Math-Net.Ru

Общероссийский математический портал

А. Б. Спельников, Метод адаптивного «окна» операций в эллиптических кривых, *Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки*, 2008, выпуск 2(), 279–281

DOI: <https://doi.org/10.14498/vsgtu613>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.209.158.208

26 апреля 2023 г., 16:32:54

УДК 512.742.72

МЕТОД АДАПТИВНОГО «ОКНА» ОПЕРАЦИЙ
В ЭЛЛИПТИЧЕСКИХ КРИВЫХ

А. Б. Спельников

Северо-Кавказский государственный технический университет,
355029, г. Ставрополь, просп. Кулакова, 2.

E-mail: fiss_run@mail.ru

*Разработан алгоритм адаптивного «оконного» умножения точки на число на эллиптической кривой, позволяющий увеличить скорость расчетов в криптографических приложениях.***Ключевые слова:** эллиптические кривые, умножение точки на число.

В общем случае умножение точки P на эллиптической кривой на число определяется как комбинация последовательных сложений и удвоений точки. Выделяют различные методики умножения [1]. Рассмотрим некоторые из них.

Метод прямой последовательности. Показатель представляется в виде

$$l = \sum_{i=0}^{n-1} l_i 2^i,$$

где $l_i \in \{0, 1\}$, i — порядковый номер бита данных. Затем последовательно вычисляются точки $2^{i+1}P$ удвоением точки 2^iP ($i = 0, 1, \dots, n-1$) и складываются те из них, для которых коэффициент l равен единице.

Метод обратной последовательности. В данном случае вычисляются точки $P_{i-1} = 2P + l_{i-1}P$ ($i = n-1, n-2, \dots, 1$).

Метод обратной последовательности ускоряется при помощи методики «окон». «Окном» называется представление основания системы счисления, равного степени числа два. Для этого показатель l разбивается на группы, по величине степени:

$$l = l_0 + 2^d l_1 + 2^{dm} l_m.$$

Вычисляются значения $2P, 3P \dots 2^d P$. Далее вычисляется $P_{i-1} = 2^d P + l_{i-1}P$, где $i = m-1, m-2, \dots, 1$.

Данным методом число сложений сокращается примерно в 4 раза по сравнению с числом удвоений [1].

Разработана методика изменяемого, адаптивного «окна».

Вычислим значения $2P, 3P \dots 2^d P$. Здесь d — минимальный размер окна.

Рассмотрим двоичное представление показателя l . В общем случае оно представляет собой набор из нулей и единиц со случайным распределением.

Вычислим первое значение $P_1 = l_m P$. Здесь l_m — значение старших d бит, представленное в десятичной системе. Это значение найдено на этапе предварительных вычислений.

Затем передвинем указатель на d бит. Рассмотрим значение нового старшего бита. Пусть это 1. Вычислим $P_2 = 2^d P_1 + l_{m-1}P$. Здесь l_{m-1} — значение новых старших d бит, представленное в десятичной системе.

Передвинем указатель на d бит. Рассмотрим значение нового старшего бита. Пусть это 0. Передвинем указатель на следующий бит. Повторяем операцию до тех

Спельников Алан Борисович — аспирант кафедры информационных систем и технологий Северо-Кавказского государственного технического университета.

пор, пока бит не будет равен единице. Пусть получилось смещение в t бит. Вычислим $P_3 = 2^{d+t}P_2 + l_{m-2}P$. Здесь l_{m-2} — значение новых старших d бит, представленное в десятичной системе (см. рисунок). Тогда представим выражение для вычислений методом адаптивного «окна»:

$$P_{i-1} = 2^{d+t}P + l_{i-1}P.$$

Здесь i — переменное число, которое определяется в процессе вычислений.

Метод адаптивного «окна»

Численный пример. Пусть дана эллиптическая кривая вида $y^2 = x^3 + 21x + 17$, определённая в поле порядка $p = 31$. Пусть исходная точка $P = (1; 15)$, показатель $l = 142$. Выберем размер «окна» $d = 2$.

Вычислим $2P = (16; 4)$, $3P = (2; 25)$.

Двоичное представление показателя $l = 10011010_2 = 154_{10}$.

Первый показатель $l = 10_2 = 2_{10}$.

Вычисляем $P_1 = 2P = (16; 4)$.

Передвигаем указатель на 2 бита. Проверяем старший бит, передвигаем на следующий и присваиваем $t = 1$. Проверяем бит: $l = 11_2 = 3_{10}$.

Вычисляем $P_2 = 2^{2+1}P_1 + 3P = (20; 6)$.

Передвигаем указатель на 2 бита. Проверяем старший бит, передвигаем на следующий и присваиваем $t = 1$. Проверяем бит: $l = 10_2 = 2_{10}$.

Вычисляем окончательно: $P_3 = 2^{2+1}P_2 + 2P = (6; 24)$.

В результате применения метода адаптивного «окна» в данном примере экономия по отношению к стандартному методу «окон» составила одну операцию сложения точек эллиптической кривой.

Рассчитаем изменение количества операций и прирост производительности умножителя, полученный вследствие применения методики адаптивного «окна».

Рассмотрим модель, представленную на рисунке. С точки зрения теории вероятностей, значение бита под указателем — случайное событие, вероятность исхода которого равна 0,5. Тогда в первом приближении количество сдвигающих нулей после блоков можно выразить по формуле

$$k_0 = \frac{0,5h}{w},$$

где h — значимая разрядность числа.

Так как значение под указателем, равное нулю, сдвигает следующий блок, то количество блоков будет уменьшаться. Значит, более точно количество блоков, после которых стоит ноль, можно вычислить по формуле

$$k_1 = \frac{0,5h}{w} - \frac{h}{8w^2} = 0,5h \left(\frac{w-1}{w^2} \right).$$

По аналогии можно вычислить количество блоков, после которых есть i нулей:

$$k_i = 0,5k_{i-1} \left(\frac{w-1}{w} \right) = 0,5^i h \left(\frac{(w-1)^i}{w^{i+1}} \right).$$

С учётом того, что блоки k_i являются подмножеством блоков k_{i-1} , получим выражение для нахождения количества блоков, после которых встречается заданное

число нулей:

$$b_i = k_i - \sum_{j=i+1}^{\frac{n}{w}-1} k_j.$$

Тогда наиболее вероятное количество операций сложения точек можно найти по формуле

$$K = \frac{1}{w} \left(h - \sum_{j=1}^{\frac{h}{w}-1} b_j \right).$$

Таким образом, разработан алгоритм адаптивного «оконного» умножения точки на число на эллиптической кривой, позволяющий увеличить скорость расчётов в криптографических приложениях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ростовцев, А. Г. Теоретическая криптография [Текст] / А. Г. Ростовцев, Е. Б. Маховенко. — СПб.: Профессионал, 2005. — 478 с. — ISBN 5-98371-012-5.

Поступила в редакцию 30/VI/2008;
в окончательном варианте — 16/X/2008.

MSC: 14H52

THE ADAPTIVE “WINDOW” METHOD FOR ELLIPTIC CURVE OPERATIONS

A. B. Spel'nikov

North Caucasus State Technical University,
355029, Stavropol', prosp. Kulakova, 2.

E-mail: fiiss_run@mail.ru

The algorithm of adaptive “window” multiplication of a point by a number on the elliptic curve is introduced, allowing to increase the calculation speed in cryptographic applications.

Key words: *elliptic curves, point at number multiplication.*

Original article submitted 30/VI/2008;
revision submitted 16/X/2008.

Spel'nikov Alan Borisovich, Postgraduate Student, Dept. of Information Systems and Technologies of North Caucasus State Technical University.