

Анализ алгоритмов эллиптических кривых и их применение в информационных системах

А.А. Селин, М.И. Шельтук, Н.Ю. Исакова

МИРЭА — Российский технологический университет, Москва

Аннотация: В современных информационных системах всё большую популярность приобретают методы повышения эффективности анализа данных, основанные на топологии и аналитической геометрии. Однако из-за высокой степени сложности топологических структур, решение основных задач по обработке и хранению информации обеспечивается именно пространственной геометрией в совокупности с модульной арифметикой и аналитическим заданием геометрических структур, описание которых участвует в разработке новых методик решения оптимизационных задач. Практическое применение эллиптической криптографии, в том числе, в сетевых протоколах, основывается на использовании интерполяционных методов приближения графиков функций, так как при совершении множества последовательных математических операций может происходить потеря точности. Данная проблема связана с особенностями вычислительной архитектуры современных устройств. Известно, что ошибка может иметь накопительный эффект, поэтому методы приближения данных необходимо использовать последовательно, по мере выполнения вычислений.

Ключевые слова: эллиптическая кривая, информационная система, анализ данных, дискретный логарифм, порядок точки, скаляр, субэкспоненциальный алгоритм.

Введение

Исследование и разработка алгоритмов на эллиптических кривых проводится не только в области криптографии, но и в сфере анализа данных. Эллиптические кривые активно используются для обработки больших объёмов данных, а также их кластеризации.

Следует выделить 2 основные задачи, которые должны решать разрабатываемые и уже существующие алгоритмы:

- практическое применение в технически сложных информационных системах [1];
- формирование новых теоретических знаний о предметной области.

Эллиптической кривой, в более простой форме, называется множество точек (x, y) , удовлетворяющих уравнению:

$$y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5 \quad (1)$$

Если для поля $\mathbb{Z}_p$ характеристика $p > 3$, то уравнение эллиптической кривой принимает вид [2]:

$$y^2 = x^3 + ax + b \pmod{p} \quad (2)$$

Очевидно, коэффициенты a и b принадлежат множеству поля нечётной характеристики, а в рамках модульной арифметики они удовлетворяют условию [3]:

$$4A^3 + 27B^2 \not\equiv 0 \pmod{p} \quad (3)$$

Отсюда следует одно простое, но очень важное свойство рассматриваемых на данном множестве кривых: точки эллиптической кривой разбиваются на пары вида (x, y) и $(x, -y)$. Что заметно в неравенстве (1.3), где при фиксированном A парой подходящих чисел являются и $+B$, и противоположное ему $-B$.

Большое значение для приведённого метода имеет теорема Хассе, согласно которой количество точек на эллиптической кривой, заданной над полем $\mathbb{Z}_p$, близко к размеру этого конечного поля.

Рассмотрение основных алгоритмов на эллиптических кривых

Если рассматривать эллиптические кривые над полями характеристик, имеющих большие числовые значения, то можно увидеть, что плотность распределения точек и их количество значительно увеличиваются.

Сложность решения задачи дискретного логарифмирования составляет $O(\sqrt{n})$ (где n -порядок точки S , передаваемой в качестве параметра при классификации данных в информационной системе) и не может быть упрощена в общем случае [4].

Проведём сравнение асимптотики дискретного логарифмирования и нахождения скалярного произведения.

Рассмотрим точку $A(x_A; y_A)$ эллиптической кривой (1.4), заданной в общем виде над полем действительных чисел.

Определим следующее: n – натуральное число, порядок точки A ; l – натуральное число, скаляр точки lA ; s – минимальное натуральное число, такое что $2^s \geq l$.

Если представить число l в двоичной форме записи длиной r символов, то очевидно неравенство $r \leq s + 1$

Алгоритм «Удвоения – сложения» наглядно отражается в операциях над двоичными числами. Для получения из точки A точки lA , нам необходимо самым эффективным способом получить из 1 число l [5]. Для двоичных чисел данный алгоритм определяет следующие операции: добавление нуля в конце числа – то есть удвоение, замену последней цифры «0» на цифру «1», прибавление единицы к нечётному числу нам не потребуется. Итак, длина двоичной записи числа «1»: $q_1 = 1$, а длина числа l : $q_l = r$. Путём удвоения числа мы увеличиваем его длину на 1, однако нам может потребоваться не только удвоение, но и увеличение числа на 1. Таким образом, очевидно, что мы можем получить из числа 1 число l путём «удвоения-сложения» не менее чем за $2\Delta q = 2(q_l - q_1) = 2r - 2$ операций.

Таким образом:

$$\begin{cases} r \leq s + 1 \\ 2\Delta q = 2r - 2 \end{cases} \xRightarrow{2r} 2\Delta q \leq 2s \quad (4)$$

Прежде чем продолжать математические операции, заметим, что $l \leq n$ и обозначим оценённое ранее количество операций за h , тогда $h \leq 2s$.

$$2^s \geq l; 2^s \geq 2^{\log_2 l}$$

$$\log_2 l \leq s$$

$$\begin{cases} \log_2 l \leq s \\ h \leq 2s \end{cases} \xRightarrow{h=2s} h = 2 \log_2 l \quad (5)$$

Данное следствие из системы неравенств верно лишь для оценки сложности алгоритма, поскольку в данном случае мы должны рассмотреть так называемый «худший случай», то есть предположить, что требуемое количество операций будет равно верхней границе оценки.

Продолжим решение систем:

$$\begin{cases} l \leq n \\ h = 2 \log_2 l \end{cases} \stackrel{h \leq}{\Rightarrow} h \leq 2 \log_2 n \quad (6)$$

Введём две функции: $scalmult(n) = 2 \log_2 n$ – функцию сложности процесса нахождения скалярного произведения, $disclog(n) = \sqrt{n}$ – функцию сложности процесса дискретного логарифмирования, и сравним их на бесконечности.

$$\lim_{n \rightarrow \infty} \frac{scalmult(n)}{disclog(n)} = \lim_{n \rightarrow \infty} \frac{2 \log_2 n}{\sqrt{n}} = \lim_{n \rightarrow \infty} \frac{\frac{d(2 \log_2 n)}{dn}}{\frac{d(\sqrt{n})}{dn}} = \lim_{n \rightarrow \infty} \frac{4\sqrt{n}}{n \ln 2} = 0 \quad (7)$$

Не учитывая коэффициент $\frac{4}{\ln 2}$, получаем, что

$$\frac{scalmult(n)}{disclog(n)} \sim \frac{\sqrt{n}}{n} \text{ при } n \rightarrow \infty \quad (8)$$

Тогда, более строгая оценка будет выглядеть так, [6]:

$$disclog(n) = O(\sqrt{n}) \quad (9)$$

$$scalmult(n) = O(1) \quad (10)$$

Таким образом, при заранее известном значении скаляра l , асимптотическая сложность алгоритма «Удвоения-сложения» реализуется за конечное время, то есть не зависит от порядка точки, скалярное произведение которой нам необходимо вычислить [7].

Как уже было отмечено ранее, решение задачи дискретного логарифмирования в настоящее время не реализуется за счёт субэкспоненциальных алгоритмов, а лишь степенным с показателем 0,5 [8].

Особенно важным является следующее свойство эллиптической кривой – несмотря на то, что мы можем проводить суммирование двумя разными

способами (первый – последовательное сложение точки A с самой собой 3 раза, а второй – сложение $A + A$, после чего суммирование $2A + 2A$), в результате мы получим одну и ту же точку $4A$ [9]. В случае, когда скаляр точки принимает трёхзначные значения, количество способов получить её из заданной точки A будет достаточно большим, а все результаты действий будут одинаковыми, что достаточно трудно для восприятия [10].

Выводы

1) В статье предлагаются методы анализа асимптотики алгоритмов скалярного умножения и дискретного логарифмирования. Бинарная интерпретация последовательности действий по удвоению и сложению чисел отражает возможную оптимальную стратегию по получению числа из исходного за определённое количество итераций.

2) Особое внимание уделяется основным свойствам эллиптических кривых, рассмотрение и подробное описание которых необходимо для формализации данных, над которыми может производиться кластеризация, обработка и другие аналогичные действия.

3) В данной статье рассматриваются уже существующие алгоритмы действий над точками эллиптических кривых, расширяется понятие множества точек, классифицируемых по некоторым параметрам, вследствие чего создаются новые модели, описываемые математически.

Литература

1. Васильева И.Н. Криптографические методы защиты информации. – М.: Юрайт. 2024. – 350 с.
2. Романьков В.А. Введение в криптографию. Курс лекций. – М.: Форум. 2023. – 240 с.
3. Мартынов Л.М. Алгебра и теория чисел для криптографии. – М.: Лань. 2024. – 456 с.

4. Глухов М.М., Круглов И.А., Пичкур А.Б. Введение в теоретико-числовые методы криптографии. – М.: Лань. 2024. – 396 с.
5. Применко Э.А., Борисов А.В. Алгебраические основы криптографии в задачах и упражнениях. Учебное пособие. – М.: КУРС. 2023. – 104 с.
6. Солдаткина М.В. Теоретико-вероятностный подход к проблемам криптографии. – М.: Директмедиа Паблишинг. 2021. – 60 с.
7. Frank Rubin. Secret key cryptography. Ciphers, from simple to unbreakable. – New York.: Manning Publications Co. 2022. – 344 pages.
8. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации для изучающих компьютерную безопасность. – М.: Юрайт. 2024. – 474 с.
9. Рацеев С.М. Математические методы защиты информации и их основы. g Лань. 2023. – 140 с.
10. Aumasson Jean-Philippe. Serious Cryptography: A Practical Introduction to Modern Encryption. 2-nd edition. – San Francisco.: No Starch Press 2024. – 376 pages.

References

1. Vasil'eva I.N. Kriptograficheskie metody` zashhity` informacii [Cryptographic methods of information protection]. Moskva, 2024, 350 p.
2. Roman`kov V.A. Vvedenie v kriptografiyu. Kurs lekcij [Introduction to cryptography]. Moskva, 2023, 240 p.
3. Marty`nov L.M. Algebra i teoriya chisel dlya kriptografii [Algebra and number theory for cryptography]. Moskva, 2024, 456 p.
4. Gluxov M.M., Kruglov I.A., Pichkur A.B. Vvedenie v teoretiko-chislovy`e metody` kriptografii [Introduction to numerical-theoretical methods of cryptography]. Moskva, 2024, 396 p.

5. Primenko E`.A., Borisov A.V. Algebraicheskie osnovy` kriptografii v zadachax i uprazhneniyax. Uchebnoe posobie [Algebraic foundations of cryptography in problems and exercises. Textbook]. Moskva, 2023, 104 p.
6. Soldatkina M.V. Teoretiko-veroyatnostny`j podxod k problemam kriptografii [A theoretical and probabilistic approach to cryptography problems]. Moskva, 2021, 60 p.
7. Frank Rubin. Secret key cryptography. Ciphers, from simple to unbreakable. New York, 2022, 344 p.
8. Los` A.B., Nesterenko A.Yu., Rozhkov M.I. Kriptograficheskie metody` zashhity` informacii dlya izuchayushhix komp`yuternuyu bezopasnost` [Cryptographic methods of information protection for computer security students]. Moskva, 2024, 474 p.
9. Raceev S.M. Matematicheskie metody` zashhity` informacii i ix osnovy` [Mathematical methods of information protection and their basics]. Moskva, 2023, 140 p.
10. Aumasson Jean-Philippe. Serious Cryptography: A Practical Introduction to Modern Encryption. San Francisco, 2024, 376 p.

Дата поступления: 16.09.2025

Дата публикации: 26.10.2025