Розглядається задача факторизації, на якій базуються багато класичних асиметричних систем (RSA, Рабіна, інші) та криптографічно сильних генераторів псевдовипадкових послідовностей (BBS). Коротко описані методи, які послугували прообразами методу Лєнстра, та запропоновано метод факторизації чисел, який є аналогом методу Лєнстра на кривих Едвардса. Спочатку для обґрунтування коректності методу розроблено відповідний математичний апарат. Далі, з використанням цього апарату, побудовано аналог методу Лєнстра на кривих Едвардса та розроблено відповідний алгоритм факторизації чисел. Математично обґрунтовано коректність методу, коректність роботи алгоритму; отримано та строго доведено верхні аналітичні оцінки для його швидкодії та нижні оцінки імовірності успіху. Наведено та строго обґрунтовано переваги розробленого методу у порівнянні з класичним методом Лєнстра, який застосовує еліптичні криві у формі Вейєрштраса. Проведено порівняльний аналіз нового та класичного алгоритмів.

За результатами досліджень отримано строгі доведення того, що новий алгоритм на повних кривих Едвардса, у порівнянні з класичним, має переваги у швидкодії приблизно у 1.5 рази. Наведено експериментальні результати, які показують, що швидкодія зростає іще більше (до 30 відсотків), якщо замість повних кривих Едвардса використовувати скручені та квадратичні криві. Показано, що оцінка імовірності успіху нового методу зросте за рахунок появи нових умов, які приводять до успіху алгоритму та які не існують для класичного алгоритму Лєнстра на кривих Вейєрштраса.

Отримані результати дозволяють зменшити час, необхідний для розв'язку задачі факторизації, приблизно у 1.5 рази, а, отже, дають змогу швидше зламувати криптосистеми, що базуються на цій задачі

Ключові слова: криптосистема RSA, задача факторизації, методи факторизації, метод Лєнстра, криві Едвардса

UDC 519.7 + 681.3.06
DOI: 10.15587/1729-4061.2018.151090

SUBSTANTIATION OF CORRECTNESS AND ADVANTAGES OF LENSTRA FACTORIZATION METHOD ON EDWARDS CURVES

L. Kovalchuk
Doctor of Technical Sciences, Professor*
E-mail: lusi.kovalchuk@gmail.com
O. Bespalov
Postgraduate student**
E-mail: alexb5dh@gmail.com
N. Kuchynska
PhD*
E-mail: n.kuchinska@gmail.com
P. Seliukh
Postgraduate student**
E-mail: baidenko.polina@gmail.com
A. Zhylin
PhD
Department of Security of State Information Resources***
E-mail: zhylinartem@gmail.com
V. Tsurkan
PhD
Department of cybersecurity and application of automated information systems and technologies***
E-mail: v.v.tsurkan@gmail.com
*Department No. 22
Institute of Foreign Intelligence Service of Ukraine
Bulvarno-Kudriavska str., 11, Kyiv, Ukraine, 04053
**Department of Mathematical Methods of Information Security
Institute of Physics and Technology****
Institute of Special Communication and Information Security*
****National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Peremohy ave., 37, Kyiv, Ukraine, 03056

1. Introduction

The problems of information security that exist at present are solved by the methods and algorithms, the cryptographic resistance of which is based, particularly, on the complexity of solution to the factorization problem – the search for a nontrivial divisor for a large number. In 2009, the number RSA-768 was factorized in 2009 within the RSA-competition that was already closed. Specified 768-bit number (232 decimal digits) is currently the largest number, known from public sources, which was factorized. To factorize it, the researchers from 6 countries united; more than 10^{20} operations

were performed, which is equivalent to almost 2,000 years of computations on a single-core processor of 2.2 GHz and the technical potential of more than 5 grid systems, specifically, Grid'5000, was used. Factorization of 1024-bit RSA number according to the estimation of authors in [1] is 1,000 times as complex as RSA-768. That is why modern requirements for the length of the RSA number (1,024 and 2,048 bits) ensure, at a guarantee and with a significant margin, the security of a cryptosystem against a significant increase of computing capabilities or new algorithms emergence. Based on the Moore's law, it can be argued that with the increasing power of computers, it becomes possible to increase proportionally the efficiency of the factorization algorithms. However, in addition to the time of computations another important resource for this problem is the amount of memory used. For example, a significant memory capacity is needed for algorithms of sifting – a numerical sieve and a quadratic sieve.

A more detailed review of the modern factorization methods, including the Lenstra method, the relevance and modern progress in factorization problem solving can be found in papers [2, 3].

The Lenstra method [4–8] is one of the fastest general methods of integer number factorization. It can be used both as a separate factorization method, and as one of the stages of the "sifting" methods, which are the fastest factorization methods [9–11]. This algorithm uses the elliptic curve over the rational numbers field and some its reduction by the integer modulo, and requires about $2\log_2 k$ additions of the points of this curve, where k is the algorithm parameter, the choice of which defones the probability of success of the algorithm. Therefore, the operation time of the Lenstra algorithm is proportional to the time of points addition. This fact naturally suggests using such elliptic curves, on which the operation of points addition runs fastest, particularly, Edwards curves, to implement this method.

However, it should be noted that the classic Lenstra algorithm is based on some property of elliptic curves in the Weierstrass form, which is absent for Edwards curve. This property is the existence of a point on infinity, which has no coordinates and, therefore, is not a solution of the corresponding curve equation. That is why it is not possible to transfer directly the Lenstra method on Edwards curves.

The existence of fast number factorization algorithms is a sufficient condition for breaking the RSA cryptosystem and other similar cryptosystems. That is why the problem of construction and substantiation of such algorithms will be relevant as long as the RSA-like cryptosystems are widely used.

2. Literature review and problem statement

The Lenstra number factorization method was proposed in [4]. For factorization of integer $n=pq$, which is the product of two integers p and q, Lenstra suggested using an analogue of an elliptic curve in the Weierstrass form over ring Z_n. The powerful mathematical apparatus that is best described in [7] was developed to substantiate the correctness of operation, estimation of time and probability of success of the method. Although the Lenstra method is not the fastest factorization method, it can perform factorization in those cases where the fastest "sifting" methods appear to be powerless.

Later, the Lenstra method started to be used on the Montgomery curves, which made it possible to increase its speed. With the emergence of a new form of elliptic curves, the so-called Edwards form, the interest in the Lenstra method significantly increased. The first work on this topic is the research of Bernstein [9], which presented the conditions of such Edwards curves existence, which would surely contain the points of small orders, for example, orders of 2, 4, 6, 8. It was also experimentally shown that the probability of success of the algorithm on Edwards curve that contains the points of such orders is increasing within one percent.

Bernstein's ideas received further development in papers [2, 10, 11]. In 2013, using the Lenstra method, it became possible to find 274-bit divisor for 787-bit number ($7^{337}+1$).

In paper [11], the proposed ideas were improved, due to which, according to the experimental data, the probability of success is growing by another 1–2 %. In article [2], it is proposed to combine the use of curves in the Montgomery form and in the Edwards form to achieve the best results when using in some algorithms of factoring integer and computing of discrete logarithm.

However, it should be noted that the following problems were considered in none of these works:

– construction of a clear description of the Lenstra factorization algorithm that takes into consideration the specificity of Edwards curves;

– mathematical proves of correctness of this algorithm on Edwards curves;

– analytical estimations of its speed and a gain in performance speed;

– analytical estimations of the probability of success and its increase relative to the probability of success of the Lenstra method on the Weierstrass curves.

The main findings regarding the effectiveness of the method were made based on the experimental data, and the mathematical statements, obtained in them, mostly concerned certain technical details of the algorithm implementation (selection of the parameters of a curve, selection of coordinates, etc.).

That is why many theoretical problems remain unresolved. First of all, it is due to the necessity to develop such a mathematical apparatus that will make it possible to obtain for Edwards curves the similar results to previously obtained for Weierstrass curves. Consequently it appears appropriate to conduct studies in this direction to answer at least a part of the listed issues.

3. The aim and objectives of the investigations

The aim of this investigation is the development and strict mathematical substantiation of the Lenstra method on Edwards curves, as well as substantiation of its basic properties, advantages and offering the recommendations regarding the application.

That is why the objectives of this research can be stated as follows:

– to develop the mathematical apparatus, necessary for adaptation of the Lenstra method for Edwards curves;

– using the specified mathematical apparatus, to design the modification of the Lenstra method, adapted to Edwards curves, and to substantiate correctness of this method;

– to provide a detailed algorithm that implements the Lenstra method on Edwards curves;

– to construct the analytical estimates of the algorithm characteristics (speed, probability of success), to explore possible changes in the algorithm performance, using differ-

ent types of Edwards curves, make an additional analysis of the algorithm operation.

4. The Lenstra method on an elliptic curve in the Weierstrass form: connection with other methods of factorization and its merits

4. 1. Basic factorization methods. Features and benefits of the Lenstra method

Among modern factorization methods, we will separate the following exponential by complexity algorithms: the Pollard's $p-1$ algorithm, probabilistic Pollard's rho algorithm, the Shanks methods. The sub-exponential algorithms include the quadratic sieve algorithm, other sifting algorithms, the Dixon method, the Lenstra elliptic-curve factorization algorithm. We will note that the complexity of some algorithms depends on number of digits of the factorized number, while for the others, such as Pollard's rho-method, the Lenstra algorithm; it depends on the value of the sought-for divisor. We will separately emphasize that the selection of algorithm depends on the information about the factorized number, for example, about its special form or the special properties of its divisors. In addition, it is worth taking into consideration the amount of memory available for storing intermediate computations results, for example, for sifting algorithms.

In terms of security against cryptanalysis algorithms, it is possible to select prime numbers when constructing cryptosystems so that the use of number factorization algorithms would be ineffective. However, this approach will not work for the Lenstra method. This is its essential advantage. It is not possible to sort out all elliptic curves over the specified prime field to check the properties. That is, we can in advance select such prime numbers that their product surely cannot be factorized within the time acceptable for all the other methods, but this statement is not true regarding the Lenstra method. That is why one never knows beforehand how vulnerable to this method such product will be.

4. 2. The prototype of the classic Lenstra method – the Pollard's $p-1$ method

Let us start with the description of the Pollard's $p-1$ method [7, 8, 14], which can be considered as the Lenstra method prototype. The successful application of the Pollard method is possible only for the numbers of a certain kind. It is quite effective in such cases. The main purpose of this method consists in searching prime divisors of composite number n. Suppose that one of the prime divisors p of this number has the following property: all prime divisors of $p-1$ are "small", for example, they are not exceeding a certain number B.

Let us assume that a is such natural number that $(a, p)=1$. Then, according to the Fermat's little theorem $a^{p-1}=1(\text{mod } p)$, that is $p|a^{p-1}-1$, therefore, $(n, a^p-1)=p$.

But number p is unknown, so we do the following. Let $s_1, s_2,..., s_r$ be first r of prime numbers, $e_1, e_2,..., e_r$ are small prime numbers. We will compute

$$k=\prod_{i=1}^{r} s_i^{e_i}. \quad (1)$$

The algorithm operation will be successful if

$$p-1\,|\,k. \quad (2)$$

Indeed, with respect to condition (2), equality $a^k\equiv \equiv 1(\text{mod } p)$ is satisfied, that is why

$$\left(n, a^p-1\right)=p. \quad (3)$$

It should be noted that equality (2) is not a necessary condition fulfillment of equality (3). Actually, let us $(a, p)=1$, then $ord(a \bmod p)=l|p-1$. Then to fulfill condition (3), it is enough

$$ord\left(a \bmod p\right)|\,k. \quad (4)$$

That is, if number a is such that its multiplicative order is small enough in Z_p^*, it is sufficient to find divisor p of n from condition (3). In this case, condition (4) is much weaker than condition (2), and probability of its satisfaction for random number a is equal to $\frac{\sum_{d|(k,p-1)}\varphi(d)}{p-1}$.

If condition (4) is satisfied, the time of algorithm operation is equal $2\log(2kn)$ operations. The Pollard algorithm can be written down step-by-step as follows:

Algorithm 1

$p-1$ – the Pollard method

Input: n – composite.

1. Select k that has the form (1) (or we select in any other way so that k should have many small prime divisors, for example, $k=HCK(2,..., M)$ for natural number M).

2. Randomly select a so that $1<a<n$.

3. Compute $D=(a^k-1, n)$. If $1<D<n$, then $p=D$. The algorithm derives value p and completes the work.

If $D=1$, come back to step 1 and select larger value of k.

If $D=n$, come back to step 2 and select a new value of a.

Algorithm 1 successfully completes the work only in case, if one is lucky to find such a, for which condition (4) at some k is satisfied. The higher the value of k, the greater the probability of success. That is why it is necessary to select this number as high as computational capabilities allow. If for all divisors p of n, the following condition is satisfied: $p-1$ have only large prime divisors, the time algorithm operation is not essentially different from the operation time of the complete sorting algorithm.

4. 3. The classic Lenstra algorithm

The prototype of the classic Lenstra algorithm – the Pollard method – is based on the fact that under certain conditions, it is possible to pick up such natural number a that for some $p|n$, its order in group Z_p^* is small enough. However, the main shortcoming of this method is impossibility of using it under condition that all divisors p of number n are the ones that p–1 have large prime divisors. That is, number n can be constructed in advance so that the Pollard algorithm could be impossible to apply.

The method, proposed by Lenstra [4–6], does not have this drawback. The reason for this is that the group, in which the Lenstra method operate, for the same number p can be constructed in many different ways. That is why the existence of small orders elements in group does not depend on factorization of number p–1. This is what differs the Lenstra method from the Pollard methods and the others, which can operate only in group Z_p^*.

The basic idea of the Lenstra method is to use group E_p of the points at an elliptic curve above field F_p instead of group

Z_p^*, and a certain point P of this curve instead of number a. By the Hasse's theorem, the number $N(E_p)$ of the curve points is evenly distributed within

$$p+1-2\sqrt{p} \le N\left(E_p\right) \le p+1+2\sqrt{p}.$$

That is why among all the curves, it is possible to find the one, the order of which has many "small" divisors. Then, accordingly, the probability to select point $P \in E_p$, that has "small" order, specifically, the order that is a divisor of number k, determined in (1), is quite high. Specifically, if E_p is cyclic (like the group of the points on Edwards curve), the probability of selecting a "suitable" point is equal to $\frac{\sum_{d\left(k,N\left(E_p\right)\right)} \varphi(d)}{N\left(E_p\right)}$.

Particularly, if $N(E_p)|k$, the probability of success will be equal to 1. Actually, in this case $(k, N(E_p))=N(E_p)$, then

$$\frac{\sum_{d\left(k,N\left(E_p\right)\right)} \varphi(d)}{N\left(E_p\right)} = \frac{\sum_{d|N\left(E_p\right)} \varphi(d)}{N\left(E_p\right)} = \frac{N\left(E_p\right)}{N\left(E_p\right)} = 1.$$

Correctness of the Lenstra algorithm operation is provided by the following theorem.

Theorem 1 (The Lenstra theorem, [7])

Let $E: y^2=x^3+bx+c$, $b, c \in Z$ is a certain elliptic curve, for which condition $(4b^3+27c^2, n)=1$ is satisfied. Let us assume that P_1 and P_2 are such points on this curve that $P_1 \neq P_2$ and denominators of coordinates are co-prime with n. Then point P_1+P_2 has such coordinates, in which denominators are co-prime with n, then and only then when for any space p, which is a divisor of number n, the sum of points $P_1 \bmod p + P_2 \bmod p$ on curve $E \bmod p$ is not equal to a point on infinity.

The Lenstra algorithm can be written down step-by-step as follows:

Algorithm 2

Classic Lenstra method

Input: n – composite.

1. Select randomly b, x_0, y_0 from 2 to n.

2. Compute $c=(y_0^2-x_0^3-bx_0) \bmod n$.

Then consider the elliptic curve in the Weierstrass form $E: y^2=x^3+bx+c$, $b, c \in Z$ and the point on it $P(x_0, y_0)$.

3. Compute $D=\left(4b^3+27c^2, n\right)$.

If $1<D<n$, then $p=D$. The algorithm derives value p and completes the work.

If $D=n$, return to step 1 and select a new value b.

4. Select k, that has the form (1) (or select in any other way so that k should have many small prime divisors: for example, $k=HCK(2,..., M)$ for a certain natural number M).

5. Using the Horner's scheme, sequentially compute kP from the formulas of points addition on the curve [7]. In this case, if in the process of computation, there occurred a situation when at points addition $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$, denominators in coordinates of point $P_3(x_3, y_3)=P_1+P_2$ are not co-prime with n, that is, $1<D<n$, where

$$D=\begin{cases}\left(x_2-x_1, n\right), & \text{if} \quad P_1 \neq P_2;\\ \left(y_1, n\right), & \text{if} \quad P_1 = P_2,\end{cases}$$

then $p=D$, the algorithm derives the value of p and completes the work.

If $D=1$ for all the time of computations, or at a certain step $D=n$, it is necessary to return to step 4 and increase the value of k (as long as computational capabilities allow), or return to step 1 and select a new elliptic curve.

According to approximated estimates, presented in [5, 6], if number k has the form (1), the probability of success is not less than $2^{\frac{\log p}{\log s_r}\log\frac{\log p}{\log s_r}}$, where s_r is the largest prime divisor of k in (1). Specifically, if $\log s_r \approx \log p$, the probability of success is close to 1; if $s_r \approx \sqrt{p}$, the probability of success is approximately 0.25.

Repeating the algorithm several times for different parameters of the curve and different points, we increase the success probability.

The time complexity of algorithm, according to the estimations from the same work is

$$O\left(2^{\lambda(\log n)^{\frac{1}{2}}(\log\log n)^{\frac{1}{2}}}\right) \tag{5}$$

for some $\lambda>0$, where parameter λ depends on the time of performance of addition of points on the curve. As we can see, the time complexity of algorithm is the same as the best factorization algorithms.

5. Development of the mathematical apparatus necessary for the construction and substantiation of the Lenstra method on Edwards curves

The equation of the elliptic curve in the form, which later took the name "Edwards form", was suggested in paper [12]. The isomorphism (under certain conditions) between the curves in the Weierstrass form and in the Edwards form was proved. However, the curves, proposed in [12], were weak from the cryptographic point of view. But paper [12] was quickly followed by paper [13], where the Edwards curves were modified by the introduction of a certain parameter. The equations of the curves, proposed in [13], over a finite field of characteristics p>2 take the form:

$$E: x^2+y^2=e^2\left(1+dx^2y^2\right),$$

where parameter d is the quadratic non-residue by modulo p.

Hereafter, for simplification, we will consider $e=1$ and explore curve E_p, assigned over prime field F_p by equation

$$x^2+y^2=1+dx^2y^2, \quad \left(\frac{d}{p}\right)=-1. \tag{6}$$

The main differences (almost all of which are advantages) of the Edwards curve compared with the Weierstrass curve are the following.

1) *Universality of the addition law.* Indeed, the operations of different points addition and doubling a point are assigned by the same formulas:

$$\left(x_1, y_1\right)+\left(x_2, y_2\right)=\left(\frac{x_1y_2+x_2y_1}{1+dx_1x_2y_1y_2}, \frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right). \tag{7}$$

2) *The absence of "the point on infinity"*. Thus, the neutral element is a usual point of the Edwards curve with coordinates (0.1), which obviously fulfill equation (7).

3) *Group E_p is always cyclic.*

4) *The order of group E_p is always divided by 4.* The property of the Edwards curve can be considered an insignificant disadvantage due to the fact that its subgroup of the large prime order, on the basis of which cryptosystems are constructed, will have at least 4 times as few points as the whole group, that is, at least three-quarters of the points of the group are "extra".

5) *The record speed of points addition.* This property is one of the most important advantages of the Edwards curve. Thus, approximately 1.5 as little bit operations are required for two (different) points addition of the Edwards curve rather than points addition of the Weierstrass curve; at points doubling, the number of bit operations is even less. There is an especially significant gain in performance speed for the so-called twisted Edwards curves, the equations of which differ from equation (7) by the existence of a certain additional parameter [15, 16].

6) *Uniformity of the addition law.* The formulas for adding points along the Edwards curve are the same for adding different points and for doubling point. This increases stability of cryptosystems on the Edwards curves to timing and capacitive attacks, aimed at determining the number, by which the point of a curve is multiplied.

We will remind that the major operation that is performed in the Lenstra algorithm is adding points on the elliptic curve. More precisely, its implementation requires about k operations of points addition, where k is determined according to (1). That is why at a significant increase in performance speed of this operation, the algorithm time complexity will also be greatly enhanced.

If the order of Weierstrass curve has exactly two points of the fourth order, then it will be isomorphic to some Edwards curve (6).

$$W_p : v^2 = u^3 + au + b.$$

The necessary and sufficient conditions for the existence of exactly two points of the fourth order, as well as formulas that define an isomorphism, can be found in [17, 18].

The proposed Lenstra algorithm for the Edwards curve mainly consists of the same steps as the classic algorithm, but the substantiation of the correctness of its operation on the Edwards curve is quite different. Correctness of the operation of the classic algorithm is based on the Lenstra theorem, various modifications of which can be found in [4–7]. And correctness of the operation of the namesake algorithm for the case with the Edwards curve is partly based on theorem 1 from [19] and will be partly substantiated by the results, proved further in this paper.

Theorem 2.
Let

$$d \in Q_p \tag{8}$$

and a certain curve is assigned by equation

$$\widetilde{E}_p:\ x^2 + y^2 = 1 + dx^2y^2 \tag{9}$$

over F_p.

Then for any point $(x_1, y_1) \in E_p$, such point $(x_2, y_2) \in E_p$ can be found that

$$dx_1x_2y_1y_2 \equiv 1 \pmod p. \tag{10}$$

Similarly, for any point $(x_1, y_1) \in E_p$, such point $(x_2, y_2) \in E_p$ will be found that

$$dx_1x_2y_1y_2 \equiv -1 \pmod p. \tag{11}$$

Proof

Let us take an arbitrary point (x_1, y_1), which satisfies equation (9) and the one that $x_1y_1 \neq 0$. We will put

$$U = \frac{(x_1 + y_1)^2}{dx_1^2y_1^2},\quad V = \frac{(x_1 - y_1)^2}{dx_1^2y_1^2}.$$

Due to (8), $U, V \in Q_p$, therefore, there are such $A, B \in F_p$, that $U=A^2$, $V=B^2$. Now we put

$$x_2 = \frac{A+B}{2},\quad y_2 = \frac{A-B}{2}.$$

Then

$$x_2y_2 = \frac{A+B}{2}\cdot\frac{A-B}{2} = \frac{A^2-B^2}{4} =$$
$$= \frac{(x_1+y_1)^2 - (x_1-y_1)^2}{4dx_1^2y_1^2} = \frac{4x_1y_1}{4dx_1^2y_1^2} = \frac{1}{dx_1y_1}, \tag{12}$$

that is, (10) is satisfied.

Then,

$$x_2^2 + y_2^2 = \frac{(A+B)^2}{4} + \frac{(A-B)^2}{4} = \frac{2A^2+2B^2}{4} =$$
$$= \frac{A^2+B^2}{2} = \frac{(x_1+y_1)^2 + (x_1-y_1)^2}{2dx_1^2y_1^2} =$$
$$= \frac{2(x_1^2+y_1^2)}{2dx_1^2y_1^2} = \frac{1+dx_1^2y_1^2}{dx_1^2y_1^2} = 1 + \frac{1}{dx_1^2y_1^2} =$$
$$= 1 + \frac{d}{(dx_1y_1)^2} = 1 + d\frac{1}{\frac{1}{x_2^2y_2^2}} = 1 + dx_2^2y_2^2, \tag{13}$$

where the last but one equation is true due to (12).

It follows from (13) that $(x_2, y_2) \in E_p$.

Statement (11) is proved similarly.

The theorem is proved.

Then we will need the theorem that describes the structure of the Edwards curve over finite ring Z_n.

For some composite number $n \in \mathbf{N}$ and arbitrary $d \in Z_n$ we will designate

$$E_n = \left\{(x,y) \in Z_n \times Z_n : x^2 + y^2 \equiv 1 + dx^2y^2 \pmod n\right\} \tag{14}$$

a subset of a set of points of Cartesian product $Z_n \times Z_n$, which satisfies the correspondent congruence.

Definition 1: a set of points (14) will be called the generalized Edwards curve over the residue ring Z_n.

For arbitrary prime p, which is a divisor of n, we will designate by $E_n \bmod p$ the curve, formed from E_n by the reduction of its coordinates by modulo p:

$$E_n \bmod p = \left\{(x \bmod p, y \bmod p) \in Z_p \times Z_p : (x,y) \in E_n\right\}. \tag{15}$$

(15) shows that every point $P=(x,y)\in E_n$ is correspondent to a single point

$$P \bmod p=(x \bmod p, y \bmod p)\in E_n \bmod p,$$

moreover, by the properties of congruencies (since $p|n$), its coordinates fulfill the congruence

$$(x \bmod p)^2+(y \bmod p)^2\equiv$$
$$\equiv 1+(d \bmod p)(x \bmod p)^2(y \bmod p)^2 (\bmod p), \qquad (16)$$

obtained from (14) by reducing by modulo p.

We will note that so far we do not introduce the operation of points addition on this curve and do not explore its closure under this operation.

Theorem 3: let $n=pq$. Then in designations (14)–(16), representations

$$f: E_n \to (E_n \bmod p)\times(E_n \bmod q),$$

assigned as

$$\forall P\in E_n: f(P)=(P \bmod p, P \bmod q), \qquad (17)$$

or (which is the same as)

$$\forall (x,y)\in E_n: f((x,y))=$$
$$=((x \bmod p, y \bmod p),(x \bmod q, y \bmod q)),$$

is a bijection.

Proof.

To prove it, it is sufficiently to show that representation (17) is reversible, so for any pair of points $T_p\in E_n \bmod p$, $T_q\in E_n \bmod q$, there is a single point $T\in E_n$, the one that

$$f(T)=(T_p,T_q).$$

Let

$T_p=(x_p, y_p)$; $T_q=(x_q, y_q)$.

Construct point $T=(x,y)\in E_n$, for which $f(T)=(T_p, T_q)$, and show that it is single.

Coordinates of point $T\in E_n$ will be obtained from the system of congruencies

$$\begin{cases} x\equiv x_p (\bmod p);\\ y\equiv y_p (\bmod p);\\ x\equiv x_q (\bmod q);\\ y\equiv q_p (\bmod q), \end{cases} \qquad (18)$$

which is decomposed into two independent congruencies:

$$\begin{cases} x\equiv x_p (\bmod p);\\ x\equiv x_q (\bmod q), \end{cases} \text{ and } \begin{cases} y\equiv y_p (\bmod p);\\ y\equiv q_p (\bmod q). \end{cases} \qquad (19)$$

Since $(p, q)=1$, then according to the Remainder Chinese Theorem, in set $\{0, 1,...., n-1\}\times\{0, 1,...., n-1\}$ there is a single pair (x, y), which satisfies (18) and (19). In this case, $x \bmod p=x_p$, $y \bmod p=y_p$, $x \bmod q=x_q$, $y \bmod q=y_q$, that is why for point $T=(x, y)$, $T \bmod p=T_p$, $T \bmod q=T_q$ is satisfied and, as it was mentioned above, this is a single point.

We will show that $T\in E_n$, that is, (14) holds for its coordinates (x, y).

Since $T_p\in E_n \bmod p$, then

$$x_p^{\,2}+y_p^{\,2}\equiv 1+(d \bmod p)x_p^{\,2}y_p^{\,2} (\bmod p),$$

in this case, since

$$d \bmod p\equiv d (\bmod p),\quad x_p\equiv x (\bmod p),\quad y_p\equiv y (\bmod p).$$

Congruence will fulfill

$$x^2+y^2\equiv 1+dx^2y^2 (\bmod p). \qquad (20)$$

Based on similar considerations, congruence will fulfill

$$x^2+y^2\equiv 1+dx^2y^2 (\bmod q). \qquad (21)$$

Since $n=pq$ and $(p, q)=1$, then, by the properties of congruencies, fulfillment of congruencies follows from (21) and (22)

$$x^2+y^2\equiv 1+dx^2y^2 (\bmod n),$$

which means $T\in E_n$. The theorem is proved.

Now we will state the theorem, which will be used during the estimation of the probability of Lenstra algorithm success, proposed below.

Theorem 4.

Let n be composite number, which is divided by prime number p; E_n is the Edwards curve over ring Z_n, assigned by equation (9); P is its point. Let it for some $k\in \mathbb{N}$, condition holds

$$\operatorname{ord}(P \bmod p)\,|\,k, \qquad (22)$$

where by the order of point $P \bmod p$, we imply its order as an group element of Edwards curve points in the generalized form (according to the classification of curves, proposed in [15]) $E_n \bmod p$.

Then, the following condition holds for point kP: either enumerators, or denominators of its coordinates have a common divisor with number n that is larger than one.

Proof.

Let us assume that denominators of the coordinates of points $k(P \bmod p)$ are co-prime with number n. Then, according to Theorem 1 from [19],

$$P \bmod p\in E_n \bmod p,$$

and under condition of (22), point $k(P \bmod p)$ is a neutral element of group $E_n \bmod p$, i.e. $k(P \bmod p)=(0,1)$. Then for point $P=(x,y)\in E_n$, according to Theorem 3, the following condition holds:

$$\begin{cases} x\equiv 0 (\bmod p);\\ y\equiv 1 (\bmod p). \end{cases}$$

And this means that $x \vdots p$, i. e. $(x, n)\geq p$. The Theorem is proved.

6. The algorithm that implements the Lenstra method on Edwards curves, and its properties: construction and substantiation

We will state the ideas that lie at the core of the Lenstra algorithm on the Edwards curves and construct the algorithm itself. The first of the ideas is the following. If parameter $d \in Z_p$ in equation (8) is quadratic residue, then according to Theorem 2, there surely be found such pairs of points on the curve (and there will be quite of lot of such pairs), the denominator of points addition will be equal to zero. Then, we consider $n=pq$, where p and q are unknown prime numbers. If we choose such $d \in Z_n^*$, that $\left(\frac{d}{n}\right)=-1$, then by the property of multiplicativity of a Jacobi symbol,

$$-1=\left(\frac{d}{n}\right)=\left(\frac{d}{p}\right)\left(\frac{d}{q}\right),$$

that is why either $d \bmod p \in Q_p$, or $d \bmod q \in Q_q$. We will consider for certainty that $d \bmod p \in Q_p$. We will consider E_n, determined in the following way: first we will assign curve $E: x^2+y^2=1+dx^2y^2$ over the field of rational numbers, then we will construct its reduction $E_n=E \bmod n$ by modulo n (detailed explanations will be found in [7]). Then such points P_1 and P_2 are sure to be found on curve E_n, so, point $(P_1+P_2)\bmod n$ will have the denominator that is divided by p, that is, the one, for which the common divisor with number n will be equal to p.

The second idea is similar to the one that is used in the classic Lenstra algorithm. If the order of point $P \bmod p$ is "small" enough, i.e. it is a divisor of k, the x-coordinate of point $kP \bmod p$ is congruent to zero by modulo p, because the largest common divisor of point $kP \bmod p$ x-coordinate will be larger than one.

It is possible to construct the following Lenstra algorithm for an Edwards curve.

Algorithm 3

Lenstra algorithm on Edwards curves

Input: n – composite.

1. Choose randomly x_0, y_0 from 2 to $n-1$.

2. Compute $D_1=(x_0, n)$ and $D_2=(y_0, n)$. If $1<D_i<n$, $i=1, 2$, then $p=D_i$. The algorithm derives the value of p and completes the operation.

3. Compute $x_0^2+y_0^2-1$.

4. Compute $D_3=\left(x_0^2+y_0^2-1, n\right)$.

If $1<D_3<n$, then $p=D_3$, then the algorithm derives the value of p and completes the operation.

If $D_3=n$, return to step 1 and select new values of x_0, y_0.

5. If

$$\left(\frac{x_0^2+y_0^2-1}{n}\right)=1,$$

return to step 1 and select new values of x_0, y_0.

6. Compute $d=\left(x_0^2+y_0^2-1\right)\left(x_0^2y_0^2\right)^{-1}$.

7. Then consider the elliptic curve in the Edwards form

$$\widetilde{E}_n: x^2+y^2=1+dx^2y^2,$$

and the point $P(x_0, y_0)$ on it.

8. Select k, which takes the form (1) (or select in any other way so that k would have many small prime divisors: for example, $k=\mathrm{HCK}(2,..., M)$ for some natural M).

9. Using the Horner's scheme, compute sequentially kP from formulas (7). In this case, every time computing points $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ addition, we compute D_i, $i=4, 5, 6, 7$ from formulas:

$$D_4=\left(1+dx_1y_1x_2y_2, n\right), \quad D_5=\left(1+dx_1y_1x_2y_2, n\right),$$

$$D_6=\left(x_1y_2+x_2y_1, n\right), \quad D_7=\left(y_1y_2-x_1x_2, n\right). \qquad (23)$$

10. If in the course of computations there occurred the situation at points addition $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ for some $i=4, 5, 6, 7$, $1<D_i<n$, then $p=D_i$. The algorithm derives the values of p and completes the work.

11. If, when computing kP, one failed to find a non-trivial divisor of number n, return to step 1 and re-select x_0, y_0, or d, or increase the value of k (as long as computational capabilities allow).

7. Discussion of the characteristics and advantages of the constructed algorithm

Let us analyze the characteristics of Algorithm 3. The number of its points additions is the same as for Algorithm 2, but due to the fact that Algorithm 3 uses the Edwards curves, each points addition will be performed approximately by 1.5 times faster. That is why the algorithm itself will be not less than 1.5 times better.

Although the main purpose of the work to get a gain in performance speed, it is important that the probability of success of Algorithm 3 should be significantly higher than for Algorithm 2, as a minimum due to extra checks (23), correctness of which is based on Theorem 2.

It is possible to additionally increase the probability of success of the algorithm by using twisted and quadratic Edwards curves instead of full curves. Probability increase in this case will take place at the expense of special points existence on such curves, getting on which also leads to the success of the algorithm. We will note that an increase in the probability of success of the algorithm automatically leads to an increase in computing speed, since in this case the average number of steps to success decreases.

To research an increase in computing speed of Algorithm 3 during the transition to twisted and quadratic curves, we conducted a number of experiments with using standard data types, which show that when using twisted or quadratic Edwards curve, the average number of steps to success is reduced by 20–30 %. These experimental results clearly indicate that the existence of specific points on the Edwards curve greatly affects the algorithm complexity and success probability. However, the analytical expressions for the construction of enhancing speed estimates and probability when using twisted and quadratic curves have not been obtained yet.

The merits of this research in comparison with the analogues [2, 3, 9, 10] is that the theoretical proves of the correctness of the Lenstra method on the Edwards curves was presented, the appropriate step-by-step algorithm was designed and it was proved that its characteristics are better than those of the classic Lenstra algorithm.

A comprehensive analysis of the possibilities and advantages of this algorithm when using quadratic and twisted Edwards curves requires a more complicated mathematical apparatus (it especially applies to the formulation and proof

of the generalizations of theorems 3 and 4) and significant computation capacities for carrying out experiments on large numbers.

The shortcomings of the research include the fact that the obtained and theoretically grounded results apply only to the full curves by Edwards. At the same time, the experimental results indicate that time of algorithm operation and the probability of its success for quadratic and twisted curves can be significantly better than those for the full ones.

That is why we believe that further analysis should focus following directions:

– development of the mathematical apparatus, which would theoretically prove the correctness of application of the Lenstra method on the twisted and quadratic Edwards curves;

– the development of the appropriate algorithm, construction and proof of analytical estimates of its characteristics (time of operation, probability of success).

We will emphasize that one of the main advantages of this algorithm is that we can not only re-select k or P, but the elliptic curve itself, that is, the group in which the algorithm operates. That is why, unlike other known factorization algorithms, it is impossible to protect from this algorithm, picking up some prime divisors of number n, since it is impossible to sort out all elliptic curves over the corresponding fields and check the orders of all points.

8. Conclusions

1. The new mathematical apparatus was developed and proved that allowed to construct and prove an analogue to the Lenstra algorithm for the full Edwards curves. The necessity of developing the new mathematical apparatus is related to the fact that Lenstra algorithm operation correctness proof on Edwards curve is based on completely different principles than classic case with Weierstrass form elliptic curve.

2. Using the developed mathematical apparatus, the modification to the Lenstra method for Edwards curves was created; the correctness of this method was proved. To substantiate the correctness of the Lenstra method, the theorems about the properties of the group of points at Edwards curves were stated and proved. These theoretical results also make it possible to construct the algorithm that implements the Lenstra method on Edwards curves.

3. A detailed step-by-step algorithm that implements the Lenstra method on Edwards curves was constructed. Theorem 2 and 4 were proved, from which it directly follows that the conditions for the success of this algorithm are wider than those of the classic Lenstra method. That is why the probability of success of the constructed algorithm is higher.

4. Comparative estimates of algorithm time complexity and probabilities of its success were constructed. It was proved that the time complexity of Lenstra algorithm modification on the Edwards curves is at least 1.5 times more efficient in comparison with classic algorithm.

The experimental results of the algorithm application made the basis for a reasonable assumption that using twisted and quadratic Edwards curves (instead of full ones) cause increase of success probability of the algorithm. This is due to the existence of a large number of special points, reaching which during the algorithm implementation leads to its successful completion.

References

1. Factorization of a 768-Bit RSA Modulus / Kleinjung T., Aoki K., Franke J., Lenstra A. K., Thomé E., Bos J. W. et. al. // Lecture Notes in Computer Science. 2010. P. 333–350. doi: https://doi.org/10.1007/978-3-642-14623-7_18
2. Bouvier C., Imbert L. Faster cofactorization with ECM using mixed representations // IACR Cryptology ePrint Archive. 2018. 669 p.
3. Lenstra A. K. General Purpose Integer Factoring // Topics in Computational Number Theory Inspired by Peter L. Montgomery. 2017. P. 116–160. doi: https://doi.org/10.1017/9781316271575.006
4. Lenstra A. K., Lenstra H. W. Jr. Algorithms in number theory // Technical Report 87-008. Chicago: University of Chicago, 1987.
5. Lenstra H. W. Jr. Elliptic curves and number-theoretic algorithms // Report 86-19. Amsterdam: Mathematisch Instituut, Universiteit van Amsterda, 1986.
6. Lenstra H. W. Factoring Integers with Elliptic Curves // The Annals of Mathematics. 1987. Vol. 126, Issue 3. P. 649. doi: https://doi.org/10.2307/1971363
7. Koblitz N. A Course in Number Theory and Cryptography. Springer, 1994. 235 p. doi: https://doi.org/10.1007/978-1-4419-8592-7
8. Ellipticheskie krivye i sovremennye algoritmy teorii chisel / Solov'ev Yu. P., Sadovnichiy V. A., Shavgurlidze E. T., Belokurov V. V. Moscow: Izhevsk, 2003. 192 p.
9. ECM using Edwards curves / Bernstein D. J., Birkner P., Lange T., Peters C. // Mathematics of Computation. 2012. Vol. 82, Issue 282. P. 1139–1179. doi: https://doi.org/10.1090/s0025-5718-2012-02633-0
10. Twisted Edwards Curves Revisited / Hisil H., Wong K. K.-H., Carter G., Dawson E. // Lecture Notes in Computer Science. 2008. P. 326–343. doi: https://doi.org/10.1007/978-3-540-89255-7_20
11. Gélin A., Kleinjung T., Lenstra A. K. Parametrizations for Families of ECM-friendly curves // IACR Cryptology ePrint Archive. 2016. URL: https://eprint.iacr.org/2016/1092.pdf
12. Edwards H. M. A normal form for elliptic curves // Bulletin of the American Mathematical Society. 2007. Vol. 44, Issue 03. P. 393–423. doi: https://doi.org/10.1090/s0273-0979-07-01153-6
13. Bernstein D. J., Lange T. Faster Addition and Doubling on Elliptic Curves // Lecture Notes in Computer Science. 2007. P. 29–50. doi: https://doi.org/10.1007/978-3-540-76900-2_3
14. Pollard J. M. Theorems on factorization and primality testing // Mathematical Proceedings of the Cambridge Philosophical Society. 1974. Vol. 76, Issue 03. P. 521. doi: https://doi.org/10.1017/s0305004100049252
15. Bessalov A. V. Ellipticheskie krivye v forme Edvardsa i kriptografiya: monografiya. Kyiv, 2017. 272 p.

16. Twisted Edwards Curves / Bernstein D. J., Birkner P., Joye M., Lange T., Peters C. // Lecture Notes in Computer Science. 2008. P. 389–405. doi: https://doi.org/10.1007/978-3-540-68164-9_26
17. Bessalov A. V., Kovalchuk L. V. Exact Number of Elliptic Curves in the Canonical Form, Which are Isomorphic to Edwards Curves Over Prime Field // Cybernetics and Systems Analysis. 2015. Vol. 51, Issue 2. P. 165–172. doi: https://doi.org/10.1007/s10559-015-9709-x
18. Bessalov A. V., Dihtenko A. A. Cryptographically resistant Edwards curves over prime fields // Applied Radio Electronics. 2013. Vol. 12, Issue 2. P. 285–291.
19. Bespalov O. Yu., Kuchynska N. V. Kryva Edvardsa nad kiltsem lyshkiv yak dekartiv dobutok kryvykh Edvardsa nad skinchenymy poliamy // Prikladnaya radioelektronika. 2017. Vol. 16, Issue 3-4. P. 170–175.

Метод Ферма вважається кращим при факторизації чисел $N=p\cdot q$ у випадку близьких p і q. Обчислювальна складність базового алгоритму методу визначається кількістю пробних значень X при вирішенні рівняння $Y^2=X^2-N$, а також складністю арифметичних операцій. Для її зниження запропоновано в якості допустимих розглядати ті з пробних X, для яких $(X^2-N)\,\mathrm{mod}\,bb$ є квадратним залишком по модулю bb, названого базовым. При використанні базової основи модуля bb число пробних X зменшується в число раз, близьке до $Z(N,bb)=bb/bb^*$, де bb^* – число елементів множини T коренів рівняння $(Y\,\mathrm{mod}\,b)^2\,\mathrm{mod}\,b=((X\,\mathrm{mod}\,b)^2-N\,\mathrm{mod}\,b)\,\mathrm{mod}\,b$, а Z – коефіцієнт прискорення.

Визначено, що на величину Z(N,bb) впливають значення залишків $N\,\mathrm{mod}\,p$ (при p=2 використовуються залишки $N\,\mathrm{mod}\,8$). Запропоновано постановку задачі пошуку bb з максимальным Z(N,bb) при обмеженях на обсяг пам'яті ЕОМ, де визначаються показники степенів простих чисел – множників bb, та спосіб її вирішення.

Для зменшення числа арифметичних операцій з великими числами попонується замість таких виконувати операції зі значеннями різниць між найближчими значеннями елементів множини T. Тоді арифметичні операції множення і додавання з великими числами виконуються рідко. А якщо квадратний корінь з X^2-N визначати тільки у випадках, коли значення

$(X^2-N)\,\mathrm{mod}\,b$ будуть квадратними залишками для багатьох різних основ модуля b, то обчислювальною складністю цієї операції можна знехтувати.

Встановлено, що тоді запропонований модифікований алгоритм методу Ферма для чисел 2^{1024} забезпечує зниження обчислювальної складності в порівнянні з базовим алгоритмом в середньому в 10^7 раз

Ключові слова: факторизація, метод Ферма, обчислювальна складність, базова основа, проріджування, квадратні залишки

UDC 511:003.26.09
DOI: 10.15587/1729-4061.2018.150870

APPLICATION OF THE BASIC MODULE'S FOUNDATION FOR FACTORIZATION OF BIG NUMBERS BY THE FERMAT METHOD

S. Vynnychuk
Doctor of Technical Sciences,
Senior Researcher, Head of Department
Department of modeling of
energy processes and systems
Pukhov Institute for Modelling in Energy
Engineering National Academy of
Sciences of Ukraine
Henerala Naumova str., 15, Kyiv, Ukraine, 03164
E-mail: vynnychuk@i.ua
Y. Maksymenko
PhD*
E-mail: maksimenco@gmail.com
V. Romanenko
PhD, Head of Department*
E-mail: roma_38@ukr.net
*Institute of Special Communication
and Information Security
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
Verhnyoklyuchova str., 4, Kyiv, Ukraine, 03056

1. Introduction

At present, the issue of information security is one of the most relevant. One of the ways to solve it is information encryption. Among the ways of encryption, the asymmetric crypto-algorithm (ACA) RSA has acquired widespread application. Its cryptographic resistance is caused by the complexity of factorization of big numbers $N=p\cdot q$, where p and q are prime numbers. In papers [1, 2], it was shown that the known examples of compromising the RSA algorithm work only for its specific implementations, and, as a rule, in the general case are not most effective for solving a factorization problem.

Up to now, many factorization methods have been developed. The most frequently used methods include the methods of the number field sieve (GNFS), the quadratic sieve method (QS), the Pollard method and the Fermat method [3–6]. In this case, it is believed that each of these methods is the best (most effective in terms of computational complexity) for its application area. Thus, the Fermat method is most effective at sufficiently close values of prime factors p and q, The Pollard