Methods of cryptographically steady elliptic curves generation

L Cherckesova¹, O Safaryan¹, P Razumov¹, B Akishin¹, V Chumakov², I Smirnov³, and I Trubchik¹

¹Don State Technical University, Gagarin sq., 1, Rostov on Don, 344003, Russia
²Don state technical University Shakhty, Rostov region, 147 Shevchenko street, 346500, Russia
³Specialist Institute of artificial intelligence problems 118B Artyom street, Donetsk, 83048, Ukraine

E-mail: safari_2006@mail.ru

Abstract This article is devoted to a complex study of elliptic curves and description and characteristics of it are presented. Moreover, algorithms for generating cryptographically stable elliptic properties that ensure the greatest curves are revealed. The detailed description is given, and the resistance of the elliptic curves to the different types of cryptographic attacks are determined, grounding on the comparative analysis of information security system.

1. Introduction
Due to the ubiquitous distribution of information systems there is a question which sharply rises today of security of the stored and transmitted data. On the one hand, need of subjects of information systems for the reliable mechanism of authenticity of transmitted data is observed. On the other hand, modern cryptographic protocols, having the high level of cryptographic firmness, allow subjects of systems of data transmission to have absolute confidence in reliability of communication systems [1].

Thereof, various information systems using means of asymmetric cryptography which work is based on use of an open key of enciphering in recent years were widely used. According to scientific research of scientists, among the cryptosystems using an open key the cryptosystem based on the elliptic curves (EC) are the most resistant to different attacks.

Results of this work are based on researches of such scientists as Neil Koblits, Rene Chuf, Joseph Silverman, Artur Atkin, Scott Vanstoun, Alfred Menezes, and Tatsuaki Okamoto [1].

Some provisions, in relation to generation techniques cryptographic of resistant elliptic curves, have gained development during writing of the work.

Use of elliptic curves in cryptosystems was offered the American scientists Neil Koblits and Victor Miller in 1985 [2].

Need of development of methods of generation cryptographic strong curve taking place to application in real cryptosystems is the choice problem cryptographic strong curve for asymmetric cryptosystem which is caused by labor input of calculations and difficult realization of the existing algorithms [3].

2. Problem Formulation
During the research two, the most perspective approaches to realization of methods of generation cryptographic strong elliptic curve are revealed. The algorithms discussed in work are a technique of...
"the random choice" of an elliptic curve and the approach, which is based on application of a method of complex multiplication.

In general, use of these algorithms of generation promotes increase in cryptofirmness of the system.

The description of elliptic curves is provided in this work, their general characteristic is given and also generation algorithms cryptographic of resistant elliptic curves are considered. Their detailed description is provided.

The purpose of this work is the research of algorithms of generation cryptographic strong elliptic curves for definition of an optimum method of their application in the conditions of reflection of the attack of the malefactor to the confidential ciphered data transferred on a communication channel.

In the course of achievement of author’s purpose, the following tasks have formulated and successfully solved:

– Research of elliptic curves from positions of safety and effectiveness and performance.
– Identification of generation cryptographic resistant elliptic curves methods.

Analysis of existing approaches to generation of elliptic curve based on its random search as the mathematical objects using method of complex multiplication.

3. History of Investigations

The American scientists Neil Koblits and Victor Miller who in 1985, independently of each other, have offered the systems of cryptographic protection on the basis of an open key which use properties of the additive set (group) of points of the elliptic curve for enciphering realization became founders of cryptography on the basis of elliptic curves. Subsequently works of these researchers have formed the cryptography basis on elliptic curves [4].

The German scientist Gerald Bayer and the Swiss researcher Johannes Bauchman were engaged in studying of a question of generation of crypto resistant elliptic curves. In the collaboration, "Methods of the generation of elliptic curves" published in August 27, 2002 in the report to information technology development agency of Japan.

In the work they have described approaches to creation elliptic curves relative to field (hereis some prime simple number) and over field, therefore they have given the comparison of studied methods [5].

In Russia, V.V. Pylin in the thesis "Algorithms and methods of generation of an elliptic curve for asymmetric cryptosystem" (2008) and Rastorguyeva N.V. in the thesis "Selection of parameters of elliptic curves and the analysis of their cryptofirmness for use in asymmetric cryptosystems" dealt with this problem (2014) [6].

4. Elliptic Curves Application in the Cryptography

Safety of cryptosystems based on elliptic curves is defined by quantity of points. Therefore, to decide whether the rational points group is applicable for using in cryptography, it is necessary to understand the order of studied group.

The first approach called random approach chooses a casual curve. The order of group is defined by using algorithms of calculation of points. Based on calculation of quantity of points we can define whether this group is applicable for using in cryptography, or is not. If result determines that received elliptic curve is not satisfying to cryptosystem security, then another elliptic curve is selected.

Another is CM–method, which uses complex multiplication theory, which was included in the name of eponymous method. The considered method has rather big difference from previous. In this method, first of all search of suitable points of group is executed. It can be realized without knowledge of the appropriate elliptic curves of the given input data. After the points group is detected, the elliptic curve is determined with the assistance of complex multiplication formulas [7].

5. Cryptographic Application of Elliptic Curves

Let is a prime number, where. Elliptic curve over the fieldis, where. Point on the curve E is solve of such that or a point on infinity, which acts as single element. Set of pointsover the fieldis denoted as [8].

Elliptic curve is cryptographic resistant if it satisfy security and efficiency conditions.
First of all, consider resistance of a curve from the point of view of safety. Safety of cryptosystem on elliptic curves is based on complexity of a solution of the problem of a discrete logarithm in. At the moment, several algorithms of the solution of discrete logarithms are known. To make their decision impossible, it is required that the elliptic curve $E$ meets the following conditions.

- prime, – integer.
- Prime numbers are not equal.
- The order in the multiplicative group from is not less than, and the value.

Condition №1 does impossible using of the common algorithms of discrete logarithm calculation. Condition №2 eliminates the abnormal attack. In addition, the last condition excludes attacks on the private keys, such as famous attack of Menezes, Okamoto, Vanstone, etc. \[9\].

Further, we will consider cryptographic resistance of cryptosystems on elliptic curves from the point of view of efficiency. We assume that elliptic curve set over the finite field meets safety conditions. The cryptographic system effectiveness depends on performance of arithmetic operations defined in the finite field. That is why must be small so as it affordable. It follows from the Hasse’s theorem:

$$\left(\sqrt{|E(F_p)| - 1}\right)^2 \leq p \leq \left(\sqrt{|E(F_p)| + 1}\right)^2$$

Therefore, the value $|E(F_p)|$ should also be small.

Take a look at first security condition:

$$|E(F_p^m)| = k \times r$$

where $r \geq 2^{160}$ is prime $k \geq 0$, –integer (cofactor).

The cryptosystem safety, in which value $|E(F_p)|$ is grounded on the complexity of problem of discrete logarithm solving, in subgroup with order, in group of points of elliptic curve $E(F_p)$. So, $k$ should be small. Next, we improve the first condition (2), where $r \geq 2^{160}$ is prime, is integer.

Third condition means that endomorphism of ring with name of elliptic curve over the algebraic closure is imaginary, quadratic order. In conclusion remind that elliptic curve cryptographic resistant if it satisfies the following conditions:

where is prime, is integer.

### 6. Generation Methods of Cryptographic Resistant Elliptic Curves

Continuing the research, consider two methods of finding cryptographic resistant elliptic curve. At first, the next task should be solved: even andare the positive integer numbers, where. It is necessary to find elliptic curves whose coefficient are such that. Therefore, integers and are the limits for and for determining the effectiveness and safety [10].

Before considering the algorithms, we describe check algorithm of simplified named. Input to algorithm are integers and, where, prime and integer. It outputs prime number, if the value is order of cryptographic enduring elliptic curve concerning field, where; else – is displayed 0. Consider this algorithm in more detail.

**Check algorithm of simple:**

1. //Checking whether N in interval Hasse
2. “if” then
3. return (0);
4. “;” //initiation of rank, which are equal 0
5. //Checking first condition
6. “for;” do
7. “if” and and then
8. “;” break;
9. if then
10. return (0);”
11. “/Checking second condition
12. “If then
13. return (0);”
14. “/Checking third condition
15. “;
16. for ; ; do
17. ;
18. if then
19. return (0);
20. return (r)” [11].

7. Algorithm based on Random Choice of Elliptic Curve
The first problem is to detect the prime number. To date, there are no well-known attacks to elliptic curves cryptosystems, that uses the properties of some field. Hence, the selection of prime number is not critical. Nevertheless, the boundary conditions and to be considered. The variable is bit length of

We propose to select such value of, at which

Method returns that prime number. User can select his own implementation of method, for example, such as use prime numbers in interval [12].

When is defined, the next acts is realized: we choose the parameters and, where, define group order of elliptic curve rational points concerning the field and, finally, we must determine whether this group is cryptographically strong, or not.

Above all, we clarify how to pick and up. As usual, the choice of parameters goes by random. The main idea is using one-sided property of cryptographic hash function. We denote it as, and is a bite length to output of. Assume. To generate a curve by random firstly it is needed to choose bit string of length not less then.

We write for the string (is makes a new sequence from bit string). As we know, the value of is used for calculating and by determined way. Thus, if we have got, hash–function, and determined algorithm of calculating from, every subject can check that and are calculated by using. One–side propertyguarantees that parameters are chosen by random way. Here we writefor any algorithm, which outputs elliptic curves are defined over random way.

If the curve is chosen, we should to define the group order of the curve. At this moment, the most known algorithm for the decision of this task is the algorithm. We denote is as [11].

Denote the result byIf then our task is solved. Otherwise, we need to recall and, until we got success.

Algorithm of random choice elliptic curve
1. “;”
2. while true do
3. “;”
4. “;
5. “;
6. if then
7. return” [11].

8. Method of Complex Multiplication
The central term in the framework of the method of complex multiplication is imaginary quadratic discriminant [7]. We designate such discriminant through. This is negative integer number: Through we denote the imaginary quadratic order of the discriminant:
Let us write for. If is prime number, then it is called the norm in; if there are integer numbers then:

\[ t^2 - Ay^2 = 4p. \]  

(4)

If is norm in, then two elliptic curves, designated as, concerning the field \( F_p \), with the ring of endomorphisms are built, according to the following scheme, using the complex multiplication:

\[ \left| E(F_p^m) \right| = p + 1 - t \quad \left| E(F_p^m) \right| = p + 1 + t \]

(5)

Though – is minimal polynomial with value. Here is modular function of elliptic curves.

Order is equal to. By the module, the polynomial is divided into the linear multipliers. Though, We will suppose that.

Therefore, we’ll receive:

Though, is quadratic nonstationary.

Together with the equation:

\[ (a_p b_p) = (3k_p, 2k_p) \]

(6)

where, we got expression:

\[ (E_{1,p} E_{2,p}) = ((a_p b_p) (a_p s^2 p b_p s^3 p)) \]

(7)

The elliptic curves, which were described above, are stranded (twisted) elliptic curves over the field[13]. In this expression, it is unknown in advance, which of these elliptic curves \((,)\) is cryptographically resistant (strong). Nevertheless, the selecting points on the every curve, as well as checking, is their order the divider of expression or expression, it is possible to identify the curves but also. We need to know representation of prime number, as in the formula (4).

Now the group orders as well as from the formula (5) understand for us. Using these orders, along with algorithm, by name, it is possible to verify and test the conditions of security. Usually most part of time, it is spent on computation of the polynomial by name. Cause is that the coefficients increases and are quite big, even if discriminant is of little importance [14].

Nevertheless, depending on value, it is possible to use the alternative polynomials, which coefficients are really very little in comparison with polynomial. Operating with mentioned polynomials significantly accelerates by the "complex multiplication" method in the practice. Bit complexity of the "complex multiplication" method has invariance.

9. Methods Comparative Analysis

This section compares the accidental random attitude (approach) and "complex multiplication" method to discover the cryptographically strong (resistant) group of elliptic curves over. We will compare influence on the safety and efficiency.

For a start, we will deal with safety. Primary benefit of accidental approach is that each cryptography strong group of elliptic curves over is calculated with approximately identical probability. The method of complex multiplication is applicable only on small discriminants, for example, discriminants with values no more than 1000 are used. Then the generated curves are special if their endomorphism ring values no more than 1000. Thus, not each cryptography strong group of elliptic curves can be brought by method of complex multiplication [15].

Now we will discuss efficiency. We will sort the case when, that is we look for group of elliptic curves of a simple order. We will write b for a bit length. Earlier we have mentioned that bit complexity of accidental attitude (approach) is depending just from the value. Nevertheless, bit complexity of complex multiplication depends on value of the used imaginary square discriminant.
We will consider for what value of both methods have the similar runtime, for one predefined fixed value \( b \). This number is called the intersection value and is designated.

For determination at first runtime of accidental approach was measured. We will mark that here the strategy of early interruption and use of the stranded curve which is described above is realized.

All tests were executed on different types of computer aids with using the free access software. Results of researches are given in the Table 1.

**Table 1.** The Average Time of Execution of Accidental Approach for Receiving of Cryptographically Resistant (Strong) Elliptic Curves Group of Simple Order.

| \( b \) | 160 | 170 | 180 | 190 | 200 | 210 |
| --- | --- | --- | --- | --- | --- | --- |
| Runtime (mins) | 3.63 | 4.87 | 7.97 | 10.3 | 13.1 | 16.7 |
| 50 | 820 | 960 | 1040 | 1090 | 1200 |

In the table means bit length100 computing experiments based on which average values were defined.

Based on the made experiments it was revealed that the method of complex multiplication would be practically more rapid algorithm if the condition is true in the case of discriminant, used in the complex multiplication method.

From Table I it can be concluded that the value of intersection is quite high.

Hence, if to consider the supplementary requirement of German Information Security Agency (GISA) that the value of the fundamental discriminant, appropriate to \( \Delta \), is at least 200, the complex multiplication method is more preferable than accidental choice method of elliptic curves on bit length of keys, which are used in the cryptosystems [16].

10. **Conclusion**

Application of elliptic curves is one of the most reliable and main technologies of creation of public keys in asymmetrical cryptography. The main criterion of firmness of such cryptography systems is the problem of complexity of the decision of the discrete logarithm.

For opposition to the available algorithms of the decision of this task of the characteristic of an elliptic curve shall meet some certain conditions. Respectively, the elliptic curves meeting such conditions are cryptography the strong.

The important task of elliptic cryptography is generation cryptography of the strong elliptic curves concerning the finite field of simple order. There are several methods of generation among which and reliable accidental approach to an elliptic curve generation and approach using complex multiplication method of are the most common and wide spread. After generation, the order of a curve is by methods of calculation of number of points and execution of the known conditions is checked. Unfortunately, the algorithms of calculation of elliptic curve number of points concerning the big fields are too slow.

If endomorphism ring of elliptic curve has small number of classes, then the method of complex multiplication is more preferable than a method of accidental generation.

Nevertheless, in the case of discriminant great values (\( D >200 \)) the existing methods of complex multiplication become impractical because of low speed.

Hence, the development of fast algorithms of elliptic curves generation by method of complex multiplication is most relevant.

**References**

[1] Cao X and Hu L 2011 *Finite Fields and Their Applications* 17 493-503  
http://dx.doi.org/10.1016/j.ffa.2011.02.012

[2] Fernando N, Hou X and Lappano S 2013 *Finite Fields and Their Applications* 18 492-521  
http://dx.doi.org/10.1016/j.ffa.2013.01.001

[3] Yuan P and Ding C 2011 *Finite Fields and Their Applications* 17 560-574  
http://dx.doi.org/10.1016/j.ffa.2011.04.001

[4] Silverman J H 2009 *The arithmetic of elliptic curves* 106 of *Graduate Texts in Mathematics*
Washington L C 2008 *Elliptic curves. Discrete Mathematics and its Applications (Boca Raton)* (Boca Raton, FL: Chapman & Hall/CRC)

Zha Z and Hu L 2012 *Finite Fields and Their Applications* 18 781-790 http://dx.doi.org/10.1016/j.ffa.2012.02.003

Maddah-Ali M, Motahari A, and Khandani A 2008 *IEEE Transactions on Information Theory* 54 3457-3470

Avestimehr S, Diggavi S, Tse D 2011 *IEEE Transactions on Information Theory* 57 1872-1905

Jafar S A and Vishwanath S 2010 *IEEE Transactions on Information Theory* 56 3297-3303

Nazer B, Jafar S, Gastpar M, and Vishwanath S 2013 *IEEE Transactions on Information Theory* 49 2188-2200

Hong S and Caire G 2013 *IEEE Transactions on Information Theory*

Nazer B and Gastpar M 2011 *IEEE Transactions on Information Theory* 57 6463-6486

Rohit Gupta, Sharma R K 2016 *Finite Fields Appl.* 41 89-96

Hou X 2014 *Acta Arith* 162 51-64