УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
июль–август 2022 Том 22 № 4 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
Jule–August 2022 Vol. 22 No 4 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

КОМПЬЮТЕРНЫЕ СИСТЕМЫ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

COMPUTER SCIENCE

doi: 10.17586/2226-1494-2022-22-4-674-680
УДК 004.021

Построение криптографических схем, основанных на эллиптических кривых над рациональными числами

Вадим Валерьевич Давыдов[1]✉, Жан-Мишель Никодэмович Дакуо[2], Иван Дмитриевич Иогансон[3], Алтана Феликсовна Хуцаева[4]

[1,2,3,4] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация

[1] vvdavydov@itmo.ru✉, https://orcid.org/0000-0002-5544-2434
[2] jeandakuo@itmo.ru, https://orcid.org/0000-0002-4084-8829
[3] ivan.ioganson@itmo.ru, https://orcid.org/0000-0002-0856-2249
[4] afkhutsaeva@itmo.ru, https://orcid.org/0000-0001-5494-7142

Аннотация

Предмет исследования. Исследована возможность использования в криптографических схемах эллиптических кривых над полем рациональных чисел ненулевого ранга. **Метод.** Впервые предложено построение криптосистем, безопасность которых основана на сложности решения математической задачи о рюкзаке на эллиптических кривых над рациональными числами ненулевых рангов. **Основные результаты.** Описан новый подход использования эллиптических кривых для криптографических схем. Выполнен ряд экспериментов для оценки поведения высот точек эллиптических кривых бесконечного порядка. Представлена модель криптосистемы, стойкой к вычислениям на квантовом компьютере и основанной на использовании рациональных точек кривой бесконечного порядка. Проведено исследование криптографической стойкости и эффективности предлагаемой схемы. Реализована атака на поиск секрета в криптосистеме, показано, что сложность атаки экспоненциальна. **Практическая значимость.** Рассмотренное решение может быть применено при построении реальных криптографических схем и протоколов.

Ключевые слова

эллиптические кривые, рациональные числа, ранг кривых, асимметричное шифрование, задача о рюкзаке

Благодарности

Работа выполнена при поддержке программы «Приоритет 2030».

Ссылка для цитирования: Давыдов В.В., Дакуо Ж.-М.Н., Иогансон И.Д., Хуцаева А.Ф. Построение криптографических схем, основанных на эллиптических кривых над рациональными числами // Научно-технический вестник информационных технологий, механики и оптики. 2022. Т. 22, № 4. С. 674–680. doi: 10.17586/2226-1494-2022-22-4-674-680

Building cryptographic schemes based on elliptic curves over rational numbers

Vadim V. Davydov[1]✉, Jean-Michelle N. Dakuo[2], Ivan D. Ioganson[3], Altana F. Khutsaeva[4]

[1,2,3,4] ITMO University, Saint Petersburg, 197101, Russian Federation

[1] vvdavydov@itmo.ru✉, https://orcid.org/0000-0002-5544-2434
[2] jeandakuo@itmo.ru, https://orcid.org/0000-0002-4084-8829
[3] ivan.ioganson@itmo.ru, https://orcid.org/0000-0002-0856-2249
[4] afkhutsaeva@itmo.ru, https://orcid.org/0000-0001-5494-7142

Abstract

The possibility of using elliptic curves over the rational field of non-zero ranks in cryptographic schemes is studied. For the first time, the construction of cryptosystems is proposed the security of which is based on the complexity of solving the knapsack problem on elliptic curves over rational numbers of non-zero ranks. A new approach to the use

of elliptic curves for cryptographic schemes is proposed. A few experiments have been carried out to estimate the heights characteristic of points on elliptic curves of infinite order. A model of a cryptosystem resistant to computations on a quantum computer and based on rational points of an infinite order curve is proposed. A study of the security and effectiveness of the proposed scheme has been carried out. An attack on the secret search in such a cryptosystem is implemented and it is shown that the complexity of the attack is exponential. The proposed solution can be applied in the construction of real cryptographic schemes as well as cryptographic protocols.

Keywords
elliptic curves, rational numbers, curve rank, asymmetric encryption, knapsack problem

Acknowledgements
This research was supported by Priority 2030 Federal Academic Leadership Program.

For citation: Davydov V.V., Dakuo J.-M.N., Ioganson I.D., Khutsaeva A.F. Building cryptographic schemes based on elliptic curves over rational numbers. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2022, vol. 22, no. 4, pp. 674–680 (in Russian). doi: 10.17586/2226-1494-2022-22-4-674-680

Введение

В настоящее время многие популярные криптосистемы с открытым ключом основаны на задачах факторизации больших целых чисел и дискретного логарифмирования в конечных группах. Например, в мультипликативной группе конечного поля и группе точек на эллиптической кривой над конечным полем. Эллиптические кривые представляют особый интерес, так как в построенных криптосистемах используются ключи меньшего размера при том же уровне безопасности по сравнению с аналогами из других областей криптографии [1].

На данный момент не существует эффективных алгоритмов, решающих задачу дискретного логарифмирования в группе точек эллиптической кривой за полиномиальное время. Это позволяет работать в полях меньшего размера, следовательно и генерировать ключи меньшего размера при том же уровне безопасности по сравнению с аналогами. Выполнение группового закона на эллиптических кривых позволяет реализовывать и применять уже известные алгоритмы в криптографии.

Один из классических протоколов на эллиптических кривых — протокол Диффи–Хеллмана [2], позволяющий осуществлять выработку общего секретного ключа. В зависимости от изначальных условий, например, если пользователи не установили общий ключ, существуют различные варианты решения таких задач. Так, в криптосистеме Месси–Омуры [3] благодаря свойствам эллиптических кривых осуществляется коммутативное шифрование: пользователи передают друг другу сообщения, не создавая при этом общего ключа. На эллиптических кривых также может быть реализована схема Эль–Гамаля [4], в которой осуществляются более эффективные вычисления, по сравнению со схемой на модульной арифметике. Это связано с тем, что операция возведения в степень сводится к сложению точек.

Кроме конечных полей, кривые можно рассматривать и над полем рациональных чисел. Эллиптические кривые над рациональным полем обладают особой групповой структурой. Луи Морделл (1922 год) выдвинул гипотезу о конечности числа рациональных точек для кривых первого рода [5], а Андре Вейль (1928 год) ввел обобщение гипотезы [6]. Впоследствии была сформулирована теорема Морделла–Вейля о том, что кривые над рациональным полем образуют конечнопорожденную абелеву группу, изоморфную группам точек кручения и точек бесконечного порядка. В 1935 году Найгел и Лутц [7] показали, каким образом можно найти точки подгруппы кручения. 1978 году Барри Мазуром было получено, что подгруппа точек кручения конечна и мала. Отметим, что подгруппа точек бесконечного порядка исследована недостаточно, количество точек генераторов данной подгруппы задает ранг кривой. В настоящее время известна кривая с максимальным рангом 28 [8], а большинство кривых имеют ранг 0 или 1. Задача подсчета точного ранга кривой является сложной, а поиск кривых высокого ранга остается открытой проблемой.

В настоящей работе предложено построение модели криптосистемы с использованием задачи о рюкзаке [9] на эллиптических кривых над рациональными числами.

Задача о рюкзаке является NP-полной и находит применение во многих областях. Первое упоминание о ней можно найти в трудах Данцига [10] и Мэтьюза [11], в общем случае она заключается в поиске таких m_i из множества $M = \{m_1, m_2, \dots m_n\}$, которые при умножении на известные коэффициенты из множества $K = \{k_1, k_2, \dots k_m\}$ в сумме дают целое число C:

$$C = \sum_{i=1}^{m} m_i \cdot k_i.$$

Впервые криптосистема, основанная на задаче о рюкзаке, была предложена Ральфом Мерклом и Мартином Хеллманом [12], где использована сверхвозрастающая последовательность секретного ключа. С помощью ключа осуществлена расшифровка текста, а в качестве открытого ключа использована несверхвозрастающая последовательность, по которой расшифровать число C без знания секретного ключа невозможно. Существует эффективная аппроксимирующая LLL-атака на данную криптосистему, где с помощью редуцированного базиса решетки появляется возможность решить задачу упаковки рюкзака с определенной вероятностью. Однако данная атака не применима к эллиптическим кривым, так как, в отличие от классической криптосистемы рюкзака, вместо чисел используются точки кривой [13].

Формулировка математической задачи

Пусть $E(\mathbb{Q})$ — эллиптическая кривая над полем рациональных чисел ($\mathbb{Q}$), заданная уравнением в обобщенной форме Вейерштрасса:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

где коэффициент $a_i \in \mathbb{Q}$ для $i \in \{1,2,3,4,6\}$, переменные $x, y \in \mathbb{Q}$.

По теореме Морделла–Вейля [13] группа точек на такой кривой — конечно сгенерированная абелева группа:

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r,$$

где $E(\mathbb{Q})_{tors}$ и $\mathbb{Z}^r$ — группы точек кручения кривой и бесконечного порядка соответственно; r — ранг эллиптической кривой.

Группа точек кручения кривой может быть представлена следующим образом:

$$E(\mathbb{Q})_{tors} = \{\text{точка } P \in E(\mathbb{Q}) \text{ и число } n \in \mathbb{N} \text{ такое, что } nP = \mathcal{O}\},$$

где $\mathcal{O}$ — точка на бесконечности. По теореме Мазура [14] порядок такой группы не превышает 16, также известно, каким группам изоморфна $E(\mathbb{Q})_{tors}$. Наибольший интерес при построении криптографических схем представляет группа $\mathbb{Z}^r$. Если ранг кривой равен нулю, то такая схема неприменима в криптографии, так как количество рациональных точек на кривой конечно и не превышает 16, что позволяет осуществить элементарный перебор точек.

Однако при $r > 0$ такие кривые обладают следующей особенностью. Пусть на кривой $E(\mathbb{Q})\{T_1, T_2, \ldots, T_n\}$ — множество точек кручения конечного порядка, а $\{P_1, P_2, \ldots, P_r\}$ — множество точек бесконечного порядка. Тогда любая точка $E(\mathbb{Q})$ имеет вид:

$$Q = a_1T_1 + a_2T_2 + \ldots + a_nT_n + b_1P_1 + b_2P_2 + \ldots + b_rP_r, \quad (1)$$

где $\{a_1, \ldots, a_n\}$, $\{b_1, \ldots, b_r\} \in \mathbb{Z}$, и сложение точек осуществляется по групповому закону.

Основная математическая проблема, на сложности которой можно строить криптосистемы – поиск коэффициентов $\{a_1, \ldots, a_n\}$, $\{b_1, \ldots, b_r\}$, при известных точке Q и группе $E(\mathbb{Q})/2E(\mathbb{Q})$. Если не существует алгоритма, с помощью которого данная задача может быть решена за полиномиальное время, тогда ее использование допустимо. Для оценки необходимо учитывать специфические свойства эллиптических кривых над рациональными числами. Одним из таких свойств является высота точки.

Пусть высота дроби $\frac{m}{n} \in \mathbb{Q}$, НОД$(m, n) = 1$, где НОД — наибольший общий делитель, задается как [15]:

$$h\left(\frac{m}{n}\right) = \log(\max\{|m|, |n|\}).$$

Высотой точки эллиптической кривой называют высоту ее значения по координате x. Спецификой процесса последовательного сложения точек кривой является предсказуемый рост высоты координат точки.

Также существует понятие о канонической высоте $\hat{h}$ точки P на кривой $E(\mathbb{Q})$ [15]:

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h(2^nP)}{4^n}.$$

Для канонической высоты верно, что для всех $P \in E(\mathbb{Q})$ и $m \in \mathbb{Z}$:

$$\hat{h}(mP) = m^2\hat{h}(P).$$

Таким образом, значение высоты точки можно аппроксимировать квадратичной функцией.

Высота позволяет получить некоторую информацию о коэффициентах, но не об их значениях. Следовательно, чем больше ранг эллиптической кривой, тем сложнее поиск коэффициентов в уравнении (1) из-за большего числа возможных вариантов.

Проведем оценку необходимого количество точек бесконечного порядка для достижения уровня безопасности, при котором время поиска таких коэффициентов будет больше полиномиального.

В уравнении (1) злоумышленнику известны координаты точки Q, соответственно, ему известно и значение высоты.

В случае, когда $r = 0$, число рациональных точек на кривой конечно. Как следует из теоремы Мазура, порядок подгруппы точек кручения не может быть больше 16, а порядки самих точек не превышают 12. Тогда необходимо перебрать один или два коэффициента у суммы точек подгруппы $E(\mathbb{Q})_{tors}$, что выполняется за линейное время $O(1)$.

Если $r = 1$, уравнение (1) приобретает вид:

$$Q = a_1T_1 + a_2T_2 + \ldots + a_nT_n + b_1P_1.$$

В данном случае по значению $h(Q)$ возможно определить небольшой диапазон для значения b_1 и найти коэффициент за полиномиальное время.

Если $r > 1$, зная высоту точки Q, нет возможности определить, какие коэффициенты $\{a_1, \ldots, a_n\}$, $\{b_1, \ldots, b_r\}$ использовались в уравнении (1).

Выберем кривую с $r = 2$ и тривиальной подгруппой точек кручения. Тогда уравнение (1) можно переписать в виде:

$$Q = b_1P_1 + b_2P_2.$$

Задача злоумышленника – поиск коэффициентов b_1 и b_2. Очевидно, что с увеличением количества точек бесконечного порядка (или ранга кривой), а следовательно, и коэффициентов, увеличивается сложность поиска.

Оценка вычислительной сложности поиска коэффициентов и точек в уравнении

Рассмотрим подробнее уравнение (1). Пусть злоумышленнику известны точки кручения, точки бесконечного порядка и итоговая точка (или ее высота).

Тогда задача злоумышленника — найти коэффициенты $\{a_1, \ldots, a_n\}$, $\{b_1, \ldots, b_r\}$.

Очевидно, что можно оптимизировать полный перебор коэффициентов, так как знание итоговой высоты дает дополнительную информацию о коэффициентах. Для простоты положим, что группа точек кручения тривиальна. Для поиска коэффициентов предлагается использовать следующий алгоритм поиска (Алгоритм).

Алгоритм. Алгоритм поиска коэффициентов уравнения (1) при условии, что подгруппа точек кручения T тривиальна

```
ФУНКЦИЯ Перебор_по_точкам(Q, r, {P_1, …, P_r})
Входные данные:  Q — целевая точка,
                 r — количество точек
                 бесконечного
                 порядка,
                 {P_1, P_2, …, P_r} — набор точек
                 бесконечного порядка.
НАЧАЛО
  ЕСЛИ  r == 2
        i_1 := 1
        ПОКА h(i_1 × P_1) < h(Q)
          i_1 := i_1 + 1
        i_2 := 0
        ПОКА h(i_2 × P_2) < h(Q)
          ПОКА   h(i_1 × P_1 + i_2 × P_2) > h(Q)
                 i_1 := i_1 – 1
          ПОКА h(i_1 × P_1 + i_2 × P_2) > h(Q)
                 i_2 := i_2 + 1
          ЕСЛИ Q == i_1 × P_1 + i_2 × P_2
                 ВЕРНУТЬ {{i_1, P_1}, {i_2, P_2}}
        ВЕРНУТЬ 0
  ИНАЧЕ
        i := 0
        ПОКА h(i × P_r) < h(Q)
          res := Перебор_по_точкам (Q – i × P_r, r – 1,
          {P_1, …, P_r–1})
          ЕСЛИ res ≠ 0
                 ВЕРНУТЬ res ∪ {{i, P_r}}
          i := i + 1
        ВЕРНУТЬ 0
КОНЕЦ
```

Заметим, что алгоритм поиска рекурсивно перебирает все возможные коэффициенты для точек бесконечного порядка. Тогда, в случае двух точек, данный алгоритм будет перебирать $O(\sqrt{(h(Q))})$ значений. Каждая дополнительная точка будет увеличивать сложность перебора еще в $O(\sqrt{(h(Q))})$. Таким образом, можно сделать вывод, что вычислительная сложность алгоритма поиска будет равна $O((h(Q))^{\frac{r-1}{2}})$.

Модель криптографической схемы, построенной на эллиптических кривых над рациональными числами

Построим криптографические схемы и протоколы. Приведем модель криптосистемы, основанной на задаче о рюкзаке. Выберем эллиптическую кривую $E(\mathbb{Q})$ с $r > 1$, наборами точек кручения $\{T_1, \ldots, T_n\}$ и бесконечного порядка $\{I_1, \ldots, I_r\}$.

Зададим секретный ключ как сверхвозрастающую последовательность точек $P_1, P_2, \ldots, P_n$, при условии, что такие точки задаются как набор линейных комбинаций:

$$P_i = q_1T_1 + \ldots + q_nT_n + k_1I_1 + \ldots + k_rI_r;\ q, k \in \{0, 1\}.$$

Под сверхвозрастающей последовательностью точек $P_1, P_2, \ldots, P_n$ будем понимать:

$$\forall i \in \{2 \ldots n\},\ h(P_i) > h(\sum_{j=1}^{i-1} P_j).$$

Зададим секретное преобразование φ, удовлетворяющее следующим свойствам:

1) сохраняется операция сложения над точками эллиптической кривой, т. е. $\varphi(P + Q) = \varphi(P) + \varphi(Q)$;
2) сверхвозрастающая последовательность точек $P_1, P_2, \ldots, P_n$ преобразуется в несверхвозрастающую $\varphi(P_1), \varphi(P_2), \ldots, \varphi(P_n)$;
3) преобразований подобных φ должно существовать достаточное количество, чтобы избежать атаки перебором.

Открытым ключом является последовательность $\varphi(P_1), \varphi(P_2), \ldots, \varphi(P_n)$.

Для шифрования сообщения $m = (b_1, b_2, \ldots, b_n)$, где $b_i \in \{0, 1\}$, вычислим точку: $C = \sum_{i=1}^{n} b_i \cdot \varphi(P_i)$.

Для расшифрования сообщения вычислим $Q = \varphi^{-1}(C)$. При условии, что i от n до 1, получим:

1) если $h(Q) \geq h(P_i)$, то $b_i = 1$, иначе $b_i = 0$;
2) $Q = Q - P_i$.

В результате расшифрования получим сообщение $m = (b_1, b_2, \ldots, b_n)$.

Основная проблема такой модели — большие размеры ключей, так как необходимо хранить координаты точек, размеры значений которых достаточно велики при больших значениях коэффициентов. Можно утверждать, что такая криптосистема обладает стойкостью к квантовому компьютеру, а также задача о рюкзаке не может быть вскрыта с помощью алгоритма LLL (Ленстра–Ленстра–Ловаса), так как работа ведется с точками эллиптической кривой.

Результаты экспериментов

Для проверки полученных результатов и оценки применения кривых различных рангов в криптографии выполнен ряд экспериментов. Основные эксперименты проведены с целью исследования поведения высот, а также уровня безопасности используемой задачи упаковки рюкзака. Для моделирования разработаны программы на языке Python с использованием программного обеспечения SAGE Math на персональном компьютере со следующими характеристиками: процессор AMD Ryzen 7 5800H, NVIDIA GeForce RTX 3070 Laptop GPU, оперативная память 32 ГБ, SSD 2024 ГБ.

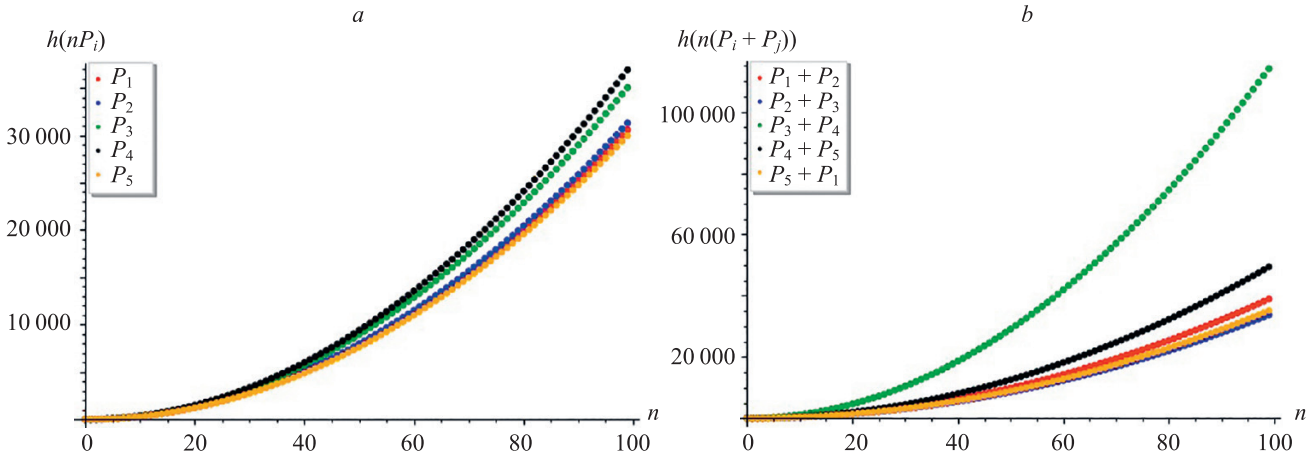

Рис. 1. Зависимости высот отдельных точек $\{P_1, \ldots, P_5\}$ (*a*) и суммы двух из них (*b*) на эллиптической кривой $E(\mathbb{Q})$ от умножающего коэффициента n

Fig. 1. The dependences of the individual points $\{P_1, \ldots, P_5\}$ heights (*a*) and the sum of two of them (*b*) on the elliptic curve $E(\mathbb{Q})$ on the multiplying factor n

Для определения аппроксимирующей функции для высот точек в зависимости от помножающего коэффициента осуществлен следующий эксперимент. Выбрана кривая $E(\mathbb{Q})$: $y^2 + y = x^3 - 79x + 342$ с рангом $r = 5$ и точками бесконечного порядка $P_1 = (3,11)$, $P_2 = (7,11)$, $P_3 = (10,23)$, $P_4 = (-6,24)$, $P_5 = (4,9)$. На рис. 1 показан рост высот каждой точки и суммы двух точек при умножении на различные коэффициенты от 1 до 100.

Как видно из полученных результатов, наблюдается квадратичный рост высот, в то же время для каждой точки рост незначительно отличается. Отсюда следует, что при поиске коэффициентов в уравнении (1) достаточно сложно определить, у какой точки был наибольший коэффициент.

Рассмотрим следующую задачу. Пусть на кривой $E(\mathbb{Q})$ точка Q задана в виде:

$$Q = b_1 P_i + b_2 P_j.$$

Зафиксируем сумму коэффициентов $b_1 + b_2 = 100$, последовательно увеличивая коэффициент b_1 и уменьшая коэффициент b_2. На рис. 2 показана зависимость высоты суммы при изменении соотношения умножающих коэффициентов.

Заметим, что минимальное значение итоговой высоты рис. 2 наблюдается при примерном равенстве коэффициентов $b_1 = b_2$, в то время как максимальные значения получаются, когда коэффициенты сильно различаются. Однако примерно одна и та же высота точки может получаться большим числом различных вариантов, например, когда коэффициенты дают меньшую или большую суммы. Необходимо иметь в виду, что при получении большого значения высоты точки кривой с помощью расчетов трудно определить, с помощью каких именно коэффициентов она была получена.

Проведем сравнение алгоритма полного перебора всех значений и предложенного алгоритма поиска, для оценки сложности решения задачи. В таблице показано время, полученное в процессе моделирования для разных кривых и с различным ограничением сверху на коэффициенты уравнения. За относительную единицу принято время решения задачи поиска коэффициентов с помощью алгоритма поиска для эллиптической кривой $E(\mathbb{Q})$: $y^2 + xy = x^3 + 1$ с $r = 2$ и максимальным значением коэффициентов 10.

Как видно из таблицы, предложенный алгоритм поиска работает гораздо быстрее алгоритма полного перебора при использовании кривых более высоких рангов. Отметим, что предложенный алгоритм имеет экспоненциальную сложность, что не позволяет эффективно решать задачу поиска умножающих коэффициентов.

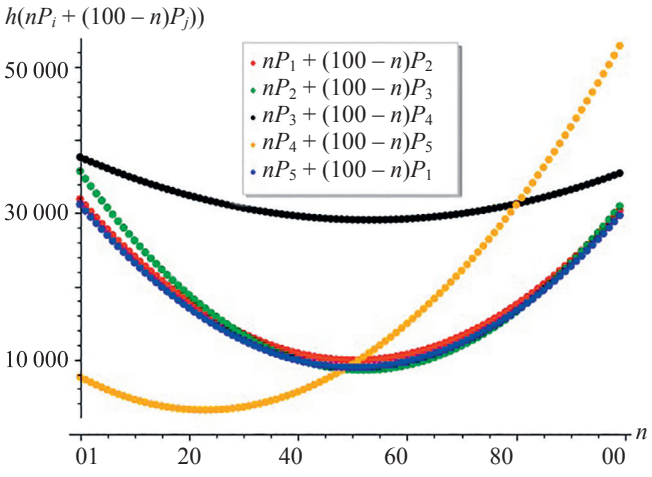

Рис. 2. Зависимость высоты от изменения соотношения умножающих коэффициентов b_1, b_2 для суммы двух точек при сохранении значения суммы

Fig. 2. The dependence of the height on the change in the ratio of multiplying coefficients b_1, b_2 for the sum of two points while maintaining the sum value

Таблица. Оценка времени решения задачи поиска коэффициентов
Table. Solution time estimation of the coefficient search problem

Эллиптическая кривая	Ранг	Максимальное значение коэффициентов	Время решения задачи поиска коэффициентов с помощью	
			алгоритма полного перебора, отн. ед.	предложенного алгоритма поиска, отн. ед.
$y^2 + xy = x^3 + 1$	2	10	2,1459	1
		15	5,6280	1,7683
$y^2 = x^3 - 52x + 100$	3	10	34,3741	30,1693
		15	136,7492	81,2948
$y^2 + y = x^3 - 79x + 342$	5	10	12508,3143	5724,5763
		15	98604,8883	33741,7067

Заключение

В работе проведено исследование применимости эллиптических кривых над рациональными числами в криптографии. Получены важные теоретические результаты – математическая задача, которую можно использовать при построении асимметричных криптографических схем, а также модель криптосистемы, использующей рассматриваемые кривые. Основная отличительная особенность таких схем — наличие на кривых над рациональным полем точек бесконечного порядка, позволяющих генерировать уникальные точки конечнопорожденной группы. Данная особенность открывает новые возможности для задач криптографии, учитывая ряд нерешенных проблем в области эллиптических кривых над рациональными числами. Отметим, что основной недостаток предложенных криптографических схем — размер секретного ключа достаточно велик по сравнению с современными криптосистемами, построенными на эллиптических кривых над конечными полями. В рамках дальнейших исследований планируется уменьшение размеров ключей, используя свойства эллиптических кривых и их рациональных точек.

Литература

1. Koblitz N., Menezes A., Vanstone S. The state of elliptic curve cryptography // Designs, Codes and Cryptography. 2000. V. 19. N 2-3. P. 173–193. https://doi.org/10.1023/A:1008354106356
2. Koblitz N. Elliptic curve cryptosystems // Mathematics of Computation. 1987. V. 48. N 177. P. 203–209. https://doi.org/10.1090/S0025-5718-1987-0866109-5
3. Washington L.C. Elliptic Curves: Number Theory and Cryptography. Chapman and Hall/CRC, 2008. 536 p.
4. Silverman J.H. The Arithmetic of Elliptic Curves. New York: Springer, 2009. 513 p. (Graduate Texts in Mathematics; V. 106).
5. Mordell L. On the rational solutions of the indeterminate equation of the third and fourth degree // Proceedings Cambridge Philosophical Society. 1922. V. 21. P. 179–192.
6. Weil A. L'arithmétique sur les courbes algébriques // Acta Mathematica. 1929. V. 52. N 1. P. 281–315. https://doi.org/10.1007/BF02592688
7. Silverman J.H. Heights and elliptic curves // Arithmetic Geometry. New York, NY: Springer, 1986. P. 253–265. https://doi.org/10.1007/978-1-4613-8655-1_10
8. Klagsbrun Z., Sherman T., Weigandt J. The Elkies curve has rank 28 subject only to GRH // Mathematics of Computation. 2019. V. 88. N 316. P. 837–846. https://doi.org/10.1090/mcom/3348
9. Menezes A.J., Van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. CRC press, 2018. 810 p.
10. Danzig T. Numbers: The Language of Science. Revised. Now York, Macmillan, 1933.
11. Mathews G.B. On the partition of numbers // Proceedings of the London Mathematical Society. 1896. V. 1. N 1. P. 486–490. https://doi.org/10.1112/plms/s1-28.1.486
12. Diffie W., Hellman M. New directions in cryptography // IEEE Transactions on Information Theory. 1976. V. 22. N 6. P. 644–654. https://doi.org/10.1109/TIT.1976.1055638
13. Noro K., Kobayashi K. Knapsack cryptosystem on elliptic curves // Cryptology ePrint Archive. 2009. P. 2009/091.

References

1. Koblitz N., Menezes A., Vanstone S. The state of elliptic curve cryptography. *Designs, Codes and Cryptography*, 2000, vol. 19, no. 2-3, pp. 173–193. https://doi.org/10.1023/A:1008354106356
2. Koblitz N. Elliptic curve cryptosystems. *Mathematics of Computation*, 1987, vol. 48, no. 177, pp. 203–209. https://doi.org/10.1090/S0025-5718-1987-0866109-5
3. Washington L.C. *Elliptic Curves: Number Theory and Cryptography*. Chapman and Hall/CRC, 2008, 536 p.
4. Silverman J.H. *The Arithmetic of Elliptic Curves*. New York, Springer, 2009, 513 p. Graduate Texts in Mathematics, vol. 106.
5. Mordell L. On the rational solutions of the indeterminate equation of the third and fourth degree. *Proceedings Cambridge Philosophical Society*, 1922, vol. 21, pp. 179–192.
6. Weil A. L'arithmétique sur les courbes algébriques. *Acta Mathematica*, 1929, vol. 52, no. 1, pp. 281–315. https://doi.org/10.1007/BF02592688
7. Silverman J.H. Heights and elliptic curves. *Arithmetic Geometry*. New York, NY, Springer, 1986, pp. 253–265. https://doi.org/10.1007/978-1-4613-8655-1_10
8. Klagsbrun Z., Sherman T., Weigandt J. The Elkies curve has rank 28 subject only to GRH. *Mathematics of Computation*, 2019, vol. 88, no. 316, pp. 837–846. https://doi.org/10.1090/mcom/3348
9. Menezes A.J., Van Oorschot P.C., Vanstone S.A. *Handbook of Applied Cryptography*. CRC press, 2018, 810 p.
10. Danzig T. *Numbers: The Language of Science. Revised*. Now York, Macmillan, 1933.
11. Mathews G.B. On the partition of numbers. *Proceedings of the London Mathematical Society*, 1896, vol. 1, no. 1, pp. 486–490. https://doi.org/10.1112/plms/s1-28.1.486
12. Diffie W., Hellman M. New directions in cryptography. *IEEE Transactions on Information Theory*, 1976, vol. 22, no. 6, pp. 644–654. https://doi.org/10.1109/TIT.1976.1055638
13. Noro K., Kobayashi K. Knapsack cryptosystem on elliptic curves. *Cryptology ePrint Archive*, 2009, pp. 2009/091.

14. Mazur B., Goldfeld D. Rational isogenies of prime degree // Inventiones Mathematicae. 1978. V. 44. N 2. P. 129–162. https://doi.org/10.1007/BF01390348
15. Lozano-Robledo Á. Elliptic curves, modular forms, and their L-functions // The Student Mathematical Library. 2011. V. 58. http://dx.doi.org/10.1090/stml/058

14. Mazur B., Goldfeld D. Rational isogenies of prime degree. *Inventiones Mathematicae*, 1978, vol. 44, no. 2, pp. 129–162. https://doi.org/10.1007/BF01390348
15. Lozano-Robledo Á. Elliptic curves, modular forms, and their L-functions. *The Student Mathematical Library*, 2011, vol. 58. http://dx.doi.org/10.1090/stml/058

Авторы

Давыдов Вадим Валерьевич — преподаватель, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57203909696, https://orcid.org/0000-0002-5544-2434, vvdavydov@itmo.ru
Дакуо Жан-Мишель Никодэмович — студент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, https://orcid.org/0000-0002-4084-8829, jeandakuo@itmo.ru
Иогансон Иван Дмитриевич — инженер, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, https://orcid.org/0000-0002-0856-2249, ivan.ioganson@itmo.ru
Хуцаева Алтана Феликсовна — инженер, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, https://orcid.org/0000-0001-5494-7142, afkhutsaeva@itmo.ru

Authors

Vadim V. Davydov — Lecturer, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 57203909696, https://orcid.org/0000-0002-5544-2434, vvdavydov@itmo.ru
Jean-Michelle N. Dakuo — Student, ITMO University, Saint Petersburg, 197101, Russian Federation, https://orcid.org/0000-0002-4084-8829, jeandakuo@itmo.ru
Ivan D. Ioganson — Engineer, ITMO University, Saint Petersburg, 197101, Russian Federation, https://orcid.org/0000-0002-0856-2249, ivan.ioganson@itmo.ru
Altana F. Khutsaeva — Engineer, ITMO University, Saint Petersburg, 197101, Russian Federation, https://orcid.org/0000-0001-5494-7142, afkhutsaeva@itmo.ru

Статья поступила в редакцию 14.04.2022
Одобрена после рецензирования 20.05.2022
Принята к печати 12.07.2022

Received 14.04.2022
Approved after reviewing 20.05.2022
Accepted 12.07.2022