

О выборе эллиптической кривой над простым полем для построения криптографических алгоритмов

1. Теоретические сведения

Эллиптические кривые над конечными полями — один из самых перспективных инструментов для построения криптографических алгоритмов [1]. Эллиптическая кривая E над простым полем \mathbf{F}_p , $p > 3$, задается уравнением в форме Вейерштрасса

$$E(\mathbf{F}_p): y^2 = x^3 + Ax + B, \text{ где } 4A^3 + 27B^2 \neq 0. \quad (1)$$

Решения этого уравнения, совместно с бесконечно удаленной точкой, задают множество точек кривой. Для числа точек N справедлива оценка, задаваемая теоремой Хассе: $|N - p| < 2\sqrt{p}$. На кривой (1) определен j -инвариант

$$j = 12^3 \frac{4A^3}{4A^3 + 27B^2}.$$

Для получения кривой с заданным j -инвариантом, отличным от 0 и 12^3 вместо (1) можно использовать следующее уравнение [8]:

$$y^2 = x^3 + 3kt^2x + 2kt^3. \quad (1a)$$

На множестве точек вводится структура абелевой группы с помощью закона сложения. Для сложения точек $P_1 = (x_1, y_1)$ и $P_2 = (x_2, y_2)$ через них проводят секущую, которая пересекает кривую в третьей точке P_3 с координатами $(x_3, -y_3)$. Тогда точка (x_3, y_3) , противоположная к точке P_3 , по определению является суммой точек P_1 и P_2 . Закон сложения описывается формулами

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

$$\lambda = \frac{3x_1^2 + A}{2y_1}, \text{ если } P_1 = P_2,$$

и

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \text{ если } P_1 \neq P_2.$$

Для модульного обращения может быть использован бинарный алгоритм Евклида [1] или проективная арифметика, исключая необходимость модульного деления при сложении или удвоении точек [2]. Эллиптическая кривая может быть параметризована над полем комплексных

чисел с помощью эллиптических функций, при этом неизоморфным эллиптическим кривым взаимно однозначно соответствует решетка периодов эллиптической функции.

В основу безопасности криптографических алгоритмов положена задача дискретного логарифмирования в группе точек: найти показатель l такой, что $P = lQ$ в циклической группе простого порядка r . Если порядок циклической группы составной, то сложность логарифмирования определяется максимальным простым делителем порядка группы.

С точки зрения теории сложности задача логарифмирования на кубической кривой является не менее сложной, чем задача дискретного логарифмирования в простом поле, так как вторая задача является частным случаем первой.

Для логарифмирования на любой эллиптической кривой может быть использован алгоритм Полларда [3] со сложностью $O(\sqrt{r})$ операций сложения точек. Кроме того, если существует небольшой показатель k такой, что $r \mid (p^k - 1)$, то для логарифмирования может быть использован метод, основанный на спаривании Вейля, предложенный практически одновременно И. Семаевым и зарубежными авторами [4]. В этом случае задача логарифмирования на кривой сводится к задаче дискретного логарифмирования в подгруппе мультипликативной группе поля из p^k элементов со сложностью $O(\exp(c\sqrt{\ln p^k (\ln \ln p^k)^2}))$ для небольшой константы c . Для того чтобы не происходило снижение сложности по сравнению с методом Полларда, на практике показатель k должен быть не менее $10 \div 20$. В случае $p = r$ задача логарифмирования на кривой решается легко с помощью алгоритма И. Семаева [5].

При правильном выборе кривой задача логарифмирования на кривой с простым порядком группы длиной 160 бит примерно соответствует сложности логарифмирования в мультипликативной группе простого поля длиной 1024 бита (однако стойкость системы RSA быстро падает — примерно в 30 раз за год).

Умножение точки на число (аналогичное возведению в степень в случае RSA) требует небольшого числа сложений. Например, для умножения точки на число длины 200 бит требуется в среднем 100 операций удвоения точки и 66 операций сложения точек. Для сравнения: возведение в степень с показателем длины 200 бит в среднем требует 300 операций умножения. Это сокращение числа операций достигается за счет использования комплексного умножения, что позволяет уменьшить вдвое эффективную длину показателя [6]. Кроме того, возможно снижение количества ненулевых цифр за счет перехода от двоичного к троичному представлению показателя с цифрами 0, 1, -1. Например, $011111 = 10000-1$ или $31 = 2^5 - 1$. Здесь пять единиц заменяются на две. В общем случае доля ненулевых цифр в таком представлении показателя равна $1/3$.

Для дополнительного ускорения вычислений можно представлять показатель не в двоичной, а в другой системе счисления. В этом случае для умножения точки Q на число k можно воспользоваться следующим методом. Для системы счисления с основанием 2^d сначала вычисляют $2Q, 3Q \dots, 2^d Q$ и записывают показатель $k = b_t 2^{td} + \dots + b_0$. Затем вычисляют рекурсивно для i , убывающего от t до 0: $P_i = 2^d P_{i+1} + b_i Q$, полагая $P_{t+1} = P_\infty$. Результатом является P_0 . Обычно оптимум достигается при $d = 3$ или $d = 4$.

Таким образом, использование эллиптической кривой позволяет обеспечить более высокую скорость вычислений по сравнению с криптоалгоритмами, использующими задачу дискретного логарифмирования, и RSA той же стойкости. Это делает эллиптические кривые привлекательными для построения криптографических алгоритмов большой стойкости, в частности, для открытого распространения ключей. Например, для установления сеансового ключа ГОСТ 28147–89 протоколом Диффи — Хеллмана без снижения стойкости первоначального криптоалгоритма необходимо использовать простое число длиной порядка 16 кбит. Эллиптическая кривая позволяет использовать размер задачи в 32 раза меньше.

2. Генерация эллиптической кривой

В настоящее время для целей криптографии используются обычно эллиптические кривые над простым полем и на поле характеристики 2. Имеются публикации о использовании кривых над полем характеристики $2^{16} + 1$. Кривых над полем характеристики 2 с требуемыми свойствами довольно мало, их едва ли наберется несколько десятков. Это обстоятельство снижает степень доверия к таким кривым, так как пользователь, по существу, лишен возможности выбрать эллиптическую кривую по своему усмотрению.

Генерация открытого ключа для криптосистемы сводится к выбору эллиптической кривой с циклической группой большого простого порядка r с учетом требований $p \neq r$; r взаимно просто с $p - 1, p^2 - 1, \dots, p^k - 1$. Число точек на кривой может быть вычислено алгоритмом Чуфа — Элкиса — Аткина [7] со сложностью, оцениваемой полиномом степени 8 от длины числа p . Этот алгоритм является непрактичным из-за большой сложности.

Сложность генерации эллиптической кривой может быть значительно уменьшена, если ограничиться классом кривых специального вида.

Наиболее простая ситуация получается, если отображение

$$x \rightarrow x^3 + Ax + B$$

является взаимно однозначным, число точек на такой кривой всегда равно $p + 1$. В этом случае $k = 2$ и задача логарифмирования на кривой над полем F_p сводится к логарифмированию в поле из p^2 элементов субэкспоненциальным алгоритмом, то есть такая кривая не позволяет строить стойкие криптоалгоритмы.

Простое число p может быть разложено на множители в порядке O_K мнимого квадратичного поля $K = \mathbf{Q}(\sqrt{-D})$. Особенно простые формулы для числа точек получаются при использовании дискриминантов D , дающих число классов поля K , равное единице. Такое число классов обеспечивают дискриминанты: $D \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. Кольцо O_K в общем случае не единственно и связано с решеткой периодов кривой и j -инвариантом [9]. Значение j и вид уравнения кривой $y^2 = f(x)$ для разных значений дискриминанта приведены в следующей таблице.

D	O_K	j	$f(x)$ или k	p	$N - (p + 1)$
1	$\mathbf{Z}[\sqrt{-1}]$	12^3	$x^3 + Ax$	$a^2 + b^2$	$\pm 2a,$ $\pm 2b$
1	$\mathbf{Z}[2\sqrt{-1}]$	66^3	$x^3 + 3kt^2x + 2kt^3, k = \frac{3^3 7^2}{11^3}$	$a^2 + 4b^2$	$\pm 2a$
2	$\mathbf{Z}[\sqrt{-2}]$	20^3	$x^3 + 3kt^2x + 2kt^3, k = \frac{5^3}{7^2 2}$	$a^2 + 2b^2$	$\pm 2a$
3	$\mathbf{Z}\left[\frac{-1 + \sqrt{-3}}{2}\right]$	0	$x^3 + B$	$a^2 - ab + b^2,$ $a \equiv 2 (3),$ $b \equiv 0 (3)$	$\pm(a + b),$ $\pm(2a - b),$ $\pm(2b - a)$
3	$\mathbf{Z}[\sqrt{-3}]$	$16 \cdot 15^3$	$x^3 + 3kt^2x + 2kt^3, k = \frac{-5^3}{11^2}$	$a^2 + 12b^2$	$\pm 2a$
3	$\mathbf{Z}\left[\frac{-1 + 3\sqrt{-3}}{2}\right]$	$-3 \cdot 160^3$	$x^3 + 3kt^2x + 2kt^3, k = \frac{-2^9 5^3}{11^2 23^2}$	$a^2 + 27b^2$	$\pm 2a$
7	$\mathbf{Z}\left[\frac{-1 + \sqrt{-7}}{2}\right]$	-15^3	$x^3 + 3kt^2x + 2kt^3, k = \frac{-5^3}{3^3 7}$	$a^2 + 7b^2$	$\pm 2a$
7	$\mathbf{Z}[\sqrt{-7}]$	255^3	$x^3 + 3kt^2x + 2kt^3, k = \frac{-5^3 17^3}{3^5 19^2 7}$	$a^2 + 28b^2$	$\pm 2a$
11	$\mathbf{Z}\left[\frac{-1 + \sqrt{-11}}{2}\right]$	-32^3	$x^3 + 3kt^2x + 2kt^3, k = \frac{-2^9}{7^2 11}$	$a^2 + 11b^2$	$\pm 2a$
19	$\mathbf{Z}\left[\frac{-1 + \sqrt{-19}}{2}\right]$	-96^3	$x^3 + 3kt^2x + 2kt^3, k = \frac{-2^9}{3^3 19}$	$a^2 + 19b^2$	$\pm 2a$
43	$\mathbf{Z}\left[\frac{-1 + \sqrt{-43}}{2}\right]$	-960^3	$x^3 + 3kt^2x + 2kt^3, k = \frac{-2^{12} 5^3}{3^5 7^2 43}$	$a^2 + 43b^2$	$\pm 2a$
67	$\mathbf{Z}\left[\frac{-1 + \sqrt{-67}}{2}\right]$	-5280^3	$x^3 + 3kt^2x + 2kt^3,$ $k = \frac{-2^9 5^3 11^3}{3^3 7^2 31^2 67}$	$a^2 + 67b^2$	$\pm 2a$
163	$\mathbf{Z}\left[\frac{-1 + \sqrt{-163}}{2}\right]$	-640320^3	$x^3 + 3kt^2x + 2kt^3,$ $k = \frac{-2^{12} 5^3 23^3 29^3}{3^3 7^2 11^2 19^2 127^2 163}$	$a^2 + 163b^2$	$\pm 2a$

Для генерации эллиптической кривой с хорошими криптографическими свойствами можно разложить простое число p на множители в O_K и подобрать число p так, чтобы число точек на кривой удовлетворяло необходимым требованиям. Разложение имеет вид:

$$p = a^2 + Db^2. \quad (2)$$

Для того, чтобы такое разложение существовало, достаточно, чтобы $-D$ являлся квадратичным вычетом по модулю p . Действительно, пусть $-D$ — квадратичный вычет. Тогда существует решение сравнения

$$x^2 + D \equiv 0 \pmod{p}$$

или разрешимо в целых числах диофантово уравнение

$$s^2 + D = tp.$$

Поскольку число классов поля K равно 1, то кольцо целых O_K поля K обладает однозначным разложением на простые множители. Имеем в O_K :

$$(s + \sqrt{-D})(s - \sqrt{-D}) = tp.$$

Если предположить, что p — простой элемент O_K , то один из сомножителей в левой части должен делиться на p . Поскольку этого нет, то p раскладывается на простые множители в O_K . Единственно возможное разложение имеет вид (2). Существует алгоритм разложения в $\mathbf{Z}[\sqrt{-D}]$ с полиномиальной сложностью [10].

Однако более перспективный алгоритм предполагает подбор коэффициентов разложения (2) таким образом, что число p будет простым и будут выполняться необходимые криптографические требования для эллиптической кривой. Сложность проверки числа на простоту оценивается полиномом степени 3 от размера задачи, а среднее число попыток до получения простого p и большого простого делителя числа N равно $O(\log^2 p)$. Поэтому итоговая сложность генерации эллиптической кривой оценивается полиномом степени 5.

Эллиптические кривые над алгебраическим замыканием конечного поля имеют тривиальные автоморфизмы, заключающиеся в умножении точки на целое число. Таким образом, множество автоморфизмов всегда содержит множество \mathbf{Z} . Однако иногда множество автоморфизмов строго больше \mathbf{Z} . Если $D = 3$, уравнение кривой имеет вид $y^2 = x^3 + B$, $p \equiv 1 \pmod{6}$. Тогда существует θ — примитивный корень степени 6 из 1 по модулю p , а также, если число точек свободно от квадратов (сравнимых с 2 по модулю 3), существует σ — примитивный корень степени 6 из простого делителя порядка группы. Автоморфизм для конечной точки (x, y) имеет вид $\phi: (\theta^2 x, \theta^3 y) = \sigma \cdot (x, y)$. Такие автоморфизмы составляют циклическую группу порядка 6 с образующей ϕ .

Если $D = 1$, $p \equiv 1 \pmod{4}$, уравнение кривой имеет вид $y^2 = x^3 + Ax$. Тогда существует i — примитивный корень степени 4 из 1 по модулю p , а также, если число точек свободно от квадратов, сравнимых с 3 по модулю 4, существует j — примитивный корень степени 4 из 1 по модулю простого делителя порядка группы. Автоморфизм для точки (x, y) имеет вид $\phi(-x, iy) = j \cdot (x, y)$. Такие автоморфизмы составляют циклическую группу порядка 4 с образующей ϕ .

Указанные автоморфизмы для этих двух типов кривых являются примерами комплексного умножения. Наличие комплексного умножения позволяет ускорить вычисления, но одновременно может приводить (и в указанных случаях приводит) к снижению сложности логарифмирования в группе точек кривой. Снижение сложности связано с тем, что алгоритм Полларда можно применять не к точкам, а к орбитам группы автоморфизмов в кольце эндоморфизмов. Поэтому задача логарифмирования в группе точек кривой сводится к логарифмированию в полугруппе орбит автоморфизмов и затем уточнению значения логарифма внутри орбиты.

Если $D = 2$, то $p = a^2 + 2b^2$ и -2 является квадратичным вычетом по модулю p . Уравнение кривой удобно записать в виде, отличном от (1), для которого удобно записываются формулы комплексного умножения [8]:

$$y^2 = x(x^2 - 4tx + 2t^2) \quad (3)$$

где t — произвольный ненулевой элемент. При этом формула для сложения двух различных точек сохраняется, а удвоение точки можно выполнять с помощью комплексного умножения. Число точек кривой равно $N = p + 1 \pm 2a$. Если найдена кривая с одним из двух возможных вариантов числа точек, то умножением коэффициента t на произвольный квадратичный невычет получается скрученная кривая со вторым вариантом числа точек. Нетрудно заметить, что всегда $N \equiv 0 \pmod{2}$. Случай $N \equiv 2 \pmod{4}$ получается лишь при нечетных a, b , при этом $b \equiv 0 \pmod{3}$. Эти кривые над алгебраически замкнутым полем обладают нетривиальным автоморфизмом, который можно вывести из изогении степени 2 [9]. Этот автоморфизм соответствует комплексному умножению точки (x, y) кривой (3) на $\sqrt{-2}$ и имеет вид

$$\phi: (x, y) \rightarrow \left(\frac{-y^2}{2x^2}, \frac{y(x^2 - 2t^2)}{2\sqrt{-2}x^2} \right), \quad (4)$$

то есть

$$\phi(x, y) = \sqrt{-2} \cdot (x, y). \quad (5)$$

Здесь каждому из двух значений корня из -2 по модулю p , участвующему в (4), взаимно однозначно соответствует свое значение корня из -2 по модулю q в (5). В случае проективной кривой

$$Y^2Z = X^3 - 4tX^2Z + 2t^2XZ^2$$

формулы комплексного умножения примут вид

$$\sqrt{-2} \cdot (X_1, Y_1, Z_1) = (X_2, Y_2, Z_2),$$

где

$$X_2 = Y_1^2 Z_1, \quad Y_2 = \frac{Y_1(X_1^2 - 4t^2 Z_1^2)}{\sqrt{-2}}, \quad Z_2 = 2X_1^2 Z_1.$$

Это позволяет вместо удвоения точки использовать дважды комплексное умножение.

Для этой эллиптической кривой возможна атака, связанная с разбиением множества точек на классы эквивалентности, совпадающие со смежными классами группы \mathbf{F}_r^* по подгруппе, образованной элементом $\sqrt{-2}$, и определением принадлежности данной точки некоторому классу эквивалентности. Поскольку логарифмы внутри класса связаны вычислимым образом, такая атака может иметь успех. Для исключения атаки имеет смысл выбирать эллиптическую кривую так, чтобы элемент $\sqrt{-2}$ являлся образующей всей группы \mathbf{F}_r^* .

Аналогичные формулы для комплексного умножения существуют и для других эллиптических кривых, рассмотренных в данной статье, с j -инвариантом, отличным от 0, 1728. Следовательно, в каждом рассмотренном случае целесообразно обеспечить, чтобы значение комплексного множителя, определяемого комплексным умножением, было образующей группы \mathbf{F}_r^* .

Нетрудно видеть, что в остальных случаях, предусмотренных в таблице, если рассматривается разложение $p = a^2 + Db^2$, $D \equiv 3 \pmod{4}$ или $D \equiv 0 \pmod{4}$, и $N = p + 1 \pm 2a$, то всегда $N \equiv 0 \pmod{4}$. Однако в случае разложения характеристики поля в O_K :

$$p = Db^2 + Dab + \frac{D+1}{4}a^2$$

число точек равно $N = p + 1 \pm a$ и может быть нечетным и даже простым.

Кольца O_K являются евклидовыми для случаев

$$O_K \in \left\{ \mathbf{Z}[\sqrt{-1}], \mathbf{Z}[2\sqrt{-1}], \mathbf{Z}[\sqrt{-2}], \mathbf{Z}\left[\frac{-1 + \sqrt{-3}}{2}\right], \mathbf{Z}\left[\frac{-1 + \sqrt{-7}}{2}\right], \mathbf{Z}\left[\frac{-1 + \sqrt{-11}}{2}\right] \right\}.$$

Для этих случаев работает аналог алгоритма Евклида, позволяющий для целого k найти его представление $k \equiv k_0 + k_1 \xi \pmod{r}$, где ξ — комплексное число, присоединение которого к \mathbf{Z} дает кольцо эндоморфизмов кривой над \mathbf{C} . При этом можно обеспечить единственное такое представление с минимальной нормой числа k и $|k_0|, |k_1| < \sqrt{r}$ [11]. Если формулы

для комплексного умножения не являются сложными, то можно для умножения точки на число воспользоваться следующей цепочкой:

$$k \rightarrow k_0 + k_1\xi \rightarrow (k_0Q, k_1Q) \rightarrow k_1\xi Q \rightarrow k_0Q + k_1\xi Q = kQ,$$

что позволяет ускорить вычисления, если при вычислении k_0Q , k_1Q используется общая база $2Q, 3Q, \dots, 2^dQ$.

Литература

1. Menezes A., van Oorschot P., Vanstone S. Handbook of applied cryptography. — CRC press, 1997.
2. Баранов А. П., Борисенко Н. П., Зегжда П. Д., Корт С. С., Ростовцев А. Г. Математические методы защиты информации. — Военный институт правительственной связи. Орел, 1997.
3. Pollard J. Monte Carlo methods for index computation (mod p) // Math. Comp., v. 32, № 143, pp. 918–924.
4. Menezes A., Okamoto T., Vanstone S. Reducing elliptic curve logarithms to logarithms in a finite field // Proc. of the 23–rd ACM symposium on theory of computing, 1991, pp. 80–89.
1. Semaev I. A. Evaluation of discrete logarithms in a group of p -torsion points of an elliptic curves in characteristic p // Math. Comp., v. 67, № 221, 1998, pp. 353–356.
6. Ростовцев А. Г., Буренкова А. П., Маховенко Е. Б. О комплексном умножении на эллиптических кривых // Проблемы информационной безопасности, № 16, 1996. С. 90–91.
7. Schoof R. Elliptic curves over finite fields and the computation of square roots mod p // Math. Comp., v. 44, 1984, pp. 483–494.
8. Atkin A. O., Morain F. Elliptic curves and primality proving // Math. Comp., v. 61, 1993, pp. 29–68.
9. Husemöller D. Elliptic curves. — Springer–Verlag, 1986.
10. Pollard J., Schnorr C. An efficient solution of the congruence $x^2 + ky^2 = m \pmod{n}$ // IEEE Trans. on Inform. Theory, IT–33, 1987, pp. 702–709.
11. Ростовцев А. Г. Алгебраические основы криптографии. — Мир и Семья, СПб, 2000.