МЕТОДЫ УМНОЖЕНИЯ ТОЧКИ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ НА ЧИСЛО

Короткевич А. В.
Кафедра программного обеспечения информационных технологий, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: ankor91@mail.ru

Выделены основные математические операции, используемые в эллиптической криптографии. Рассмотрены методы оптимизации выполнения умножения точки эллиптической кривой на число, дан теоретический анализ производительности данных методов. Выполнены практические исследования производительности разработанных методов.

Введение

Эллиптические криптосистемы являются на сегодняшний день одними из самых перспективных и востребованных. Объясняется это меньшим размером ключа при той же криптостойкости по сравнению с другими ассиметричными криптосистемами, что позволяет получить преимущество в производительности алгоритмов. Именно производительность является ключевой проблемой ассиметричных криптосистем. Рассмотрев метод шифрования Менезеса-Ванстоуна, можно выделить следующие основные математические операции при использовании эллиптической криптографии: умножение точки эллиптической кривой на число, мультипликативная инверсия числа по модулю, возведение числа в степень по модулю [1]. Операция умножения точки эллиптической кривой на число является ключевой в любых эллиптических криптосистемах. Методы ее оптимизации будут рассмотрены далее.

I. Бинарное представление множителя

Базовыми операциями над точкой эллиптической кривой являются операции сложения точек и удвоения точки. Потому для умножения точки эллиптической кривой P на целое число k необходимо оптимальным образом сочетать данные операции. Т.к. операция удвоения точки позволяет гораздо быстрее, чем сложение, приближать точку к требуемому значению kP, то необходимо использовать максимально возможное число таких операций.

Возможным решением поставленной задачи является следующий алгоритм, использующий бинарное представление множителя в виде массива бит длиной t: $k = (k_{t-1}, ..., k_1, k_0)_2$. На начальном шаге итоговому результату присваивается значение нулевой точки. Затем при проходе бинарного массива, начиная со старшего индекса, на каждом шаге результирующее значение удваивается, а после этого, если текущий бит равен 1, дополнительно увеличивается на P. В результате итоговое значение будет содержать сумму произведений точки P на числа, являющиеся степенью числа 2 и в сумме дающие k, что эквивалентно искомому произведению kP. Среднее число единиц в бинарном представлении числа k равно $t/2$, потому сложность данного алгоритма можно представить как $\frac{tA}{2} + tD$, где A и D – сложности операций сложения и умножения соответственно.

II. Использование $NAF(k)$

Как известно, если точка P эллиптической кривой имеет координаты (x, y), то точка $-P$ – координаты $(x, -y)$, а это означает, что операция вычитания точек фактически является операцией сложения и имеет эквивалентную сложность. Таким образом, при умножении точки эллиптической кривой на произвольное натуральное число k можно пользоваться также операциями вычитания точек, что позволяет снизить сложность алгоритма, воспользовавшись представлением числа с помощью NAF (англ. non-adjacent form). $NAF(k)$ называется такое представление положительного числа k, при котором $k = \sum_{i=0}^{l-1} k_i 2^i$, где $k_i \in \{0, \pm 1\}, k_{l-1} \neq 0$ и не существует никаких двух последовательных ненулевых значений k_i [2]. Длина такого представления равняется l.

Пусть k – натуральное число. Тогда $NAF(k)$ этого числа обладает следующими свойствами:

1. $NAF(k)$ является уникальным для любого k.
2. $NAF(k)$ содержит минимально возможное количество ненулевых чисел в своем представлении.
3. Длина $NAF(k)$ в худшем случае на 1 больше бинарного представления числа k.
4. Если длину $NAF(k)$ обозначить как l, то $2^l/3 < k < 2^{l+1}/3$.
5. Среднее количество ненулевых цифр среди всех NAF длины l составляет приблизительно $l/3$.

$NAF(k)$ может быть эффективно вычислено по алгоритму, схожему по сложности с бинарным разложением числа, потому практически не

требует никаких дополнительных затрат. Алгоритм умножения точки эллиптической кривой на число при помощи $NAF(k)$ аналогичен рассмотренному ранее бинарному за исключением замены некоторых операций сложений на операции вычитания, т.е. сложения с противоположной точкой.

Как следует из свойств $NAF(k)$, вычислительная сложность данного алгоритма составляет приблизительно $\frac{tA}{3} + tD$, где t – длина бинарного представления числа k, A и D – сложности операций сложения и умножения соответственно. Следовательно, данный алгоритм требует на $t/6$ меньше операций сложения, чем алгоритм, рассмотренный первым, однако, требует предварительного вычисления $NAF(k)$. А раз алгоритм вычисления $NAF(k)$ обладает логарифмической сложностью относительно k, что незначительно по сравнению с операцией сложения точек эллиптической кривой, то в целом алгоритм на основе $NAF(k)$ оказывается эффективнее.

III. Использование $NAF_w(k)$

Выполнение предыдущего алгоритма может быть ускорено с использованием дополнительной памяти при помощи оконного метода, который обрабатывает w цифр числа k за один такт.

Пусть $w \geq 2$ – целое положительное число (назовем его шириной). $NAF_w(k)$ положительного числа k выражается как $k = \sum_{i=0}^{l-1} k_i 2^i$, где каждое ненулевое значение k_i нечетно, $|k_i| < 2^{w-1}, k_{l-1} \neq 0$ и по крайней мере одно из подряд идущих w чисел k_i является ненулевым [3]. l является длиной $NAF_w(k)$.

$NAF_w(k)$ обладает следующими свойствами:

1. $NAF_w(k)$ является уникальным для любого k.
2. $NAF_2(k) = NAF(k)$.
3. Длина $NAF_w(k)$ по крайней мере на единицу больше длины бинарного представления k.
4. Средняя плотность ненулевых чисел среди всех NAF_w с длиной l составляет приблизительно $l/(w+1)$.

При выполнении умножения точки с использованием $NAF_w(k)$ требуется предварительное вычисление результатов умножения точки P на степени числа 2. Потому при некоторой ширине w сложность предварительных вычислений сделает данный метод неэффективным. Оптимальное значение ширины w можно получить на основании практических исследований производительности.

IV. Практический анализ алгоритмов

Для практического анализа разработанных методов были выбраны рекомендованные NIST (Национальным институтом стандартов и технологий) кривые P-192, P-224, P-256, P-384, P-521 (цифра определяет размер модуля эллиптического поля в битах). Результаты исследования оптимальной ширины w для умножения с использованием $NAF_w(k)$ представлены на рисунке 1 (на оси абсцисс расположены значения ширины w, на оси ординат – относительное время выполнения умножения).

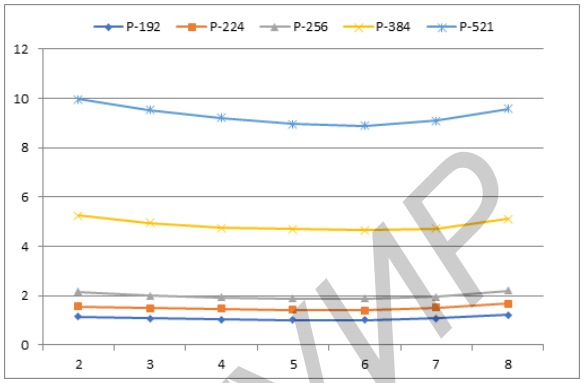

Рис. 1 – Умножение точки на число с использованием $NAF_w(k)$

По результатам практических испытаний можно заключить, что для данного набора кривых наилучшие результаты будут достигаться при $w = 5$.

На рисунке 2 представлен практический анализ выполнения умножения при помощи всех рассмотренных алгоритмов.

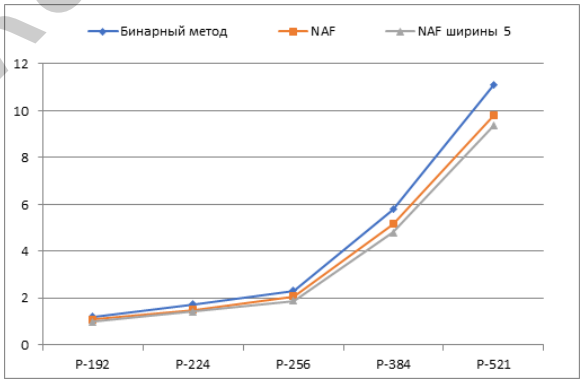

Рис. 2 – Сравнение методов умножения точки на число

Практические исследования показывают наилучшую производительность для метода на основе $NAF_w(k)$ с предварительно вычисленной оптимальной шириной $w = 5$ и наихудшую для бинарного метода, что совпадает с теоретическими оценками. В планы дальнейших исследований входит разработка и анализ более совершенных методов оптимизации умножения точки эллиптической кривой на число.

1. Hankerson, D. Guide to elliptic curve cryptography / D. Hankerson, A. Menezes, S. Vanstone – Springer-Verlag, New York, Inc, 2004 – P. 188-196.
2. Menezes, A. Handbook of applied cryptography / A. Menezes, P. Van Oorschot, S. Vanstone – CRC Press, 1997. – 810 с.
3. Schneier, B. Applied Cryptography. Protocols, algorithms and source code in C / B. Schneier – John Wiley & Sons, Inc., 1996. – 784 с.