

БЫСТРЫЕ КРИПТОГРАФИЧЕСКИЕ ВЫЧИСЛЕНИЯ С ПОМОЩЬЮ ДВУХОСНОВНЫХ ЦЕПОЧЕК

Бузук Р. В.

БГУ, факультет прикладной математики и информатики, Минск, Беларусь,
e-mail: roman.buzuk@gmail.com

Многие современные криптографические протоколы, в том числе протоколы Интернет, используют вычисления в группах точек эллиптических кривых. Основные вычисления приходится на решение следующей задачи: по точке P и натуральному числу n найти кратную точку nP . Существует множество алгоритмов определения кратной точки, каждый из них использует некоторое представление числа n . В докладе рассматривается представление, которое было предложено в работе [1] и получило название *двухосновные цепочки* (double-base chain):

$$n = 2^{d_1} 3^{t_1} (c_1 + 2^{d_2} 3^{t_2} (c_2 + \dots + 2^{d_l} 3^{t_l} \dots)) .$$

Здесь d_i, t_i – натуральные числа, $c_i \in S$, S – множество целых чисел небольшой абсолютной величины.

Цепочка для n определяет схему вычисления nP с помощью сложений, удвоений и утроений определенных точек эллиптической кривой. Длина цепочки l определяет количество сложений, сумма $d = \sum_{i=1}^l d_i$ – количество удвоений, сумма $t = \sum_{i=1}^l t_i$ – количество утроений. В свою очередь, характеристики цепочки определяются выбором S . Это множество задает также объем предвычислений: для определения кратной точки необходимо рассчитать малые кратные sP для элементов $s \in S$ больших 1. Предвычисления можно выполнить заранее, если точка P фиксирована.

В докладе рассматриваются несколько вариантов выбора S . Эти варианты индуцируют различные формы двухосновных цепочек: $S = \{1\}$ – беззнаковые цепочки, $S = \{1, -1\}$ – знаковые, $S = \{-c, -c + 1, \dots, -1, 0, 1, \dots, c - 1, c\}$ – оконные, $S = \{c_i: |c_i| \leq c, c_i \text{ не кратно } 2 \text{ и } 3\}$ – сокращенные оконные. При использовании оконных цепочек нужны предвычисления, затраты на них компенсируются уменьшением характеристик l, d, t .

Знаковые и беззнаковые цепочки просты в построении и исследовании. Получены оценки сверху для их длин: $l \leq \lceil \log_2 N \rceil$ для беззнаковых и $l \leq \lceil \log_6 \frac{5N-1}{4} \rceil$ для знаковых. Оценки достижимы.

Знаковую цепочку можно построить с помощью следующего жадного алгоритма: числа $n - 1$ и $n + 1$ делятся на максимальные степени 2 и 3, число n заменяется на минимальное из двух частных, деления продолжаются до тех пор, пока $n > 1$. Установлено, что жадный алгоритм дает цепочки, в которых средние значения d и t относятся как 2 к 1.

Для оконных и сокращенных оконных цепочек также существуют аналоги жадных алгоритмов. Эти алгоритмы использовались в вычислительных экспериментах по оценке сложности нахождения кратной точки для 256-битовых n . В экспериментах выбиралась эллиптическая кривая над простым полем, заданная коротким уравнением Вейерштрасса с коэффициентом $a = -3$. Точки кривой представлялись в якобиановых

координатах. Для произвольно выбираемой точки P максимальная производительность была достигнута на знаковых цепочках, для фиксированной точки – на сокращенных оконных.

Литература