УДК 004.94 Вестник УрФО № 2(52) / 2024, с. 99–105

Воробьев А. П., Кротова Е. Л., Воробьева Е. Ю.
DOI: 10.14529/secur240210

ПРЕИМУЩЕСТВА КРИПТОГРАФИИ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ ДЛЯ РЕШЕНИЯ ЗАДАЧ АУТЕНТИФИКАЦИИ

Цифровые технологии проникают во все сферы нашей жизни, поэтому крайне важным становится вопрос защиты информации и передачи данных. Для обеспечения безопасности, необходимо использовать современные методы криптографии. В данной статье рассматриваются эллиптические кривые, лежащие в основе таких методов, описаны их свойства и особенности выбора. Все более актуальной становится задача противостояния постоянно совершенствующимся злоумышленникам при растущих производительных мощностях при этом вычислительные ресурсы легального пользователя ограничены.

Ключевые слова: *криптография, эллиптические кривые, защита информации.*

Vorobev A. P., Krotova E. L., Vorobeva E. Yu.

ADVANTAGES OF ELLIPTIC CURVE CRYPTOGRAPHY FOR SOLVING AUTHENTICATION PROBLEMS

Digital technologies penetrate into all areas of our lives, so the issue of information protection and data transfer becomes extremely important. To ensure security, it is necessary to use modern cryptography methods. This article discusses the elliptic curves that underlie such methods, describing their properties and selection features. The task of confronting constantly improving attackers with growing production capacities is becoming increasingly urgent, while the computing resources of the legal user are limited.

Keywords: *cryptography, elliptic curves, information security.*

В современных технологиях информационной безопасности широко применяется математический аппарат, основанный на эллиптических кривых. Это связано с их универсальностью, эффективностью и высокой безопасностью [1]. Приведем лишь некоторые примеры областей, в которых он применяется:

Информационная безопасность: для защиты данных и информации в сетях передачи данных, в различных протоколах безопасности, в технологиях и системах аутентификации и авторизации.

Мобильные устройства: для обеспечения безопасности взаимодействий пользователей с приложениями, для шифрования данных и защиты личной информации.

Криптография: для построения современных криптографических методов, таких как эллиптический криптографический обмен ключами, цифровая подпись, блочные шифры.

Финансовые технологии: в различных алгоритмах шифрования платежей, электронных транзакций и других финансовых операций.

Блокчейн технологии: в криптовалютах, например, таких как Биткоин, для обеспечения безопасности транзакций, создания цифровых подписей и других криптографических операций.

Сетевая безопасность: для защиты сетей, обеспечения конфиденциальности данных и предотвращения несанкционированного доступа.

Интернет вещей (IoT): для эффективности и безопасности в устройствах с ограниченными вычислительными ресурсами.

Использование эллиптических кривых позволяет строить криптографические системы с более короткими длинами ключей, но получать при этом эквивалентный уровень безопасности по сравнению с другими методами [2]. Таким образом, криптография на эллиптических кривых может стать решением для устройств с ограниченными вычислительными ресурсами, например, такими как IoT [3].

Рассмотрим конечное поле F_p, характеристика которого $p > 3$.

Множество точек (x, y), координаты которых удовлетворяют уравнению:

$$y^2 + a_1 \cdot xy + a_3 \cdot y = x^3 + a_2 \cdot x^2 + a_4 \cdot x + a_5 \quad (1)$$

называется *эллиптической* кривой. Здесь a_1, a_2, a_3, a_4, a_5, – коэффициенты, принадлежащие полю F_p. В случае характеристики поля, отличной от 2 и 3, уравнение (1) с помощью, подходящей замены переменных может быть приведено к каноническому виду в форме Вейерштрасса:

$$E : y^2 = x^3 + ax + b \quad (2)$$

где $a, b \in F_p$. В качестве поля F_p выбирают чаще всего комплексные ($\mathbb{C}$) или действительные ($\mathbb{R}$) числа.

Наглядно можно представить эллиптические кривые E как линии пересечения поверхности $y^2 = x^3 + ax + b + z$ с плоскостями $z = const$ [4] (см. рис 1).

Эллиптические кривые, получаемые в таких сечениях, в отличие от конических, невозможно параметризировать рациональными функциями.

Свойства эллиптических кривых

1. Так как график кривой E симметричен относительно оси абсцисс, то найти точки пересечения графика с осью Ox можно, решив уравнение:

$$x^3 + ax + b = 0 \quad (3)$$

Для решения таких уравнений третьей степени можно использовать формулы Кардано с вычислением дискриминанта D, равного $E : \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2$. Известно, что при $D<0$ уравнение (3) имеет три различных действительных корня, при $D=0$ два различных (один кратный, кратности 2), а при $D>0$ один действительный и два комплексных сопряженных корня.

Эллиптическая кривая E, заданная уравнением (2), в случае $D=0$ называется сингу-

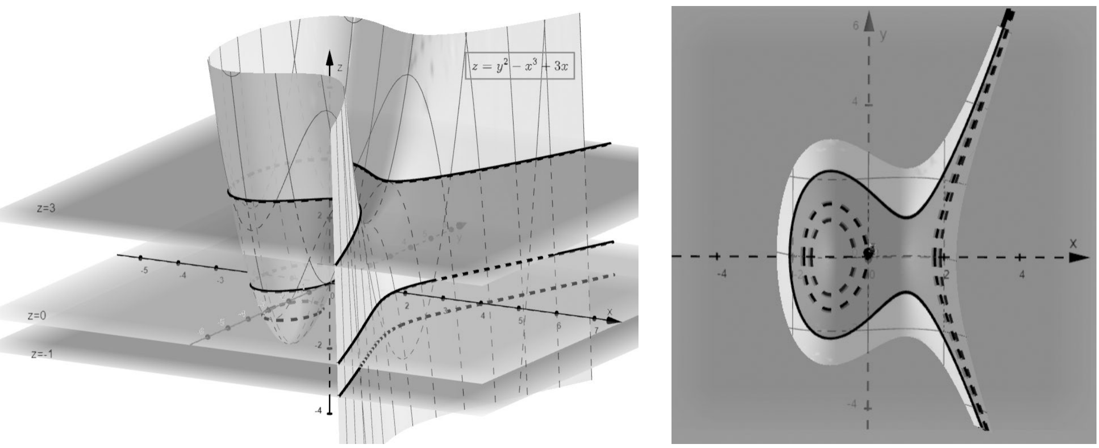

Рис. 1. Пересечение поверхности $z = y^2 - x^3 + 3x$ и плоскостей $z = -1,0,3$

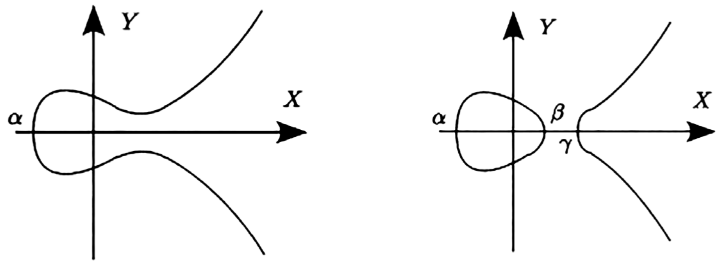

Рис. 2. Примеры несингулярных эллиптических кривых

лярной, а в случае $D \neq 0$ – несингулярной [2]. Нас будут интересовать несингулярные кривые, так как при сингулярности резко снижается криптостойкость алгоритмов. Таким образом, многочлен, стоящий в правой части уравнения (2), не имеет кратных корней и для его коэффициентов выполняется условие

$$\Delta(E) = 4a^3 + 27b^2 \neq 0 \quad (4)$$

$\Delta(E)$ называется дискриминантом кривой E.

Примеры несингулярных кривых изображены на рисунке 2.

Решения $(x,\ y)$ уравнения (2) называются афинными точками кривой E. Также в рассмотрение вводится еще одна точка, называемая точкой на бесконечности, и обозначаемая O (нейтральный, нулевой элемент) [5].

2. Введем операцию *сложения* точек на эллиптической кривой.

Отметим, что любая вертикальная прямая l, которая параллельна оси Oy, либо не пересекает кривую E, либо пересекает её дважды. Также, любая другая прямая l пересекает кривую E в одной или в трех точках. Точка касания считается двойным пересечением.

Итак, пусть Е – эллиптическая кривая, описываемая уравнением (2), и пусть некая прямая l пересекает Е в точках $P(x_1, y_1)$ и $Q(x_2, y_2)$. Тогда эта прямая пересечет кривую E в третьей точке, которую обозначим через $R'(x_3, -y_3)$, (см. рисунок 3). Суммой афинных точек P и Q назовем точку $R(x_3, y_3) = P + Q$, симметричную R' относительно оси Ox. Назовем ее обратной к точке R' и будем обозначать: $R = -R'$.

Если $P = Q$, то прямая l является касательной к кривой E (см. рисунок 3). Будем использовать обозначение: $R = P + P = [2]P$ – удвоение точки P.

В *особых* случаях, распространяя операцию сложения на бесконечно удаленную точку, определим ее так:

- Если l – вертикальная прямая, проходящая через точки P и $Q = -P$, то будем считать, что она пересекает кривую E в бесконечно удаленной точке O, т. е. $P + (-P) = O$.
- Если $P = O$ или $Q = O$, то получаем, что $P + O = P$ или $O + Q = Q$.

Итак,

1) Пусть $P \neq Q$, $P \neq -Q$, $P \neq O$, $Q \neq O$, $P + Q = -R' = R$. Определим координаты точки $R(x_3, y_3)$ [6,7].

Угловой коэффициент прямой l, проходящей через точки $P(x_1, y_1)$ и $Q(x_2, y_2)$, $k = \dfrac{y_2 - y_1}{x_2 - x_1}$.

Тогда уравнение прямой l имеет вид: $y = kx + \beta$, где $\beta = y_1 - kx_1$.

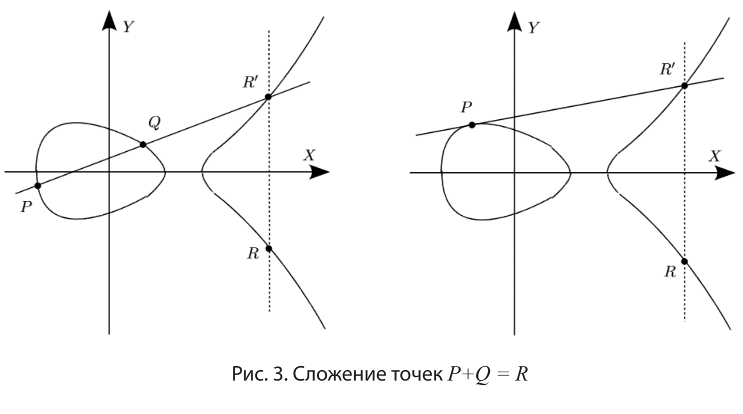

Рис. 3. Сложение точек $P+Q = R$

Точки пересечения прямой l с E являются решениями уравнения:

$$(kx+\beta)^2 - x^3 - ax - b = 0$$

или, учитывая, что оно имеет три различных действительных корня,

$$(kx+\beta)^2 - x^3 - ax - b = -(x-x_1)(x-x_2)(x-x_3) = 0$$

Приравнивая коэффициенты при одинаковых степенях x, получаем:

$$k^2 = x_1 + x_2 + x_3, \text{ откуда } x_3 = k^2 - x_1 - x_2.$$

С другой стороны, угловой коэффициент k может быть найден как $k = \frac{-y_3 - y_1}{x_3 - x_1}$, тогда имеем: $y_3 = k(x_1 - x_3) - y_1$.

Таким образом, координаты $R(x_3, y_3)$ определяются по формулам:

$$\begin{cases} x_3 = k^2 - x_1 - x_2 \\ y_3 = k(x_1 - x_3) - y_1 \end{cases} \quad (5)$$

2) Пусть $P = Q \neq O$, то есть $R = [2]P$.
Уравнение касательной к кривой $F(x, y) = 0$ в точке $P(x_1, y_1)$ имеет вид:

$$F'_x(P)\cdot(x - x_1) + F'_y(P)\cdot(y - y_1) = 0$$

Тогда угловой коэффициент k касательной определяется по формуле:

$$k = -\frac{F'_x(P)}{F'_y(P)}, \text{ если } F'_y(P) \neq 0.$$

Тогда получаем:

$$k = \frac{3x_1^2 + a}{2y_1} \quad (6)$$

Для определения координат точки $R(x_3, y_3)$ воспользуемся формулами (5) с угловым коэффициентом из (6):

$$\begin{cases} x_3 = k^2 - 2x_1 \\ y_3 = k(x_1 - x_3) - y_1 \end{cases} \quad (7)$$

Если же $F'_y(P) = 0$, то касательная является вертикальной прямой, $[2]P = O$.

<u>*Теорема:*</u> множество афинных точек кривой E, с нулевым элементом O, является аддитивной абелевой группой относительно операции сложения [5], при этом:

1) $P + Q = Q + P, \ \forall\, P, Q \in E$,

2) $P + (Q + S) = (P + Q) + S, \ \forall\, P, Q, S \in E$

3) $\exists$ нулевой элемент O, такой что $P + (-P) = O$,

4) $\forall\, P \in E \quad \exists$ обратный элемент $-P \in E$: $\ P + (-P) = O$.

Задача дискретного логарифмирования и выбор параметров эллиптической кривой

В указанных выше формулах (2-7) используются только операции сложения, вычитания, умножение и деления, поэтому при вычислениях с целыми числами по модулю простого числа p все тождества в уравнениях сохранятся, то есть мы находимся в поле вычетов по модулю p.

В результате уравнение (2) преобразуется в:

$$E : y^2 \equiv x^3 + ax + b \pmod p \qquad (8)$$

а ограничение (4) примет вид:

$$4a^3 + 27b^2 \neq 0 \pmod p \qquad (9)$$

Число $J(E) = 1728 \cdot \dfrac{4a^3}{4a^3 + 27b^2} \pmod p$ называется инвариантом эллиптической кривой.

Пусть кривая E определена над простым полем F_p и точка $P \in E(F_p)$, $P \neq O$.

n-кратным точки P назовем композицию (сумму):

$$[n]P = \underbrace{P + P + \ldots + P}_{n \text{ раз}}$$

Наименьшее натуральное число n такое, что $[n]P = O$, называется порядком P в группе $E(F_p)$. Количество точек кривой E будем обозначать N.

Для описания эллиптической кривой в национальном стандарте РФ (ГОСТ Р 34.10-2012) используются следующие параметры [8]:

p – простое число, модуль эллиптической кривой, $p>3$;

a, b – коэффициенты уравнения (8);

P – порождающая точка, или генератор точек кривой, точка большого порядка q. При $1 \leq m \leq q-1$ последовательность $\{[m]P\}$ задает все различные точки кривой, $[q]P = O$;

q – порядок точки P или порядок подгрупп; $2^{254} < q < 2^{256}$ или $2^{508} < q < 2^{512}$;

$h = \dfrac{N}{q}$ – кофактор кривой [9].

В криптографических системах используются кривые, количество точек которых является большим простым числом. В этом случае любая точка P является генератором всего множества точек. Порождающая точка используется для создания общего открытого ключа и для выполнения операций шифрования и расшифрования. Для безопасности криптосистемы при выборе точки необходимо, чтобы ее порядок был большим простым числом.

Для алгоритмов на эллиптических кривых используются подгруппы с высоким порядком, а значение кофактора h выбирается как можно меньше.

Коэффициенты a и b эллиптической кривой E по известному инварианту $J(E)$ определяются следующим образом:

$$\begin{cases} a \equiv 3k \pmod p \\ b \equiv 2k \pmod p \end{cases}$$

где $k \equiv \dfrac{J(E)}{1728 - J(E)} \pmod p$, $J(E) \neq 0$ или $J(E) \neq 0{,}1728$.

Задача состоит в нахождении такого числа m, что $[m]P = Q$ при известных P и Q. Такая задача называется задачей *дискретного логарифмирования* и является вычислительно крайне сложной, если тщательно выбирать параметры кривой; во всяком случае, на сегодняшний день не существует известного алгоритма решения такой задачи с полиномиальным временем [3].

Правильный выбор параметров эллиптической кривой для применения современных методов криптографии заслуживает особого внимания. Это поможет обеспечить высокий уровень безопасности данных и защитить их от возможных атак и утечек информации.

Основным достоинством криптосистем на основе эллиптических кривых является то, что они обеспечивают надежность, адекватную классическим криптосистемам RSA или Эль-Гамаля, на значительно меньших по длине ключах, а это существенно сокращает время кодирования и декодирования. Криптосистемы цифровой подписи на основе эллиптических кривых с длиной ключа 160 бит имеют одинаковую стойкость с криптосистемами DSA и Эль-Гемаля с длиной ключа 1024 бита. Электронная цифровая подпись – это эффективное средство защиты информации от модификации, которое переносит свойства реальной подписи под документом в область электронного документооборота. В основу ЭЦП положены такие криптографические методы, как асимметричное шифрование и хэш-функции.

Литература

1. Научные и методологические проблемы информационной безопасности (сборник статей). Под ред. В. П. Шерстюка. — М.: МЦНМО, 2004. — 208 с.

2. Рябко, Б. Я. Криптографические методы защиты информации: учеб. пособие / Б. Я. Рябко, А. Н. Фионов. — 2-е изд., стер. — М.: Горячая линия – Телеком, 2012. — 229 с.

3. Калхиташвили Д. Ш. Операционные системы интернета вещей: возможности, проблемы и решения / Д. Ш. Калхиташвили — Москва: РАНХиГС, 2023. — 5 с.

4. How Elliptic Curve Cryptography Works. [Электронный ресурс]: https://allaboutcircuits.com/technical-articleles/ elliptic-curve-cryptography-in-embedded-systems/

5. Жданов, О. Н. Применение эллиптических кривых в криптографии: учеб. пособие / О. Н. Жданов, Т. А. Чалкин. — Красноярск: СибГАУ, 2011 - 65 с.

6. Эллиптическая криптография: теория/ [Электронный ресурс]: https://habr.com/ru/articles/188958/

7. Elliptic Curve Cryptography: finite fields and discrete logarithms [Электронный ресурс]: https://andrea.corbellini.name/2015/05/23/elliptic-curve-cryptography-finite-fields-and-discrete-logarithms/

8. Национальный стандарт Российской Федерации. Криптографическая защита информации. [Электронный ресурс]: https://www.altell.ru/legislation/standards/gost-34.10-2012.pdf

9. Chandrasekhara, K.R. Elliptic Curve based authenticated session Key establishment protocol for High Security Applications in Constrained Network environment / K.R. Chandrasekhara, M.P. Pillai1 and Sebastian, 2010. [Электронный ресурс]: http://www.arxiv.org/pdf/1202.1895

References

1. Nauchnye i metodologicheskie problemy informacionnoj bezopasnosti (sbornik statej). Pod red. V. P. Sherstjuka. — M.: MCNMO, 2004. — 208 s.

2. Rjabko, B. Ja. Kriptograficheskie metody zashhity informacii: ucheb. posobie / B. Ja. Rjabko, A. N. Fionov. — 2-e izd., ster. — M.: Gorjachaja linija – Telekom, 2012. — 229 s.

3. Kalhitashvili D. Sh. Operacionnye sistemy interneta veshhej: vozmozhnosti, problemy i reshenija / D. Sh. Kalhitashvili — Moskva: RANHiGS, 2023. — 5 s.

4. How Elliptic Curve Cryptography Works. [Электронный ресурс]: https://allaboutcircuits.com/technical-articleles/ elliptic-curve-cryptography-in-embedded-systems/

5. Zhdanov, O. N. Primenenie jellipticheskih krivyh v kriptografii: ucheb. posobie / O. N. Zhdanov, T. A. Chalkin. — Krasnojarsk: SibGAU, 2011 - 65 s.

6. Jellipticheskaja kriptografija: teorija/ [Jelektronnyj resurs]: https://habr.com/ru/articles/188958/

7. Elliptic Curve Cryptography: finite fields and discrete logarithms [Электронный ресурс]: https://andrea.corbellini.name/2015/05/23/elliptic-curve-cryptography-finite-fields-and-discrete-logarithms/

8. Nacional'nyj standart Rossijskoj Federacii. Kriptograficheskaja zashhita informacii. [Jelektronnyj resurs]: https://www.altell.ru/legislation/standards/gost-34.10-2012.pdf

9. Chandrasekhara, K.R. “Elliptic Curve based authenticated session Key establishment protocol for High Security Applications in Constrained Network environment” / K.R. Chandrasekhara, M.P. Pillai1 and Sebastian, 2010. [Jelektronnyj resurs]: http://www.arxiv.org/pdf/1202.1895

ВОРОБЬЕВ Артем Павлович, студент, кафедра Технология твердых химических веществ Казанского национального исследовательского технологического университета. 420015, Республика Татарстан, Казань, ул. Карла Маркса, 68. E-mail: drsleepwalker@yandex.ru

КРОТОВА Елена Львовна, кандидат физико-математических наук, доцент, кафедра Высшей математики, Пермский национальный исследовательский политехнический университет. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: lenkakrotova@yandex.ru

ВОРОБЬЕВА Елена Юрьевна, старший преподаватель, кафедра Прикладной математики, Пермский национальный исследовательский политехнический университет. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: lena-vorobey@yandex.ru

VOROBEV Artem Pavlovich, student, Department of Solid Chemical Substances Technology, Kazan National Research Technological University. 420015, Republic of Tatarstan, Kazan, Karl Marx St., 68. Email: drsleepwalker@yandex.ru

KROTOVA Elena Lvovna, Candidate of Physical and Mathematical Sciences, Associate Professor, Department of Higher Mathematics, Perm National Research Polytechnic University. 614990, Perm Krai, Perm, Komsomolsky Prospekt, 29. Email: lenkakrotova@yandex.ru

VOROBEVA Elena Yuryevna, Senior Lecturer, Department of Applied Mathematics, Perm National Research Polytechnic University. 614990, Perm Krai, Perm, Komsomolsky Prospekt, 29. Email: lena-vorobey@yandex.ru