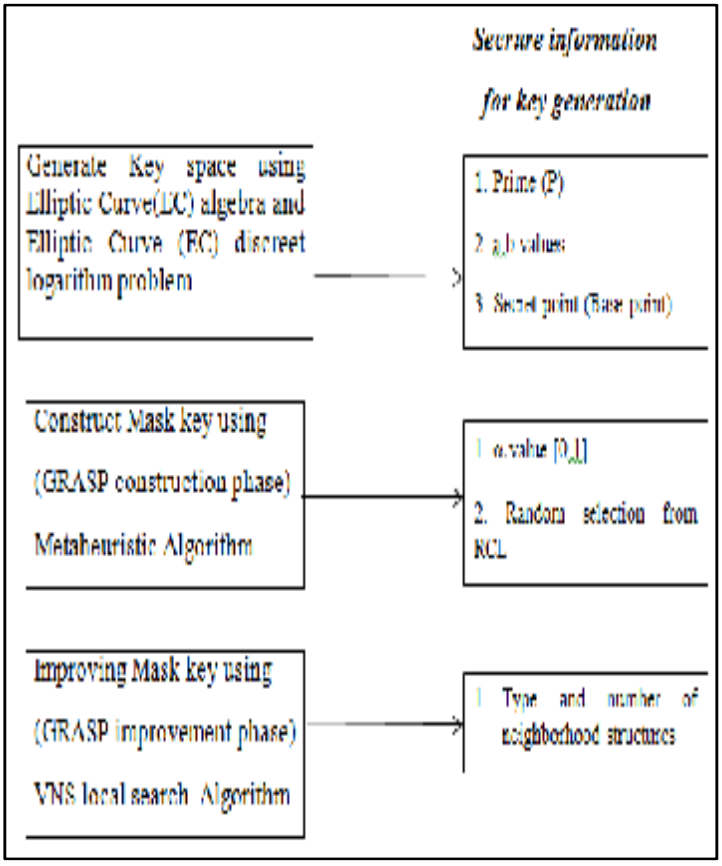

Figure (1) Elliptic curve Addition.

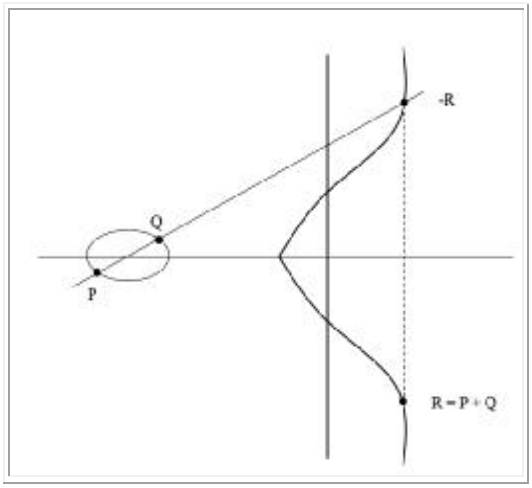

Figure (2) General Structure of key generation.

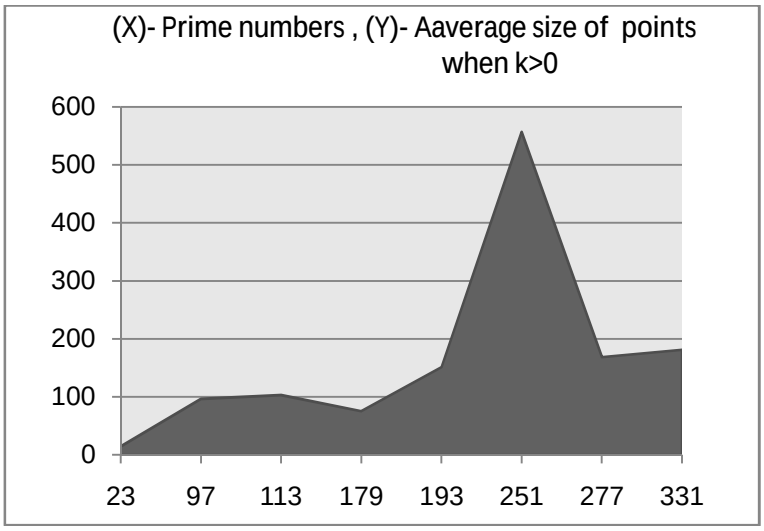

Figure (3) Key space for diffrents prime numbers when k>0.

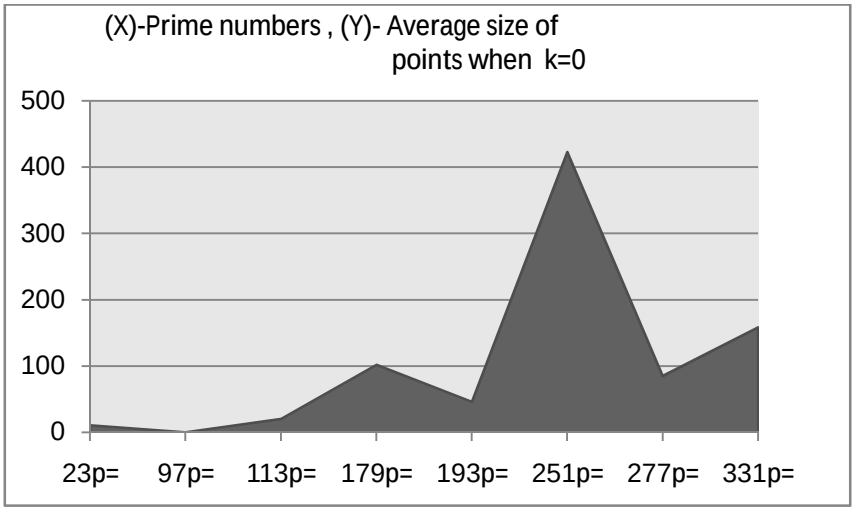

Figure (4) Key space for diffrents prime numbers when k=0.

Table (1) Effect of (α) value on Mask key length.

$ECC_p(a,b)$	Secret point	(α)	RCL size	RCL range [max ,μ]	Maximum length of mask key
$E_{251}(1,1)$	(220,53)	1.0	1 point	[138]	1
		0.7	14 points	[138-125]	2
		0.5	42 points	[138-97]	4
		0.3	70 points	[138-69]	7
		0.2	97 points	[138-42]	8
		0.0	138 points	[138-1]	26
	(110,178)	1.0	1 point	[44]	1
		0.7	5 points	[44-40]	2
		0.5	14 points	[44-31]	3
		0.3	23 points	[44-22]	5
		0.2	31 points	[44-14]	7
		0.0	44 points	[44-1]	22
$ECC_{997}(1,1)$	(996,836)	1.0	(1) point	[992]	1
		0.7	(298) points	[992-695]	4
		0.5	496 points	[992-497]	7
		0.3	694 points	[992-229]	10
		0.2	793 points	[992-200]	15
		0.0	992 points	[992-1]	92

Table (2) New solutions with their case.

New solution (S"	Fitness	Worst Solution	Not good Solution	Good Solution	Optimal Solution
{(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**			

Table (3) New solutions with their case.

New solution (S")	Fitness	Worst Solution	Not good Solution	Good Solution	Optimal Solution
{{(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				