УДК 621.391

А.А. КУЗНЕЦОВ, канд. техн. наук (г. Харьков),
В.Н. ЛЫСЕНКО, канд. техн. наук (г. Сумы),
В.Е. ЧЕВАРДИН (г. Полтава)

БЫСТРЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ В ГРУППЕ ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Розробляються швидкі перетворення в групі точок еліптичної кривої. Проводяться порівняння за складністю групових операцій. Показано, що застосування запропонованого способу дозволить істотно підвищити швидкодію несиметричної криптографічної системи.

Rapid transformations in group of points of elliptic curve are developed. Comparisons on complication of group operations are conducted. It is shown, that application offered methods will allow substantially to promote the fast-acting of the asymmetrical cryptographic system.

Постановка проблемы в общем виде, анализ литературы. Несимметричные методы криптографического преобразования информации получили в последнее время широкое развитие [1 – 3]. Это обусловлено многочисленными практическими приложениями, в которых, не накладывая ограничения на секретность ключа, можно успешно решать задачи обеспечения конфиденциальности и подлинности информации. Особое место занимают несимметричные криптосистемы, построенные на основе использования трудноразрешимой задачи взятия дискретного логарифма в группе точек эллиптической кривой [1 – 4]. Они обеспечивают наибольшую эффективность в отношении затратность/обеспечиваемая стойкость. В то же время, возрастающие объемы обрабатываемой и передаваемой криптографически защищенной информации выдвигают повышенные требования к скорости криптографических преобразований.

Целью статьи является разработка быстрых криптографических преобразований в группе точек эллиптической кривой.

Общетеоретические положения криптографических преобразований в группе точек эллиптической кривой. В качестве основного криптографического примитива в несимметричных криптосистемах, построенных над группой точек эллиптической кривой, используют групповые операции сложения и удвоения точек.

Несуперсингулярная эллиптическая кривая (*EC*) *над полем* *GF*(*q*) – множество точек над $GF(2^m)$, удовлетворяющих уравнению [4]:

$$y^2 + a_1xy = x^3 + a_2x^2 + a_5\,. \qquad (1)$$

Группа точек фиксируется применением метода секущих Диофанта [5]. Рассмотрим уравнение прямой (секущей), проходящей через произвольные две точки кривой $P_1(X_1, Y_1)$ и $P_2(X_2, Y_2)$: $y = ax + b$, где $a = (Y_2 + Y_1)/(X_2 + X_1)$, $b = aX_1 + Y_1$. Подставив в выражение (1), получим $(ax + b)^2 + a_1(ax + b)x = x^3 + a_2x^2 + a_5$. Раскроем скобки и приведем подобные. После этого получим: $x^3 + (a_2 - a^2 - a_1a)x^2 - a_1bx + a_5 - b^2 = 0$. Следовательно, $X_1 + X_2 + X_3 = a^2 + a_1a - a_2$.

Зафиксируем абелеву группу над множеством точек *EC*: зафиксируем множество элементов группы как множество точек эллиптической кривой *EC*; зафиксируем операцию сложения элементов группы как сложение элементов множества точек *EC*; зафиксируем единичный элемент группы как бесконечно удаленную точку *O*, причем $O + P = P$, $\forall P \in EC$; для всех элементов группы определим обратные элементы как точки с отрицанием *y*-координаты. Групповая операция сложения (рис.1) точек *EC* запишется в виде [4]:

$$X_3 = a^2 + a_1a - a_2 - X_1 - X_2; \qquad (2)$$

$$Y_3 = aX_3 + b.$$

Проведем через точку $P_1(X_1, Y_1)$ касательную к *EC*. Подставив уравнение касательной в выражение (1), получим $(ax + b)^2 + a_1(ax + b)x = x^3 + a_2x^2 + a_5$, где $a = (\partial y_{P_1} / \partial x_{P_1}) = y_1 / x_1 + x_1 / a_1$ – производная уравнения *EC* в точке $P_1(X_1, Y_1)$, $b = aX_1 + Y_1$. Раскроем скобки и приведем подобные, получим $x^3 + (a_2 - a^2 - a_1a)x^2 - a_1bx + a_5 - b^2 = 0$, откуда $X_3 = a^2 + a_1a - a_2$. Групповая операция удвоения (рис. 2) точек *EC* запишется в виде:

$$2P_1(X_1, Y_1) = P_3(X_3, Y_3);$$

$$X_3 = a^2 + a_1a - a_2; \qquad (3)$$

$$Y_3 = aX_3 + b.$$

Последнее выражение равносильно следующему:

$$2P_1(X_1, Y_1) = P_3(X_3, Y_3);$$

$$X_3 = (a_5 - b^2) / x_1^2; \qquad (4)$$

$$Y_3 = aX_3 + b.$$

Конечная группа точек *EC* обладает следующими свойствами [4]: замкнутость, ассоциативность, существование единицы, существование обратных элементов, коммутативность. В основе криптосистем с открытым ключом лежит трудноразрешимость взятия дискретного логарифма [1 – 3].

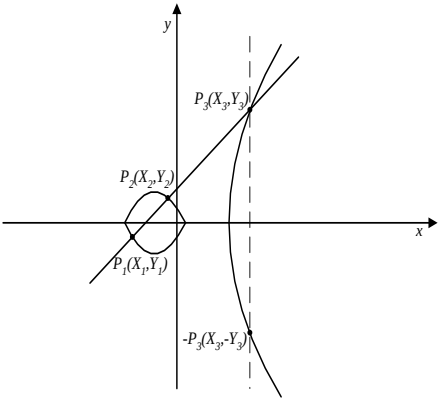

Рис. 1. Сложение точек эллиптической кривой

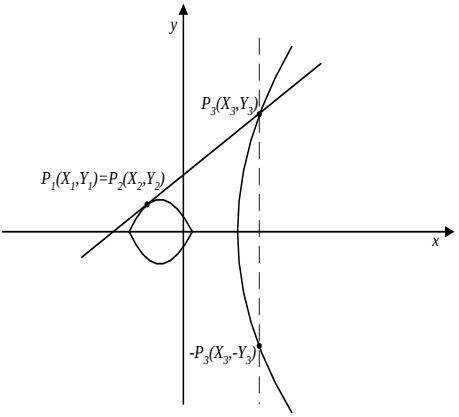

Рис. 2. Удвоение точек эллиптической кривой

Воспользуемся понятием дискретного логарифма, введенного в [6]. Пусть H – конечная группа, g и y – элементы этой группы. Любое целое x такое, что $g^x = y$ называется *дискретным логарифмом* y по основанию g. Каждый элемент $y \in H$ имеет дискретный логарифм по основанию g только тогда, когда H является циклической группой с образующей g. Применительно к группе точек эллиптической кривой используют следующее понятие дискретного логарифма на кривой.

Пусть H_{EC} – конечная группа точек эллиптической кривой, P_i и P_j – элементы этой группы. Любое целое x такое, что $xP_i = P_j$, называется *дискретным логарифмом на эллиптической кривой.* Криптостойкость алгоритмов, построенных на эллиптических кривых, основана на трудности взятия дискретного логарифма и состоит в определении x по известным P_i и P_j.

Современные требования к стойкости и производительности криптоалгоритмов с открытым ключом существенно возросли. Эффективным решением задачи повышения быстродействия криптосистмемы является использование быстрых преобразований в группе точек эллиптической кривой.

Быстрые преобразования в группе точек эллиптической кривой. Рассмотрим плоскую алгебраическую кривую, заданную уравнением $f(x, y) = 0$, т.е. множество пар (x, y), обращающих в ноль уравнение кривой. Если $f(x, y) = 0$ – многочлен с коэффициентами из конечного поля $GF(q)$,

алгебраическая кривая задается множеством решений (x, y) над $GF(q)$. Алгебраическая кривая, заданная множеством решений уравнения $f(x, y) = 0$ является *рациональной*, если координаты ее точек могут быть выражены через рациональные функции от одного параметра, т.е. если существуют две такие рациональные функции $\varphi(t)$ и $\psi(t)$, из которых хотя бы одна не постоянна, что $f(\varphi(t), \psi(t) = 0$ тождественно относительно t. Если $t = t_0$ – значение параметра, отличное от конечного числа значений, обращающих в ноль знаменатели функций $\varphi(t)$ и $\psi(t)$, то точка $(\varphi(t), \psi(t))$ принадлежит кривой. Устанавливаемое таким образом соответствие между значением параметра t и точками кривой является однозначным (если исключить из значений параметра и из множества точек конечные подмножества). При этом параметр t может быть выражен как рациональная функция от x и y. Таким образом, если известно, что кривая $f(x, y) = 0$ рациональна, а коэффициенты $\varphi(t)$ и $\psi(t)$ принадлежат полю рациональных чисел, то, когда t пробегает все рациональные значения параметризация $x = \varphi(t)$, $y = \psi(t)$ дает все точки кривой (за исключением, возможно, конечного их числа). Справедливы следующие утверждения.

Утверждение 1. Рассмотрим рациональную кривую $f(x, y) = 0$ третьей степени. Пусть $P_1(X_1, Y_1)$ и $P_2(X_2, Y_2)$ две простые точки кривой. Прямая, проходящая через $P_1(X_1, Y_1)$ и $P_2(X_2, Y_2)$, пересекает эту кривую еще не более чем в одной *простой* точке.

Доказательство. Кратность пересечения двух многообразий не превышает mn, где m и n степени соответствующих многочленов. В данном случае прямая, заданная уравнением первой степени, пересечет кривую, заданную многочленом третьей степени не более, чем в трех точках, с учетом кратности (рис. 3). Если две из трех точек пересечения простые, то третья точка имеет индекс пересечения не более 1, т.е. третья точка пересечения (если она есть) простая.

Нахождение третьей простой точки пересечения прямой и рациональной кривой третьей степени положим в основу операции сложения точек (рис. 3).

Утверждение 2. Пусть, как и прежде $P_1(X_1, Y_1)$, $P_2(X_2, Y_2)$ две простые точки кривой. Тогда касательная, проходящая через $P_1(X_1, Y_1) = P_2(X_2, Y_2)$ пересекает эту кривую еще не более, чем в одной *простой* точке.

Доказательство. Аналогично доказательству утверждения 1. Кратность пересечения двух многообразий не превышает mn, где m и n степени соответствующих многочленов. В данном случае прямая, заданная уравнением первой степени пересечет кривую, заданную многочленом третьей степени не более, чем в трех точках с учетом кратности (рис. 4). Если две из трех точек пересечения простые: $P_1(X_1, Y_1) = P_2(X_2, Y_2)$ (касательная к кривой в точке P_1), то третья точка имеет индекс пересечения не более 1, т.е. третья точка пересечения (если она есть) простая.

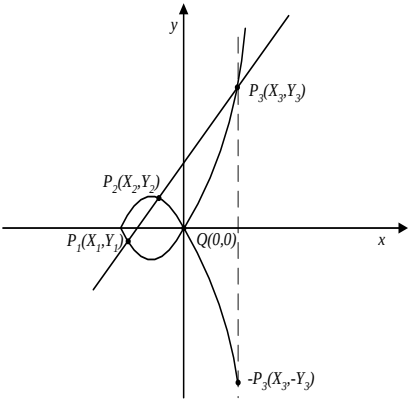

Рис. 3. Сложение точек рациональной кривой третьей степени

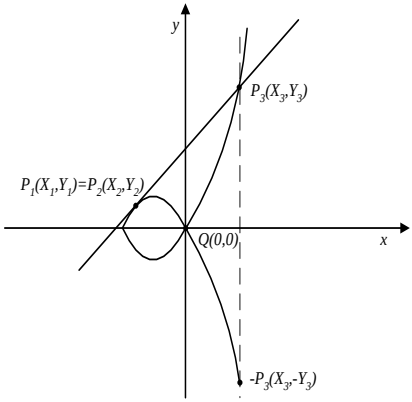

Рис. 4. Удвоение точек рациональной кривой третьей степени

Нахождение третьей простой точки пересечения касательной и рациональной кривой третьей степени положим в основу операции удвоения точек.

Отсутствие третьей точки пересечения соответствует случаю прохождения прямой параллельно оси $0Y$. Это соответствует инвертированию точки $P_1(X_1, Y_1)$ в точку $P_2(X_2, Y_2)$, т.е. в самое себя.

Рассмотрим рациональную кривую

$$y^2 + xy = x^3 + x^2 \tag{5}$$

над $GF(2^m)$. Кривая содержит одну особую точку $Q(0, 0)$. Кратность особой точки равна 2. Род кривой

$$g = (n-1)(n-2)/2 - \sum_X m_p(m_p - 1)/2 = 0,$$

кривая рациональна. Рассмотрим уравнение прямой (секущей), проходящей через две произвольные простые точки кривой $P_1(X_1, Y_1)$ и $P_2(X_2, Y_2)$. Подставив уравнение прямой (секущей), проходящей через две произвольные простые точки кривой $P_1(X_1, Y_1)$ и $P_2(X_2, Y_2)$ в выражение (5), получим в явном виде координаты третьей точки пересечения секущей и кривой (5):

$$X_3 = a^2 + a - a_2 - X_1 - X_2; \tag{6}$$

$$Y_3 = aX_3 + b.$$

Результат утверждения 1 доказывает замкнутость операции сложения простых точек на рациональной кривой третьей степени. Зафиксируем абелеву группу: зафиксируем множество элементов группы как множество

точек кривой (5), включая бесконечно удаленную точку и исключив особую точку $Q(0, 0)$; зафиксируем операцию сложения элементов группы как сложение элементов множества точек кривой (выражение (6)); зафиксируем единичный элемент группы как бесконечно удаленную точку O, причем $O + P = P$, $\forall P \in EC$; для всех элементов группы определим обратные элементы как точки с отрицанием y-координаты.

Проведем через точку $P_1(X_1, Y_1)$ касательную к кривой (5). Подставим уравнение касательной в выражение (5), групповую операцию удвоения точек кривой (5):

$$2P_1(X_1, Y_1) = P_3(X_3, Y_3);$$
$$X_3 = a^2 + a - a_2; \quad (7)$$
$$Y_3 = aX_3 + b.$$

Последнее выражение равносильно следующему:

$$2P_1(X_1, Y_1) = P_3(X_3, Y_3);$$
$$X_3 = b^2 / x_1^2; \quad (8)$$
$$Y_3 = aX_3 + b.$$

Результат утверждения 2 доказывает замкнутость операции удвоения простых точек на рациональной кривой третьей степени. Конечная абелева группа на кривой (5) обладает свойствами замкнутости, ассоциативности, существование единицы, существование обратных элементов, коммутативности.

Используя множество простых точек рациональной кривой, операции сложения и удвоения точек, зафиксируем конечную абелеву группу, определим задачу взятия дискретного логарифма в группе точек. Сложность решения последней положим в основу открытой криптосистемы. Справедливы следующие утверждения.

Утверждение 3. Рассмотрим плоскую рациональную кривую $f(x, y) = 0$. Пусть $Q(0, 0)$ – особая точка на кривой, $m_Q = 2$. Проведем через точку $Q(0, 0)$ секущую, заданную уравнением $y = tx$, где t – угловой коэффициент секущей (рис. 5). Прямая, проходящая через особую точку, пересекает эту кривую еще не более чем в одной *простой* точке.

Доказательство. Аналогично доказательству утверждений 1 – 2. Кратность пересечения двух многообразий не превышает mn, где m и n степени соответствующих многочленов. В данном случае прямая, заданная уравнением первой степени, пересечет кривую, заданную многочленом третьей степени, не более чем в трех точках с учетом кратности (рис. 5). Первая точка пересечения – особая, ее кратность $m_Q = 2$. Следовательно, еще

прямая пересечет кривую третьей степени не более чем в одной точке и эта точка (если она есть) – простая.

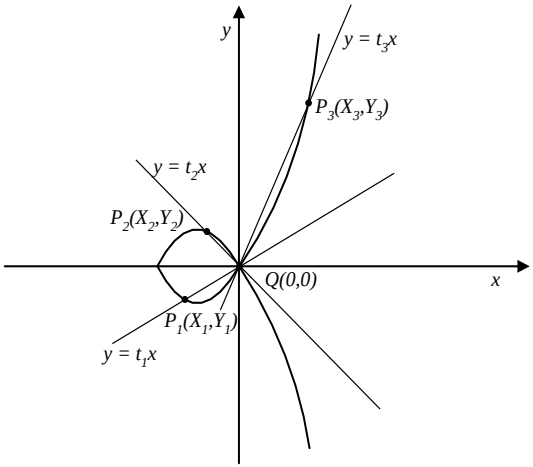

Рис. 5. Параметризация рациональной кривой третьей степени

Отсутствию третьей точки пересечения соответствует случай прохождения прямой параллельно оси 0*Y*. При этом значении углового коэффициента *t* прямая пересекается с кривой в бесконечно удаленной точке.

Выразим координаты точек рациональной кривой через рациональные функции от параметра *t*, т.е. две такие рациональные функции $\varphi(t)$ и $\psi(t)$, хотя бы одна из которых не постоянна, что $f(\varphi(t),\psi(t))=0$ тождественно относительно *t*. Когда *t* пробегает все значения *GF*(*q*), параметризация $x = \varphi(t)$, $y = \psi(t)$ дает все точки кривой (за исключением, возможно, конечного их числа).

Рассмотрим плоскую рациональную кривую $f(x, y) = 0$, заданную множеством решений уравнения (5) над $GF(2^m)$. Проведем через особую точку $Q(0, 0)$ секущую, заданную уравнением $y = tx$, где *t* – угловой коэффициент секущей. По утверждению 3 секущая пересечет кривую (5) еще в одной точке. Подставив уравнение секущей в (5), получим координаты искомой точки пересечения секущей с кривой:

$$X = t^2 + t + 1; \qquad (9)$$

$$Y = tX = t^3 + t^2 + t.$$

Таким образом, когда t пробегает все значения $GF(2^m)$, параметризация $x = \varphi(t)$, $y = \psi(t)$ дает все точки кривой (за исключением, возможно, конечного их числа).

Утверждение 4. Групповая операция сложения точек рациональной кривой третьей степени, заданной уравнением (5), в параметрическом виде тождественна выражению

$$t_3 = \frac{t_1 t_2 + 1}{t_1 + t_2 + 1}, \tag{10}$$

где t_1, t_2 и t_3 – локальные параметры точек $P_1(X_1, Y_1)$, $P_2(X_2, Y_2)$ и $P_3(X_3, Y_3)$ соответственно.

Доказательство. Воспользуемся выражениями (6) и (9). Подставим координаты точек $P_1(X_1, Y_1)$ и $P_2(X_2, Y_2)$ в параметрическом виде в выражение, задающее групповую операцию сложения точек. Получим:

$$X_3 = X_1 + X_2 + a^2 + a + 1 = t_1 + t_1^2 + 1 + t_2 + t_2^2 + 1 + \left(\frac{t_1 + t_1^2 + t_1^3 + t_2 + t_2^2 + t_2^3}{t_1 + t_1^2 + 1 + t_2 + t_2^2 + 1} \right)^2 +$$

$$+ \frac{t_1 + t_1^2 + t_1^3 + t_2 + t_2^2 + t_2^3}{t_1 + t_1^2 + 1 + t_2 + t_2^2 + 1} + 1 = \left(\frac{t_1 + t_1^2 + t_1^3 + t_2 + t_2^2 + t_2^3}{t_1 + t_1^2 + 1 + t_2 + t_2^2 + 1} + t_1 + t_2 \right)^2 +$$

$$+ \left(\frac{t_1 + t_1^2 + t_1^3 + t_2 + t_2^2 + t_2^3}{t_1 + t_1^2 + 1 + t_2 + t_2^2 + 1} + t_1 + t_2 \right) + 1 = t_3^2 + t_3 + 1.$$

$$Y_3 = aX_3 + b = \left(\frac{t_1 + t_1^2 + t_1^3 + t_2 + t_2^2 + t_2^3}{t_1 + t_1^2 + 1 + t_2 + t_2^2 + 1} \right) \left(\frac{t_1 + t_1^2 + t_1^3 + t_2 + t_2^2 + t_2^3}{t_1 + t_1^2 + 1 + t_2 + t_2^2 + 1} + t_1 + t_2 \right)^2 +$$

$$+ \left(\frac{t_1 + t_1^2 + t_1^3 + t_2 + t_2^2 + t_2^3}{t_1 + t_1^2 + 1 + t_2 + t_2^2 + 1} \right) \left(\frac{t_1 + t_1^2 + t_1^3 + t_2 + t_2^2 + t_2^3}{t_1 + t_1^2 + 1 + t_2 + t_2^2 + 1} + t_1 + t_2 \right) + \left(\frac{t_1 + t_1^2 + t_1^3 + t_2 + t_2^2 + t_2^3}{t_1 + t_1^2 + 1 + t_2 + t_2^2 + 1} \right) +$$

$$+ \left(\frac{t_1 + t_1^2 + t_1^3 + t_2 + t_2^2 + t_2^3}{t_1 + t_1^2 + 1 + t_2 + t_2^2 + 1} \right) \left(t_1 + t_1^2 + 1 \right) + \left(t_1 + t_1^2 + t_1^3 \right) =$$

$$= \left(\frac{t_1 + t_1^2 + t_1^3 + t_2 + t_2^2 + t_2^3}{t_1 + t_1^2 + 1 + t_2 + t_2^2 + 1} + t_1 + t_2 \right)^3 + \left(\frac{t_1 + t_1^2 + t_1^3 + t_2 + t_2^2 + t_2^3}{t_1 + t_1^2 + 1 + t_2 + t_2^2 + 1} + t_1 + t_2 \right)^2 +$$

$$+ \left(\frac{t_1 + t_1^2 + t_1^3 + t_2 + t_2^2 + t_2^3}{t_1 + t_1^2 + 1 + t_2 + t_2^2 + 1} + t_1 + t_2 \right) = t_3^3 + t_3^2 + t_3.$$

Откуда имеем:

$$t_3 = \frac{t_1 + t_1^2 + t_1^3 + t_2 + t_2^2 + t_2^3}{t_1 + t_1^2 + 1 + t_2 + t_2^2 + 1} + t_1 + t_2 = \frac{t_1^3 + t_2^3}{t_1 + t_1^2 + 1 + t_2 + t_2^2 + 1} + t_1 + t_2 + 1 =$$

$$= \frac{(t_1 + t_2)^3 + t_1 t_2 (t_1 + t_2)}{(t_1 + t_2)(t_1 + t_2 + 1)} + t_1 + t_2 + 1 = \frac{t_1 t_2 + 1}{t_1 + t_2 + 1}.$$

Утверждение 5. Групповая операция удвоения точек рациональной кривой третьей степени, заданной уравнением (5), в параметрическом виде тождественна выражению

$$t_3 = t_1^2, \tag{11}$$

где $t_1 = t_2$ и t_3 – локальные параметры точек $P_1(X_1, Y_1) = P_2(X_2, Y_2)$ и $P_3(X_3, Y_3)$ соответственно.

Доказательство. Воспользуемся выражениями (8) и (9). Подставим координаты точек $P_1(X_1, Y_1) = P_2(X_2, Y_2)$ в параметрическом виде в выражение, задающее групповую операцию удвоения точек. Получим:

$$X_3 = \frac{b^2}{x_1^2} = \left(t_1^2 + t_1 + 1\right)^2 = t_1^4 + t_1^2 + 1 = t_3^2 + t_3 + 1;$$

$$Y_3 = aX_1 + b = \left(t_1^2 + t_1 + 1\right)^3 + \left(t_1^2 + t_1 + 1\right)^2 + t_1^3 + t_1^2 + t_1 = t_1^6 + t_1^4 + t_1^2 = t_3^3 + t_3^2 + t_3.$$

Откуда имеем

$$t_3 = t_1^2.$$

Результат последнего утверждения показывает, что групповые операции сложения и удвоения точек рациональной кривой можно существенно упростить и снизить затратность реализации криптографических преобразований на рациональной кривой третьей степени. Проанализируем сложность выполнения групповых операций по выражениям (2 – 4) и (10 – 11), соответственно. На рис. 6 – 7. представлены диаграммы сложности операций сложения и удвоения точек ЕС: темным цветом – по формулам (2 – 4), светлым – по (10 – 11).

Выводы. В результате проведенных исследований теоретически обоснованы быстрые преобразования в группе точек ЕС, которые позволяют существенно снизить сложность сложения и удвоения элементов группы. Перспективным направлением является исследование стойкости криптосистем с использованием предложенных быстрых преобразований.

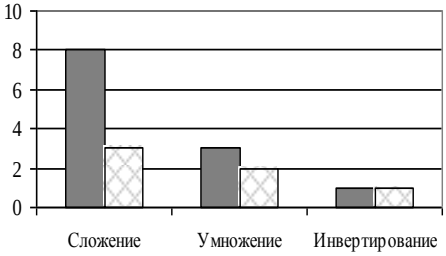

Рис. 6. Сложность сложения точек

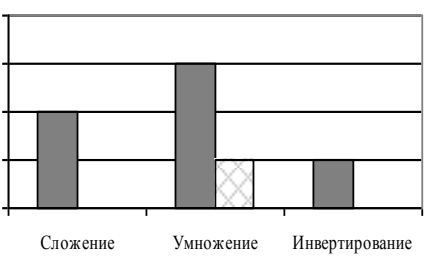

Рис. 7. Сложность удвоения точек

Список литературы. 1. *D. Johnson, A. Menezes, S. Vanstone.* The elliptic curve digital signature algorithm (ECDSA). – Certicom Research. – 2001. **2.** *ДСТУ 4145-2002.* Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевірка. **3.** *IEEE P1363-2000.* Standard Specifications for Public Key Cryptography. **4.** *Болотов А.А. и др.* Алгоритмические основы эллиптической криптографии. – М.: МЭИ, 2000. – 100 с. **5.** *Соловьев Ю.П.* Рациональные точки на эллиптических кривых // Соросовский образовательный журнал. – 1997. – №10. – С. 138 – 143. **6.** *Саломаа А.* Криптография с открытым ключом: Пер. с англ. – М.: Мир, 1995. – 318 с.

Поступила в редакцию 05.10.2004