

## Два подхода к логарифмированию на эллиптической кривой

В основу безопасности криптосистем с открытым ключом на эллиптической кривой  $E(\mathbb{F}_p)$  положена задача дискретного логарифмирования в группе точек простого порядка  $r$ . Наилучший известный способ логарифмирования — алгоритм Полларда для орбит автоморфизмов — имеет сложность  $S = O(\sqrt{r})$ . Предлагаются подходы к логарифмированию, основанные на вложении кривой  $E(\mathbb{F}_p)$  в мультиквадратичное расширение поля  $\mathbb{Q}$  рациональных чисел. Показано, что ранг эллиптической кривой растет экспоненциально от числа присоединенных элементов  $\sqrt{D_i}$ . Первый подход использует числовое поле  $K$ , для которого ранг кривой  $E(K)$  имеет порядок  $O(\ln r)$ . Задача логарифмирования сводится к вычислению ранга кривой, вычислению образующих группы Морделла–Вейля и поднятию точек. Второй подход использует числовое поле, для которого ранг кривой велик. Задача дискретного логарифмирования на эллиптической кривой указанными методами предположительно имеет субэкспоненциальную сложность.

Rostovtsev A.G., Makhovenko E.B., SPbSTU

## Two approaches to computing elliptic curve discrete logarithms

Security of elliptic curve public key cryptosystems depends on discrete logarithm problem complexity. Let  $E(\mathbb{F}_p)$  be elliptic curve with cyclic subgroup of large prime order  $r$ . The best known method of computing discrete logarithms is Pollard's algorithm for automorphism orbits with complexity  $S = O(\sqrt{r})$ . Two approaches to computing discrete logarithms, based on embedding elliptic curve  $E(\mathbb{F}_p)$  into multiquadratic extension of the field  $\mathbb{Q}$ . It is shown that elliptic curve rank grows as exponent of number of joint elements  $\sqrt{D_i}$ . First method uses such number field  $K$  that the rank of elliptic curve  $E(K)$  is approximately  $O(\ln r)$ . Discrete logarithm problem is reduced to computing Mordell–Weil group and point lifting under the condition that height of lifted point is relatively small. The second one uses number field such that elliptic curve rank is large. It is conjectured that there exists algorithm for computing discrete logarithms with subexponential complexity.

### 1. Эллиптическая кривая и задача логарифмирования

Эллиптическая кривая  $E(\mathbb{F}_p)$  над простым конечным полем  $\mathbb{F}_p$ ,  $p > 3$ , задается уравнением

$$Y^2Z = X^3 + AXZ^2 + BZ^3, \quad (1)$$

где многочлен в правой части не имеет кратных корней. Точки  $(X, Y, Z)$ , где  $X^2 + Y^2 + Z^2 \neq 0$  и  $(X, Y, Z) = (uX, uY, uZ)$  для  $u \in \mathbb{F}_p^*$ , образуют абелеву группу с нулевым элементом  $P_\infty = (0, 1, 0)$ . В аффинной плоскости  $Z \neq 0$ , и уравнение (1) можно записать в виде  $y^2 = x^3 + Ax + B$ , где  $x = \frac{X}{Z}$ ,  $y = \frac{Y}{Z}$ , при этом  $-(x, y) = (x, -y)$ . Закон сложения  $P_3 = P_1 + P_2$ , где  $P_i = (x_i, y_i)$  задается формулами

$$x_3 = \lambda^2 - x_1 - x_2, y_3 = \lambda(x_1 - x_3) - y_1$$

где  $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$  при  $P_1 \neq P_2$  и  $\lambda = \frac{3x_1^2 + A}{2y_1}$  при  $P_1 = P_2$ .

Согласно теореме Хассе [1] выполняется неравенство  $|\#E(\mathbb{F}_p) - p - 1| < 2\sqrt{p}$ . Эллиптическая кривая обладает изоморфизмом  $(x, y, A, B) \rightarrow (u^2x, u^3y, u^4A, u^6B)$ . Инвариант эллиптической кривой равен  $j = 1728 \frac{4A^3}{4A^3 + 27B^2}$ . Эллиптические кривые изоморфны тогда и только тогда, когда равны их  $j$ -инварианты [1].

Эллиптические кривые обладают автоморфизмами. Если  $j = 0$  (то есть  $A = 0$ ) и  $p \equiv 1 \pmod{6}$ , то группа автоморфизмов определяется отображением  $(x, y) \rightarrow (\frac{-1 + \sqrt{-3}}{2}x, -y)$  и имеет порядок 6. Этому автоморфизму соответствует комплексное умножение на  $\frac{1 + \sqrt{-3}}{2}$ . Орбита точки  $(x, y)$  относительно группы автоморфизмов задается значением  $x^3$  или  $y^2$ . Если  $j = 1728$  (то есть  $B = 0$ ) и  $p \equiv 1 \pmod{4}$ , то группа автоморфизмов определяется отображением  $(x, y) \rightarrow (-x, \sqrt{-1}y)$  и имеет порядок 4. Этому автоморфизму соответствует комплексное умножение на  $\sqrt{-1}$ . Орбита точки  $(x, y)$  относительно группы автоморфизмов задается значением  $x^2 - A$ . В остальных случаях группа автоморфизмов имеет порядок 2 и определяется отображением  $(x, y) \rightarrow (x, -y)$ , при этом орбита точки  $(x, y)$  относительно группы автоморфизмов задается значением  $x$ .

На эллиптической кривой, заданной уравнением  $f(x, y) = 0$  определено координатное кольцо  $\mathbb{F}_p[E] = \mathbb{F}_p[x, y]/(f(x, y))$  и поле рациональных функций  $\mathbb{F}_p(E)$  как поле частных этого кольца.

Эллиптические кривые широко используются для построения криптосистем с открытым ключом [2]. Это объясняется следующими причинами.

1. Эллиптические кривые обеспечивают максимально возможную для криптосистем с открытым ключом стойкость на один бит размера задачи.

2. Эллиптические кривые позволяют реализовать широкий спектр криптографических защитных функций (шифрование с открытым ключом, аутентификацию на основе диалоговых и бездиалоговых доказательств с нулевым разглашением и т.п. [3]). Эллиптические кривые положены в основу российского (ГОСТ Р34.10–2001) и американского (ECDSS) стандартов подписи.

3. Эллиптические кривые обеспечивают практически нулевую скорость падения стойкости во времени, что позволяет сохранять размер задачи. Для сравнения: в криптосистемах, основанных на логарифмировании в конечном поле или разложении чисел на множители размер задачи нужно удваивать примерно каждые 5 лет.

4. Криптосистемы с открытым ключом на эллиптических кривых позволяют выполнять независимую смену персональных ключей в информацион-

ной системе. В криптосистемах, основанных на логарифмировании в конечном поле, это не так. Наилучший метод логарифмирования (решето числового поля) предполагает создание базы данных для данной характеристики поля, с помощью которой логарифмы быстро вычисляются. Поэтому смена персонального ключа практически не позволяет увеличить срок его службы, необходимо менять характеристику поля и все персональные ключи [3].

Безопасность криптосистем основана на задаче дискретного логарифмирования в группе точек простого порядка  $r$ : для заданных точек  $P, Q$  найти такой показатель  $l$ , что  $P = lQ$ . Оценку сложности  $S$  этой задачи в общем случае принято определять алгоритмом Полларда [4]:  $S = O(\sqrt{r})$ , который не может быть улучшен за счет увеличения объема памяти и не допускает эффективного распараллеливания.

Алгоритм Полларда можно применять не к точкам, а к их орбитам относительно группы автоморфизмов. При этом задача логарифмирования разбивается на две подзадачи: вычисление логарифма для орбит и уточнение логарифма внутри орбиты. Чем больше орбита, тем сильнее снижается сложность. По-видимому, этим можно объяснить то обстоятельство, что в отечественном стандарте подписи не разрешаются эллиптические кривые с  $j = 0, 1728$ .

Частные методы логарифмирования на эллиптических кривых основаны на специфических свойствах группы  $E(\mathbb{F}_p)$ . Как показал И.А. Семаев, кривую  $E(\mathbb{F}_p)$  можно вложить в группу  $\mathbb{F}_q^*$  расширенного поля из  $q = p^n$  элементов, где  $q - 1 \equiv 0 \pmod{r}$ , используя спаривание Вейля (при  $r \neq p$ ), или в аддитивную группу поля  $\mathbb{F}_p$  методом логарифмической производной (при  $r = p$ ) [5].

В стандарте ГОСТ Р 34.10–2001 числа  $p$  и  $r$  имеют длину 256 и 254–256 бит соответственно. Кроме того, для противостояния частным методам логарифмирования необходимо выполнение условий  $p \neq r$  и  $p^k \neq 1 \pmod{r}$  для  $k = 1, \dots, 31$ .

Между эллиптическими кривыми  $E_1(\mathbb{F}_p)$  и  $E_2(\mathbb{F}_p)$  может существовать изогения — пара функций из  $\mathbb{F}_p(E)$ , отображающая  $E_1$  в  $E_2$ , причем точка  $P_\infty \in E_1(\mathbb{F}_p)$  переходит в точку  $P_\infty \in E_2(\mathbb{F}_p)$ . Изогении задают гомоморфизм эллиптических кривых как абелевых групп. Ядро изогении степени  $l$  состоит из точек кручения порядка  $l$ , образующих циклическую группу. Всего существует не более чем  $l + 1$  изогений степени  $l$ . Если  $r \neq l$  и число точек не делится на  $r^2$ , то изогения задает изоморфизм групп порядка  $r$ . Изогении малых степеней эффективно вычислимы [6], а  $j$ -инварианты эллиптических кривых, изогенных данной кривой для изогении степени  $l$ , могут быть найдены как корни модулярного полинома. Согласно теореме Тейта [7], эллиптические кривые изогенны тогда и только тогда, когда они имеют одинаковое число точек над полем  $\mathbb{F}_p$ .

Существует много эллиптических кривых, которые удовлетворяют требованиям ГОСТ Р 34.10–2001, но являются изогенными кривым с инварианта-

ми  $j = 0, j = 1728$ , запрещенными стандартом. Для вычисления логарифма на эллиптической кривой, изогенной кривой с инвариантом  $j = 0$  или  $j = 1728$ , можно с помощью соответствующей изогении перейти к кривой с неполным уравнением и дальше вычислять логарифм на этой кривой. Поэтому применительно к задаче логарифмирования на эллиптической кривой изогенные кривые одинаковы.

Эллиптическую кривую  $E(\mathbb{F}_p)$  можно вложить в кривую  $E(\mathbb{Q})$  над полем  $\mathbb{Q}$  рациональных чисел. Эллиптическая кривая  $E(\mathbb{Q})$  состоит из группы кручения и конечно порожденной свободной группы (группы Морделла–Вейля). Число образующих группы Морделла–Вейля называется рангом кривой  $E(\mathbb{Q})$  и обозначается  $\text{rk}(E(\mathbb{Q}))$ .

Высота  $h_x$  точки  $P$  эллиптической кривой определяется как функция  $h_x: E(\mathbb{Q}) \rightarrow \mathbb{R}$ ,

$$h_x(P) = \begin{cases} \log(\max(|u|, |v|)), & \text{если } P \neq P_\infty, \\ 0, & \text{если } P = P_\infty, \end{cases}$$

где  $u$  и  $v$  — числитель и знаменатель несократимой дроби, представляющей  $x$ -координату точки  $P$ . Аналогично можно определить высоту для эллиптической кривой над произвольным числовым полем  $K$ . При этом вместо абсолютной величины можно использовать норму целого алгебраического числа.

На кривой  $E(\mathbb{Q})$  определена каноническая высота  $\hat{h}: E(\mathbb{Q}) \rightarrow \mathbb{R}$ :

$$\hat{h}(P) = \lim_{N \rightarrow \infty} \frac{h(2^N P)}{4^N}.$$

Точки кручения и бесконечно удаленная точка имеют нулевую каноническую высоту. Для всех остальных точек каноническая высота является ненулевым вещественным числом. Функция канонической высоты обладает следующими свойствами:

$$\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q); \quad \hat{h}(mP) = m^2\hat{h}(P). \quad (2)$$

Отсюда следует, что на эллиптической кривой  $E(\mathbb{Q})$  задача вычисления индекса в группе Морделла–Вейля решается легко.

В 1999 г. Дж. Сильверман в статье [8] предложил для решения задачи логарифмирования на эллиптической кривой  $E(\mathbb{F}_p)$  использовать метод Пойа (метод обобщения и редукции). Для этого нужно вложить кривую  $E(\mathbb{F}_p)$  в кривую  $E(\mathbb{Q})$  над полем рациональных чисел, вычислить образующие группы Морделла–Вейля, поднять несколько линейных комбинаций точек  $P$  и  $Q$  так, чтобы в формуле (1) сравнение перешло в равенство, и найти их индексы в группе Морделла–Вейля. После этого вычислить логарифм  $l$  по модулю  $r$  не составляет труда.

Для поднятия точек можно использовать алгоритм Сильвермана Xedni calculus или решать систему из двух уравнений Пелля [9].

Если ранг эллиптической кривой  $E(\mathbb{Q})$  мал, то почти все из  $r$  точек кривой имеют большую каноническую высоту, что обуславливает большую емкостную сложность задачи. Таким образом, независимо от сложности задач поднятия и вычисления образующих группы Морделла–Вейля метод Сильвермана может быть практичным лишь в том случае, когда ранг кривой  $E(\mathbb{Q})$  достаточно велик и составляет десятки или сотни.

Однако в действительности ранг кривой  $E(\mathbb{Q})$  обычно мал и не превышает 5 (обычно для эллиптических кривых с небольшими коэффициентами ранг равен 0, 1 или 2). «Рекордные» ранги эллиптических кривых над полем  $\mathbb{Q}$  заключены в интервале 20–25 и получены специальным конструированием кривых. Для таких рангов каноническая высота поднятой точки оказывается настолько большой, что сложность вычисления логарифма указанным методом сравнима со сложностью алгоритма Полларда (даже если задача поднятия оказывается несложной).

Таким образом, предложенный Дж. Сильверманом метод логарифмирования, основанный на поднятии точки в поле  $\mathbb{Q}$ , непрактичен. Для снижения сложности метода необходимо существенно увеличить ранг эллиптической кривой так, чтобы он был сравнимым  $\log_2 r$ .

## 2. Эллиптические кривые над мультикватратичными расширениями

Пусть  $k$  — поле характеристики 0,  $D \in k$ ,  $\sqrt{D} \notin k$ ,  $k_1 = k[\sqrt{D}]$  и  $E(k)$ ,  $E(k_1)$  — эллиптические кривые с одним и тем же уравнением (1), заданные над полями  $k$  и  $k_1$  соответственно. Будем считать, что кривая  $E(k_1)$  свободна от кручения, в противном случае вместо  $E(k_1)$  можно рассматривать факторгруппу по подгруппе кручения. Поскольку  $k_1 \supset k$ , группа  $E(k)$  является нормальной подгруппой группы  $E(k_1)$ . Пусть  $\tilde{E}(k_1)$  — подгруппа группы  $E(k_1)$ , порожденная точками,  $x$ -координаты которых лежат в  $k$ .

**Теорема 1.** На кривой  $E(k_1): y^2 = x^3 + Ax + B$  с коэффициентами  $A, B \in k$ , рассматриваемой над полем  $k_1$ , существует точка  $(x, y\sqrt{D})$ , где  $x, y \in k$ , тогда и только тогда, когда на кривой

$$E_D(k): v^2 = u^3 + AD^{-2}u + BD^{-3} \quad (3)$$

существует точка  $(uD, vD)$ . Подгруппа  $\hat{E}(k_1)$ , порожденная точками  $(x, y\sqrt{D})$  кривой  $E(k_1)$ , изоморфна группе  $E_D(k)$ .

Доказательство. На кривой  $E(k_1)$  существует точка  $(x, y\sqrt{D})$  тогда и только тогда, когда на кривой  $E_1(k): Dy^2 = x^3 + Ax + B$  существует точка  $(x, y)$ .

Эллиптическая кривая  $E_1(k)$  изоморфна над полем  $k$  кривой  $y^2 = x^3 + A'x + B'$ , где  $x = x'D$ ,  $y = y'D$ ,  $A = A'D^2$ ,  $B = B'D^3$ , которая совпадает с кривой  $E_D$ . Гомоморфизм  $\hat{E}(k_1) \rightarrow E_D(k)$  (как и обратный к нему) обладает ядром  $\{P_\infty\}$  и является изоморфизмом. ■

**Следствие.** Имеет место изоморфизм групп  $\tilde{E}(k_1) \cong E(k) \oplus E_D(k)$ , при этом выполняется равенство  $\text{rk}(\tilde{E}(k_1)) = \text{rk}(E(k)) + \text{rk}(E_D(k))$ .

Аналогично можно показать, что для поля  $k_2 = k[\sqrt{D_1}, \sqrt{D_2}]$  имеет место изоморфизм групп  $\tilde{E}(k_2) \cong E(k) \oplus E_{D_1}(k) \oplus E_{D_2}(k) \oplus E_{D_1 D_2}(k)$ . По индукции рассуждения продолжаются на произвольное число присоединяемых элементов  $\sqrt{D_i}$ .

**Теорема 2.** Пусть  $G$  — конечно порожденная абелева группа без кручения и  $H$  — ее подгруппа. Ранги групп  $G$  и  $H$  равны тогда и только тогда, когда порядок любого элемента факторгруппы  $G/H$  конечен.

Доказательство. Пусть ранги групп  $G$  и  $H$  равны и  $\mathbf{g} = (g_1, \dots, g_n)$ ,  $\mathbf{h} = (h_1, \dots, h_n)$  — множества образующих для групп  $G$  и  $H$  соответственно. Тогда существует такая невырожденная матрица  $M = (a_{ij})$  над кольцом  $\mathbb{Z}$  целых чисел, что  $\mathbf{h} = M\mathbf{g}$ . Матрицу  $M$  над кольцом  $\mathbb{Z}$  можно привести к диагональному виду  $M = (m_{ii})$ , где  $m_{ii} \neq 0$ ,  $m_{ij} = 0$  для  $i \neq j$ . Пусть  $m$  — наименьшее общее кратное чисел  $m_{ii}$ . Любой элемент вида  $c_1 g_1 + \dots + c_n g_n \in G$ , где  $c_i \in \mathbb{Z}$ , после умножения на  $m$  будет лежать в группе  $H$ .

Обратно, пусть порядок любого элемента факторгруппы  $G/H$  конечен и  $\mathbf{g} = (g_1, \dots, g_n)$ ,  $\mathbf{h} = (h_1, \dots, h_l)$  — множества образующих для групп  $G$  и  $H$  соответственно. Предположим, что  $n > l$ . Тогда существует такая вырожденная матрица  $M = (a_{ij})$  над кольцом  $\mathbb{Z}$  целых чисел, что  $\mathbf{h} = M\mathbf{g}$ . Матрицу  $M$  над кольцом  $\mathbb{Z}$  можно привести к диагональному виду  $M = (m_{ii})$ , где  $m_{ii} \neq 0$ ,  $m_{ij} = 0$  для  $i \neq j$ . Тогда порядок элемента  $m_{ln}$  в группе  $G/H$  не может быть конечным. ■

Пусть  $L$  — поле, порожденное над полем  $\mathbb{Q}$  рациональных чисел элементами  $\sqrt{D}$ , где  $D$  пробегает все множество  $\mathbb{Z}$  целых чисел,  $E(L)$  — эллиптическая кривая с целыми коэффициентами, рассматриваемая над полем  $L$ , и  $\tilde{E}(L)$  — группа точек, порожденная точками вида  $(x, y\sqrt{d})$ , где  $x, y \in \mathbb{Q}$  и  $d$  — целое число. И.А. Семаев доказал, что порядок любой точки  $(x_1, y_1) \in E(L)$  в факторгруппе  $E(L)/\tilde{E}(L)$  конечен [10], причем это доказательство справедливо и для конечных расширений. Поэтому согласно теореме 2 ранги свободных групп  $E(L)$  и  $\tilde{E}(L)$  равны.

Пусть  $K = \mathbb{Q}[\sqrt{D_1}, \dots, \sqrt{D_n}]$  — мультикватратичное расширение поля  $\mathbb{Q}$  и  $E(K)$  — эллиптическая кривая с целыми коэффициентами. Ранг группы  $E(K)$  равен рангу группы  $\tilde{E}(K)$ . Согласно теореме 1 и следствию из нее вычисление ранга группы  $\tilde{E}(K)$  сводится к вычислению рангов групп эллиптических кривых  $E_{\prod D_i}(\mathbb{Q})$ , заданных уравнениями (3) над полем  $\mathbb{Q}$  рациональных чисел. Отметим, что при увеличении числа  $n$  ранг группы  $\tilde{E}(K)$  имеет тенденцию к возрастанию и стремится к бесконечности [11].

Сумма точек  $(x_1, y_1\sqrt{D_1}) + (x_2, y_2\sqrt{D_2})$  имеет следующий вид:  $x$ -координата суммы равна  $x = \frac{y_2^2 D_2 + y_1^2 D_1 - 2y_1 y_2 \sqrt{D_1 D_2}}{(x_2 - x_1)^2} - x_1 - x_2$  и лежит в поле  $\mathbb{Q}[\sqrt{D_1 D_2}]$  степени 2 над  $\mathbb{Q}$ ;  $y$ -координата суммы лежит в поле  $\mathbb{Q}[\sqrt{D_1}, \sqrt{D_2}]$  степени 4 над  $\mathbb{Q}$ . Аналогично можно показать, что точки  $(x_1, y_1\sqrt{D_1})$ ,  $(x_2, y_2\sqrt{D_2})$ ,  $(x_3, y_3\sqrt{D_3})$  порождают группу, у каждого элемента которой  $x$ -координата лежит в поле степени 4 над  $\mathbb{Q}$ , а  $y$ -координата лежит в поле степени 8 над  $\mathbb{Q}$ .

Ранг эллиптической кривой, заданной над полем  $\mathbb{Q}$ , можно вычислить на основе гипотезы Берча и Свиннертона-Дайера как кратность нуля вычислимой  $L$ -функции эллиптической кривой.

Ранг и множество образующих свободной группы  $E(K)$  можно также найти методом Ю.И. Манина, основанного на минимизации канонической высоты, или методом 2-спуска [10]. Похожий способ вычисления множества образующих свободной группы  $E(K)$  описан в работе Кремоны [12].

### 3. Логарифмирование через поднятие точки в числовое поле

В работе [13] был предложен метод логарифмирования, основанный на поднятии точек из конечного поля в числовое поле. Наиболее удобным представляется мультикватратичное расширение  $K = \mathbb{Q}[\sqrt{D_1}, \dots, \sqrt{D_n}]$  поля  $\mathbb{Q}$ , где

$|D_i|$  — гладкие числа (включая  $-1$ ) такие, что  $\left(\frac{D_i}{p}\right) = 1$ . Например, если

$\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = -1$ , то можно положить  $D = 6$  или  $D = 10$ . Расширение  $K$

является нормальным и абелевым над полем  $\mathbb{Q}$  и представляется естественным для построения алгоритмов логарифмирования на эллиптической кривой над простым конечным полем.

Отображение  $E(K) \rightarrow E(\mathbb{F}_p)$ , вычисляемое редукцией координат и элементов  $\sqrt{D_i}$  по модулю  $p$ , является гомоморфизмом групп. Факторгруппа  $E(\mathbb{F}_p)$  по подгруппе порядка  $r$  изоморфна группе кручения кривой  $E(K)$ , если эта

группа кручения не содержит элементов порядка  $r$ . Последнее условие не сложно проверить, так как согласно теореме Лутца–Нагеля координаты точек кручения являются целыми в поле  $K$ , а дискриминант  $4A^3 + 27B^2$  эллиптической кривой должен быть квадратом в  $K$  и делиться на квадрат  $y$ -координаты точки кручения [11]. Поскольку группа кручения кривой  $E(K)$  невелика, вероятность того, что она содержит точки большого порядка  $r$ , мала.

Образующие группы Морделла–Вейля могут быть найдены методом спуска [11]. В частности, для группы  $E(K)$   $x$ -координата образующей точки не может быть квадратом в  $K$ .

Кольцо эндоморфизмов подгруппы порядка  $r$  кривой  $E(\mathbb{F}_p)$  изоморфно кольцу классов вычетов  $\mathbb{Z}/r\mathbb{Z}$ , а кольцо эндоморфизмов группы Морделла–Вейля кривой  $E(K)$  (рассматриваемой как свободная абелева группа) представляет собой кольцо квадратных матриц над кольцом  $\mathbb{Z}$ , размер которых равен рангу кривой. Поэтому для вычисления логарифма необходимо поднять в  $E(K)$  несколько точек вида  $aP + bQ$  так, чтобы их векторные индексы были линейно зависимы. При этом можно поднимать точки не исходной кривой  $E(\mathbb{F}_p)$ , а произвольной кривой, которая изоморфна или изогенна исходной.

Возможны два варианта вычисления логарифмов. В первом случае рассматривается такое поле  $K$ , что ранг  $\text{rk}(\tilde{E}(K))$  составляет несколько десятков (оптимальное значение ранга должно обеспечивать минимум сложности). Для этого можно использовать изогении и изоморфизмы кривых над полем  $\mathbb{F}_p$ . Метод включает в себя следующие шаги.

1. Вычисление ранга свободной группы  $\tilde{E}(K)$ .
2. Вычисление образующих группы  $\tilde{E}(K)$ .
3. Поднятие  $\text{rk}(\tilde{E}(K)) + 1$  точек вида  $aP + bQ$  в поле  $K$  методом Сильвермана [8].
4. Вычисление индексов поднятых точек путем минимизации канонической высоты.
5. Выражение  $P$  через  $Q$  методом гауссова исключения и вычисление логарифма по модулю  $r$ .

Таким образом, задача логарифмирования на эллиптической кривой сводится к задачам вычисления ранга кривой, вычисления образующих группы Морделла–Вейля и поднятия точек. При этом число  $n$  присоединяемых элементов  $\sqrt{D_i}$ , где  $D_i \in \mathbb{Z}$ , желательно выбирать небольшим (это всего лишь инструмент для увеличения ранга).

Второй метод включает в себя следующие шаги.

1. Вычисление ранга свободной группы  $\tilde{E}(K)$ .
2. Вычисление образующих  $\{R_i\}$  группы  $\tilde{E}(K)$ .

3. Подбор  $\text{rk}(\tilde{E}(K)) + 1$  точек вида  $a_iP + b_iQ = (x_i, y_i) \in E(\mathbb{F}_p)$ , каждая из которых может быть представлена в виде суммы  $\sum_i a_iR_i$  на кривой  $E(K)$ .
4. Вычисление индексов подобранных точек путем минимизации канонической высоты.
5. Выражение  $P$  через  $Q$  методом гауссова исключения и вычисление логарифма по модулю  $r$ .

Этот вариант в отличие от предыдущего не требует поднятия точек. Кроме того, здесь оптимальное расширение должно обеспечивать возможно меньший положительный ранг эллиптической кривой и большое число дискриминантов  $D_i$ , присоединяемых к  $\mathbb{Q}$ , — это облегчит шаги 3, 4, 5.

Вероятность того, что свободная от квадратов часть числа  $x_i^3 + Ax_i + B$  будет гладкой относительно базы  $\{D_i\}$ , оценивается субэкспонентой  $\exp(-c\sqrt{\ln p \ln \ln p})$ , где  $c$  — вещественное число, близкое к 1 (см., например, методику работы [3]). Тогда сложность подбора одиночной точки на шаге 3 не превышает субэкспоненциальной. Выберем ранг эллиптической кривой  $\tilde{E}(K)$ , который тоже оценивается субэкспонентой (это можно сделать выбором соответствующего расширения  $K/\mathbb{Q}$ ). Тогда сложность шагов 1, 2, 4, 5 тоже будет субэкспоненциальной. Поэтому можно предположить, что при любом выборе кривой существует алгоритм логарифмирования на эллиптической кривой, обладающий субэкспоненциальной сложностью.

Таким образом, задача вычисления логарифма на эллиптической кривой свелась к задаче вычисления группы Морделла–Вейля и задаче поднятия точки. Поскольку образующие группы Морделла–Вейля имеют малую каноническую высоту, их вычисление не представляется трудным.

Можно предположить, что рассмотренные методы логарифмирования на эллиптической кривой позволят снизить общепринятую оценку сложности. Их можно использовать и для решения задачи логарифмирования в конечном поле  $\mathbb{F}_p$ , которая является частным случаем задачи логарифмирования на эллиптической кривой  $E(\mathbb{F}_p)$  с числом точек  $p - 1$  (сводимость осуществляется спариванием Вейля).

### Библиографический список

1. Husemöller D. Elliptic curves. Springer–Verlag, 1987.
2. Koblitz N. Elliptic curve cryptosystems // Mathematics of Computation. 1987. Vol. 48. No. 177. P. 203–209.
3. Ростовцев А.Г., Маховенко Е.Б. Введение в криптографию с открытым ключом. СПб.: Мир и Семья, Интерлайн, 2001.

4. Pollard J. Monte Carlo methods for index computation (mod  $p$ ) // Mathematics of Computation. 1978. Vol. 32. P. 918–924.
5. Semaev I.A. Evaluation of discrete logarithms in a group of  $p$ -torsion points of an elliptic curve in characteristic  $p$  // Mathematics of Computation. 1998. Vol. 67. P. 353–356.
6. Lercier R., Morain F. Algorithms for computing isogenies between elliptic curves // Computational perspectives on number theory. AMS/IP Studies on Advanced Mathematics. Vol. 7.
7. Galbraith S.D. Constructing isogenies between elliptic curves over finite fields // <http://citeseer.ist.psu.edu/galbraith99constructing>.
8. Silverman J.H. The Xedni calculus and the elliptic curve discrete logarithm problem. Designs, Codes and Cryptography. 2000. Vol. 20. P. 5–40.
9. Bennett M.A. Solving families of simultaneous Pell equations // Journal of Number Theory. 1997. Vol. 67. P. 246–251.
10. Semaev I.A. Elliptic curves points over the maximal multiquadratic extension of rational numbers // <http://www.wis.kuleuven.ac.be/algebra/artikels/semaev.htm>.
11. Zimmer H.C. Basic algorithms for elliptic curves // <http://www.rzuser.uni-heidelberg.de/~hb3/elleng.html>.
12. Cremona J.E. On the computation of Mordell–Weil and 2-Selmer groups of elliptic curves // [www.maths.nott.ac.uk/personal/jec/papers/filter.pdf](http://www.maths.nott.ac.uk/personal/jec/papers/filter.pdf).
13. Ростовцев А.Г. Логарифмирование через поднятие // Проблемы информационной безопасности. Компьютерные системы, СПб. 2000. № 2. С. 49–53.