вимагає вихідну послідовність довжиною $2n$.

Запропонований алгоритм атаки на конструкцію проріджуючого ГПВЧ в деякій мірі є адаптацією і загальненням запропонованих ідей алгоритму диференційної атаки збоїв на базовий LFSR. Це свідчить про те, що диференційна атака на основі внесення збоїв може бути перенесена на більшість конструкцій потокових шифрів.

Основним недоліком запропонованих атак є те, що модель атаки є надзвичайно строгою. Крім основної вимоги, що накладається атаками побічних каналів – безпосередній доступ до пристрою, криптоаналітик також повинен вміти направлено вносити збої у конкретну комірку аналізованого регістру зсуву. Така строгість вносить певну додаткову складність у практичну реалізацію таких атак, проте отримані в ході дослідження науково-практичні результати можуть слугувати базисом для розробки диференційних атак на основі збоїв на реальні криптографічні пристрої, що реалізують потокове шифрування.

*Література:**1.** J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Side Channel Cryptanalysis of Product Ciphers," in Proceedings of ESORICS '98 , Springer- Verlag, September 1998, pp. 97- 110. **2.** James Alexander Muir. Techniques of side channel cryptanalysis // University of Waterloo. Dept. of Combinatorics and Optimization, 2001. **3** Sergei P. Skorobogatov, Ross J. Anderson. Optical Fault Induction Attacks // Proceedings of the 4th International Workshop Redwood Shores, CA, USA, August pages 2-12. **4.** Eli Biham , Adi Shamir, Differential Fault Analysis of Secret Key Cryptosystems // Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, p.513-525, August 17-21, 1997. **5.** P. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems. In N. Koblitz (ed.), Advances in Cryptology — Crypto '96, Lecture Notes in Computer Science, vol. 1109, pages 104-113, Springer-Verlag, 1996. **6.** D. Boneh, R. DeMillo, and R. Lipton, "On the importance of checking cryptographic protocols for faults", Proceedings of Eurocrypt, Lecture Notes in Computer Science, Springer-Verlag, LNCS 1233, pp. 37_51, 1997. **7.** Jonathan J. Hoch, Adi Shamir, Fault Analysis of Stream Ciphers, Lecture Notes in Computer Science, Volume 3156, Jul 2004, Pages 240 – 253. **8.** Schneier B. Applied cryptography. – N.Y.: John Wiley & Songs Inc., 1996. – 757 p. **9.** Menezes A., Oorshot P., Vanstone S. Handbook of applied cryptography. – N.Y: CRC Press Inc., 1996. – 816 p. **10.** Valery Shyrochyn, Ihor Vasyltsov, Bohdan Karpinskij. Hemming Weight Power Analysis of LFSR-based Stream Ciphers // Матеріали VIII міжнародної науково-технічної конференції "Досвід розробки та застосування приладо-технологічних САПР в мікроелектроніці" CADSM 2005, 23-26 лютого, 2005, Львів-Поляна, Україна, ст. 168-171. **11.** http://ssl.stu.neva.ru/psw/crypto/ potok/str_ciph.htm.

УДК 681.3.06

МЕТОД ПОДНЯТИЯ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ ПРИ ПОСТРОЕНИИ ЕЁ ПАРАМЕТРОВ С ИСПОЛЬЗОВАНИЕМ МОДУЛЯРНОГО ПОЛИНОМА

Ольга Илясова

Харьковский национальный университет радиоэлектроники

Анотація: **Розглянуто процес підняття еліптичної кривої за допомогою модулярного полінома. Доведено, що складність підняття еліптичної кривої поліноміальная.**

Summary: **The process of lifting elliptic curve with the modular polinomial was considered. At his been proved that the complication of lifting the elliptic curve is polinomial.**

Ключевые слова: **Эллиптическая кривая, порядок эллиптической кривой, поднятие кривой, модулярный полином.**

Введение

Развитие информационных технологий, способствовало возникновению и развитию электронного бизнеса. Два из наиболее важных условий существования электронного бизнеса – информационная безопасность и аутентификация. Задачи проверки целостности документа и подлинности его автора решаются при использовании ассиметричных криптосистем [1].

В настоящее время криптосистемы RSA и Эль Гамаля и их различные модификации исчерпывают свои возможности [2, 3]. Альтернативой этим системам являются криптосистемы, основанные на преобразованиях в группе точек эллиптической кривой. Такие системы в последнии годы получили широкое распространение в электронной комерции. Это связано с тем, что эти криптосистемы

обеспечивают необходимую стойкость при небольшой длине параметров. Так, согласно работам [4, 5] криптосистемы на эллиптических кривых с размером поля в 160 бит обеспечивают ту же стойкость, что и RSA с размером модуля в 1024 бит.

Для формирования ключей в криптосистемах, основанных на преобразованиях в группе точек эллиптической кривой, необходимо вычислять порядок случайно сгенерированной кривой. Для получения "приемлемых" значений стойкости и скорости преобразований используют криптосистемы над полями F_{2^n}. Для построения таких систем необходимо вычислять порядок эллиптической кривой над полем F_{2^n}. При этом сложность вычисления должна быть минимизирована. Алгоритм вычисления порядка эллиптической кривой, предложенный Т. Сатохом [6] и его модификация [1], позволяют вычислять порядок кривой с рекордной скоростью. Так для поля размерности 240 бит порядок кривой вычисляется за 25 секунд, а для поля размерности 1000 бит за 1 час [7] (вычисления производились с помощью процессора *PENTIUM* с частотой 500 МГц), в то время как наилучший результат 1999 года для поля в 2000 бит составлял около 1500 часов. При этом сложность вычислений полиномиальная. В этих модификациях используют алгоритмы поднятия кривой из поля F_{2^n} до кольца Z_{2^n}.

Цель данной статьи: 1) дать математическое описание одного из наиболее сложных этапов определения порядка кривой – процесса поднятия эллиптической кривой; 2) доказать, что сложность поднятия эллиптической кривой из поля F_{2^n} до кольца Z_{2^n} – полиномиальная.

I Алгоритм вычисления порядка эллиптической кривой

Существует два подхода для вычисления порядка эллиптической кривой. Первый подход основан на построении кривой с заданным порядком [6]. Второй подход основан на случайном выборе параметров кривой [7]. В данной статье рассмотрим алгоритм, который обеспечивает случайный выбор кривой. В нём случайным образом выбирают параметры *a, b* эллиптической кривой, после чего определяется порядок кривой. Наиболее эффективным из таких алгоритмов является алгоритм Т. Сатоха и его модификация, которая представлена в [1].

Модификация алгоритма Т. Сатоха состоит в следующем. Генерируются случайным образом параметры *a, b* эллиптической кривой *E*, определённой над полем F_{p^n}, j инвариант которой $j(E) \notin F_{p^2}$. Далее выполняются следующие шаги.

1. Строится последовательность, которая состоит из n изоморфных кривых E_i, вычисляются j инварианты кривых E_i. Данный процесс осуществляется с помощью малого эндоморфизма Фробениуса [1]. В качестве кривой E_0 рассматривается базовая кривая, все остальные кривые входящие в данную последовательность получаются в результате действия малого эндоморфизма Фробениуса на базовую кривую.

2. Осуществляетя поднятие j – ых инвариантов кривых E_i. Способ поднятия j – ых инвариантов основан на использовании модернизированых итераций Ньютона.

3. Выполняется поднятие каждой кривой с помощью вычисления её коэффициентов *a, b*. Коэффициенты вычисляются с помощью итераций Ньютона с требуемой точностью.

4. На основании данных поднятых кривых. вычисляется след эндоморфизма Фробениуса с помощью формул, выведенных J. Velu [8].

В данной статье рассматривается способ поднятия эллиптической кривой. Дается математическое описание данного процесса.

II Понятие поднятия j инварианта эллиптической кривой

Рассмотрим сначала процесс поднятия эллиптической кривой над простым полем F_p, хотя он будет таким же и в случае расширенного поля.

Эллиптическая кривая E над полем F_p, заданная уравнением $y^2 = x^3 + ax + b$ может быть вложена в кривую E' над полем *K*. Отображение точки Q кривой *E* в точку Q' кривой E' называется поднятием точки Q из поля F_p в поле K, при этом точки кривой $y^2 = x^3 + ax + b(\mathrm{mod}\, p)$ станут точками кривой

$y^2 = x^3 + Ax + B$ [9]. Такое отображение называется поднятием эллиптической кривой. Сумме точек кривой E' соответствует сумма точек кривой *E*, причем, обратное неверно. Модификация алгоритма Т. Сатоха, представленная в [1], рассматривает поднятие эллиптической кривой из поля F_{p^n} в кольцо p-адических целых Z_{p^n}. Любой элемент Z_{p^n} может быть представлен полиномом $a_{n-1}t^{n-1} + \ldots + a_1 t + a_0$, где a_i принадлежат кольцу *p*-адических целых Z_p [1]. Сумма и произведение в кольце Z_{p^n} представляет собой сумму и произведение полиномов, взятых по модулю полинома $f(t)$. Степень данного полинома $f(t)$ равна *n* , а его редукция по модулю *p* представляет собой неприводимый полином над полем F_p.

Для вычисления порядка эллиптической кривой над полем F_{p^n}, $(p=2)$ $y^2 + xy = x^3 + ax + b$, на основании теоремы Хассе используется формула $\#E = 2^n + 1 - tr(Fr_{2^n})$, где $tr(Fr_{2^n})$ – след *n*-ой степени эндоморфизма Фробениуса. Согласно оценке Хассе [10] $\left|tr(Fr_{2^n})\right| \le 2\sqrt{2^n}$. Для нахождения следа *n*-ой степени эндоморфизма Фробениуса рассматривают отображения малого эндоморфизма Фробениуса $\sigma : x \alpha\ x^2$ [5] и представляют *n*-ую степень в виде последовательности эллиптических кривых $E_0 \leftarrow E_1 \leftarrow E_2 \leftarrow \ldots \leftarrow E_{n-1} \leftarrow E_n$, $\mathrm{E}_0 = E_n$. E_0 – базовая кривая, а все остальные кривые получены одна из другой применением отображения малого эндоморфизма Фробениуса. Малый эндоморфизм Фробениуса может быть преобразован в изогении между поднятыми кривыми [10] $E_0' \leftarrow E_1' \leftarrow E_2' \leftarrow \ldots \leftarrow E_{n-1}' \leftarrow E_n'$, $\mathrm{E}_0' = E_n'$. При этом рассматривают дуальные изогении в силу их сепарабельности. В результате редукция по модулю два кривой E_i', $i = 0,\ 1,\ \ldots,\ n-1$ приводит к кривой. E_i, $i = 0,\ 1,\ \ldots,\ n-1$. Отсюда следует задача поднять решение системы уравнений

$$\begin{cases} \Phi_2(x_0, x_1) \equiv \Phi_2(x_1, x_2) \equiv \ldots \equiv \Phi_2(x_{n-1}, x_0) \equiv 0 \bmod 2 \\ x_i \equiv j(E_i) \bmod 2 \end{cases} \tag{1}$$

до решений системы

$$\begin{cases} \Phi_2(y_0, y_1) = \Phi_2(y_1, y_2) = \ldots = \Phi_2(y_{n-1}, y_0) = 0 \\ y_i \equiv j(E_i) \bmod 2. \end{cases} \tag{2}$$

Модулярный полином, рассмотренный в работе [1]

$$\Phi_2(X,\ Y) = X^3 + Y^3 - X^2Y^2 + 2^4 \cdot 3 \cdot 31\left(X^2Y + XY^2\right) - 2^4 3^4 5^3\left(X^2 + Y^2\right) + 3^4 5^3 \cdot 4027XY$$
$$+ 2^8 3^7 5^6 \cdot (X + Y) - 2^{12} 3^9 5^9,$$

обладает свойством, которое выражено в теореме, представленной в работе [11]:

Теорема 2.1. Пусть E и E' эллиптические кривые над полем комплексных чисел, тогда для изогении $\lambda : E \to E'$ с циклическим ядром степени *n* необходимо и достаточно, чтобы j – инвариант j_E являлся корнем уравнения $\Phi_n(x, j_{E'}) = 0$.

Подъём j – инварианта возможен на основе теоремы Lubin – Serre – Tate [1].

Теорема 2.2. Пусть *E* эллиптическая кривая над F_{p^n}, её j инвариант $j(E) \notin F_{p^2}$, тогда существует J из кольца Z_{p^n} такой, что $\Phi_p\left(J, \sigma^{-1}(J)\right) = 0$, $J \equiv j \bmod \mathrm{p}$, J является j инвариантом поднятой кривой.

В данной теореме $\sigma^{-1}(J)$ – это отображение, обратное отображению малого эндоморфизма Фробениуса.

Однако, непосредственное использование данной теоремы требует выполнения сложных вычислений над кольцом Z_{p^n} поля K. Поэтому на практике используют усовершенствованный метод вычисления J

без использования $\sigma^{-1}(J)$. Данный метод состоит в следующем.

1. Поднимаем j инварианты $j_i, i = 0, 1, ..., n-1$ цикла кривых $E_0 \leftarrow E_1 \leftarrow E_2 \leftarrow ... \leftarrow E_{n-1} \leftarrow E_n$, где кривая E_0 совпадает с кривой E_n;

2. Вычисляем j инварианты $j_i, i = 0, 1, ..., n-1$ поднятых кривых $E_0' \leftarrow E_1' \leftarrow E_2' \leftarrow ... \leftarrow E_{n-1}' \leftarrow E_n', \mathrm{E}_0' = E_n'$;

3. Решаем систему уравнений $\Phi_p(J_i, J_{i+1}) = 0$, в результате получаем поднятые j инварианты.

Все вычисления производятся в указанном порядке, что позволяет найти J_i без вычисления $\sigma^{-1}(J_i)$.

Описанный метод эффективен только для значений $p = 2$. Это связано с тем, что коэффициенты модулярного полинома стремительно возрастают при значениях $P > 2$, кроме этого увеличивается степень полинома.

III Алгоритм поднятия j инварианта с помощью модифицированных итераций Ньютона

Рассмотрим последовательность кривых $E_0 \leftarrow E_1 \leftarrow E_2 \leftarrow ... \leftarrow E_{n-1} \leftarrow E_n, \mathrm{E}_0 = E_n$, j инварианты которых связаны соотношением $j_i^2 \equiv j_{i+1} \bmod 2$. Для того, чтобы поднять j инварианты данных кривых, необходимо найти решения $y = (y_0, y_1, ..., y_{n-1})$ системы, представленной в [6]

$$\begin{cases} \Phi_2(y_0, y_1) = \Phi_2(y_1, y_2) = ... = \Phi_2(y_{n-1}, y_0) = 0 \\ y_i \equiv j(E_i) \bmod 2. \end{cases} \tag{3}$$

При этом считаем, что $j_i, i = 0, 1, ..., n-1$ являются приближенными корнями системы. С помощью модернизированых итераций Ньютона находим решение системы с заданной точностью. Для этого алгоритм решения уравнения с помощью итераций Ньютона преобразуем в алгоритм решения системы уравнений с помощью модернизированных итераций Ньютона. Для описания алгоритма модернизированных итераций Ньютона рассмотрим отображение $g: R^n \to R^n$, которое ставит в соответствие каждому n мерному вектору $(x_0, x_1, ..., x_{n-1})$ вектор $(\Phi_2(x_0, x_1), \Phi_2(x_1, x_2), ..., \Phi_2(x_{n-1}, x_0))$. Кроме этого рассмотрим Якобиановую матрицу A следующего вида:

$$A = \begin{pmatrix} \frac{\partial \Phi_2(j_0, j_0^{n-1})}{\partial x} & \frac{\partial \Phi_2(j_0, j_0^{n-1})}{\partial y} & 0 & \dots & 0 \\ 0 & \frac{\partial \Phi_2(j_0^{n-1}, j_0^{n-2})}{\partial x} & \frac{\partial \Phi_2(j_0^{n-1}, j_0^{n-2})}{\partial y} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ \frac{\partial \Phi_2(j_0^2, j_0)}{\partial x} & 0 & 0 & \dots & \frac{\partial \Phi_2(j_0^2, j_0)}{\partial y} \end{pmatrix}. \tag{4}$$

Обозначим матрицу, обратную матрице A, как A^{-1}. В результате получаем модернизированные итерации Ньютона, которые позволяют найти решение системы уравнений, рассмотренной выше. Данная формула [3] имеет вид:

$$(y_0, y_{n-1}, ... y_1, y_0)^t = (j_0, j_0^{n-1}, ..., j_0^2, j_0)^t - A^{-1} \cdot (\Phi_2(j_0, j_0^{n-1}), \Phi_2(j_0^{n-1}, j_0^{n-2}) ..., \Phi_2(j_0^2, j_0))^t \tag{5}$$

Элементы матрицы A обладают следующим свойством:

Утверждение: Модулярный полином

$$\Phi_2(X,Y)=X^3+Y^3-X^2Y^2+2^4\cdot 3\cdot 31\left(X^2Y+XY^2\right)-2^4 3^4 5^3\left(X^2+Y^2\right)+3^4 5^3\cdot 4027XY \\ +2^8 3^7 5^6\cdot(X+Y)-2^{12}3^9 5^9 \quad (6)$$

при следующем соотношении $z_{i+1}=z_i^2$ удовлетворяет условию

$$\frac{\partial\Phi_2(z_i,z_{i+1})}{\partial x}=\frac{\partial\Phi_2(z_{i+1},z_i)}{\partial y}. \quad (7)$$

Доказательство. Рассмотрим модулярный полином (6)

$$\Phi_2(X,Y)=X^3+Y^3-X^2Y^2+2^4\cdot 3\cdot 31\left(X^2Y+XY^2\right)-2^4 3^4 5^3\left(X^2+Y^2\right)+3^4 5^3\cdot 4027XY \\ +2^8 3^7 5^6\cdot(X+Y)-2^{12}3^9 5^9.$$

Пусть $A=2^4\cdot 3\cdot 31$, $B=2^4 3^4 5^3$, $C=3^4 5^3\cdot 4027$, $D=2^8 3^7 5^6$, $F=2^{12}3^9 5^9$.

Тогда модулярный полином будет иметь вид:

$$\Phi_2(X,Y)=X^3+Y^3-X^2Y^2+A\left(X^2Y+XY^2\right)-B\left(X^2+Y^2\right)+CXY+D\cdot(X+Y)-F. \quad (8)$$

Найдем частные производные данного модулярного полинома (8):

$$\frac{\partial\Phi_2(X,Y)}{\partial x}=3X^2-2XY^2+A\left(2XY+Y^2\right)-2BX+CY+D, \\ \frac{\partial\Phi_2(X,Y)}{\partial y}=3Y^2-2X^2Y+A\left(X^2+2XY\right)-2BY+CX+D. \quad (9)$$

В полученные выражения (9) для частных производных подставим вместо переменных X, Y следующие выражения: $X=z_i$, $\mathrm{Y}=\mathrm{z}_{\mathrm{i+1}}=z_i^2$. В результате получим

$$\frac{\partial\Phi_2\left(z_i,z_i^2\right)}{\partial x}=3z_i^2-2z_i z_i^4+A\left(2z_i z_i^2+z_i^4\right)-2Bz_i+Cz_i^2+D, \\ \frac{\partial\Phi_2\left(z_1^2,z_i\right)}{\partial y}=3z_i^2-2z_i^4 z_i+A\left(z_i^4+2z_i^2 z_i\right)-2Bz_i+Cz_i^2+D. \quad (10)$$

Преобразуем правые части выражений (10). Получаем следующие равенства

$$\frac{\partial\Phi_2\left(z_i,z_i^2\right)}{\partial x}=3z_i^2-2z_i^5+A\left(2z_i^3+z_i^4\right)-2Bz_i+Cz_i^2+D, \\ \frac{\partial\Phi_2\left(z_i^2,z_i\right)}{\partial y}=3z_i^2-2z_i^5+A\left(z_i^4+2z_i^3\right)-2Bz_i+Cz_i^2+D. \quad (11)$$

Итак, $$\frac{\partial\Phi_2\left(z_i,z_i^2\right)}{\partial x}=\frac{\partial\Phi_2\left(z_i^2,z_i\right)}{\partial y}.$$

Данное свойство модулярного полинома позволяет уменьшить количество операций умножения, которые необходимо выполнить для вычисления матрицы A^{-1}. Для обращения матрицы A необходимо вычислять алгебраические дополнения её злементов. В силу того, что матрица имеет особый вид, вычисления алгебраических дополнений сводятся к вычислению произведений элементов соответствующих миноров матрицы, стоящих на главной диагонали. Как уже было отмечено выше, сложность вычисления порядка эллиптической кривой с помощью данного алгоритма является полиномиальной. При использовании данного алгоритма для нахождения матрицы, обратной матрице A, необходимо выполнить одну инверсию и $\left(n^3+n^2+2n\right)$ операций умножения. Итак, общая формула для вычисления сложности имеет вид: $\left(n^3+n^2+2n\right)M+1I$, где M – количество умножений, а I – количество выполняемых инверсий над полем F_{2^n}.

IV Поднятие эллиптической кривой

Поднятие эллиптической кривой в рассматриваемом алгоритме осуществляется за счёт поднятия j инвариантов цикла кривых. Рассмотрим поднятие эллиптической кривой, которая задаётся уравнением $y^2 + xy = x^3 + ax^2 + b$. Для каждой такой кривой существует изоморфное отображение, при котором уравнение вида $y^2 + xy = x^3 + ax^2 + b$ приводится к виду $y^2 + xy = x^3 + B$ [13]. Если известно уравнение эллиптической кривой, тогда можно вычислить j инвариант этой кривой по её параметрам [13]. Для эллиптической кривой с параметром B j инвариант вычисляется по формуле: $J = \dfrac{-1}{B + 432B^2}$ [13]. Если j инвариант известен, то коэффициент B можно найти как корень полинома $f(x) = 432Jx^2 + Jx + 1$. Для нахождения корня можно использовать итерации Ньютона

$$x_{i+1} = x_i - \frac{432Jx_i + Jx_i + 1}{864Jx_i + J}.$$

Чтобы получить результат с удвоенной точностью в качестве приближённого корня рассматривают

$$f(x_{i+1}) = 432J\left[\frac{f(x_i)}{f'(x_i)}\right]^2 + f(x_i) - J\left[\frac{f(x_i)}{f'(x_i)}\right].$$

В результате, удваивая точность на каждом шаге, можно получить результат с заранее заданой точностью.

Количество действий, необходимых для выполнения одного шага в итерациях Ньютона, равно 3 умножениям и 1 инверсии. На каждом следующем шаге количество умножений увеличивается до 6, а количество инверсий не изменяется.

Выводы

Рассмотренный алгоритм поднятия эллиптической кривой имеет полиноминальную сложность и позволяет вычислять коэффициенты поднятой кривой с требуемой точностью. Эти преимущества, а также невысокая временная сложность вычислений, выделяют этот алгоритм среди других известных алгоритмов, прежде всего таких, как алгоритм Р. Скуфа [14] и алгоритм *SEA* [7], как один из наиболее перспективных алгоритмов.

Литература: ***1.*** *Fouquet M., Gaudry P. and. Harley R.: An extention of Satoh's algorithm and its implementation, J. Ramanujan Math. Soc. 15 2000, 281–318.* ***2.*** *ElGamal: A pablic Key Criptosystems and Signature Scheme Based on Discrete Logrithms. IEEE Trans. on Information Theory. 1985, 469– 472* ***3.*** *Горбенко І. Д., Гріненко Т. О.: Захист інформації в інформаційно – телекомунікаційних системах, Харків 2004, 30– 33.* ***4.*** *Curent Public – Key Cryptographic Systems. A Certicom Whitepaper. Certicom, 1997. www. certicom. com.* ***5.*** *Elliptic Curve and Cryptography. A Certicom Whitepaper. Certicom, 1998. www. certicom. com.* ***6.*** *Satoh T.: Canonical lifting of elliptic curves and p – adic. point counting (theoretical background, Departament of Mathematics, Faculti of Sience, Saitame University, 2001, 1–21.* ***7.*** *Телижненко А., Бессалов А.: Криптосистемы на эллиптических кривы ,Киев "Политехника" 2004.* ***8.*** *Velu J.: Isogenies entre courbes elliptiques, C. R. Acad. Sc. Paris 273, 1971, 238–241.* ***9.*** *Ростовцев А. Г.: Логарифмирование через поднятие, "Проблемы информационной безопасности. Компьютерные системы", СПб, №2 2000, 49–54.* ***10.*** *Skjernaa B.: Satoh's algorithm in Characteristic 2. Math. Comput. 72 2003, 447–487.* ***11.*** *Ленг С.: Эллиптические функции, Москва, "Наука", 1984.* ***12.*** *Morein F. Buldingcykle elliptic curves modulo large primes. INRIA, B. P. 1005, 78153 LE CHESNAY CEDEX (Franse), 1993, 328 – 336.* ***13.*** *Silverman J.H.: The arifmetic of Elliptic Curve, GTM 106, Springer – Verlad, New–York, 1986.* ***14.*** *Schoof R.: Counting points on an elliptic curve over finit fields, Proc. Journees Arifmetiques, 93. 1995, 219 – 252.*