



ГРУППА
КОМПАНИЙ
«СПБ»



ЗАЩИЩЕННЫЕ
ТЕЛЕКОММУНИКАЦИОННЫЕ
СИСТЕМЫ

02 июня 2026 г.
CTCrypt2026

Обзор методов решения задачи дискретного логарифмирования в группе точек эллиптической кривой

к 25-летию принятия стандарта ГОСТ Р 34.10-2001

Алексей Нестеренко

anesterenko@hse.ru (<https://www.hse.ru/org/persons/47634770>)



Стандарты и рекомендации

ГОСТ Р 34.10 - 2001¹ (2012, 2018) Процессы формирования и проверки электронной цифровой подписи.

2016 г.	Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования
2017 г.	Схемы выработки общего ключа с аутентификацией на основе открытого ключа
2018 г.	Задание параметров алгоритмов электронной подписи и функции хэширования в профиле EMV сертификатов открытых ключей платежных систем
2019 г.	Параметры эллиптических кривых для алгоритмов и протоколов
2020 г.	Использование российских криптографических алгоритмов в протоколе TLS 1.2
2022 г.	Использование ГОСТ Р 34.10–2012 в инфраструктуре открытых ключей X.509
2023 г.	Использование российских криптографических алгоритмов в протоколе IKEv2
2025 г.	Схема формирования и проверки кода проверки

В Республике Беларусь: стандарт СТБ 34.101.45-2013 «Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых».

¹Постановление Госстандарта РФ от 12.09.2001 №380-ст о принятии ГОСТ Р 34.10-2001 взамен ГОСТ Р 34.10-94 с датой введения в действие с 1 июля 2002 года.



Постановка задачи

Эллиптическая кривая в короткой форме Вейерштрасса

Определение

Пусть $\mathbb{K}$ – произвольное поле, $\text{char} \mathbb{K} \neq 2, 3$. Пусть $a, b \in \mathbb{K}$ такие, что $4a^3 + 27b^2 \neq 0$. Рассмотрим однородное уравнение

$$\mathcal{E}(\mathbb{K}) : Y^2Z = X^3 + aXZ^2 + bZ^3. \quad (1)$$

Множество точек проективного пространства $\mathbb{P}^2(\mathbb{F}) = \{(X : Y : Z)\}$, удовлетворяющих равенству (1) называется эллиптической кривой в короткой форме Вейерштрасса. Точку $(0 : 1 : 0)$ называют бесконечно удаленной точкой $\mathcal{O}$.

Множество точек образует коммутативную группу относительно операции сложения.

Отображение $\varphi : (X : Y : Z) \rightarrow (x, y)$

$$x = \frac{X}{Z}, \quad y = \frac{Y}{Z}, \quad Z \neq 0$$

позволяет записать аффинную форму кривой

$$y^2 \equiv x^3 + ax + b. \quad (2)$$



Постановка задачи

Задача дискретного логарифмирования для эллиптической кривой над полем $\mathbb{F}_p$

Определение

Пусть $P \in \mathcal{E}(\mathbb{K})$ произвольная точка эллиптической кривой порядка q . Точка $Q \in \mathcal{E}(\mathbb{K})$ называется точкой кратности $k \in \mathbb{N}$, если

$$Q = [k]P = \underbrace{P + \dots + P}_{k \text{ раз}}. \quad (3)$$

Задача определения неизвестного значения k по известным точкам P, Q называется задачей дискретного логарифмирования в группе точек эллиптической кривой $\mathcal{E}(\mathbb{K})$.

Теорема (Хассе)

Пусть $p > 3$ простое число. Тогда порядок m группы точек эллиптической кривой $\mathcal{E}(\mathbb{F}_p)$ удовлетворяет неравенству $m = p + 1 + t$, где $|t| < 2\sqrt{p}$.

Группа точек $\mathcal{E}(\mathbb{F}_p)$ конечна, а каждая точка имеет порядок q такой, что $q|m$.



Действующие ограничения на параметры кривой

согласно ГОСТ Р 34.10-2012 и СТБ 34.101.45-2013

Эллиптическая кривая $\mathcal{E}(\mathbb{F}_p)$: $y^2 \equiv x^3 + ax + b \pmod{p}$, $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$.

	СТБ 34.101.45-2013	ГОСТ Р 34.10-2012
l	$l \in \{128, 192, 256\}$	$l \in \{128, 256\}$
p	$2^{2l-1} < p < 2^{2l}$ $p \equiv 3 \pmod{4}$	нечетное простое
a, b	$a \not\equiv 0 \pmod{p}$ $\left(\frac{b}{p}\right) = 1$	$ab \not\equiv 0 \pmod{p}$
q	$q = m = \mathcal{E}(\mathbb{F}_p) $ $q \neq p$ $2^{2l-1} < q < 2^{2l}$	$q m = \mathcal{E}(\mathbb{F}_p)$, $cq = m$ $m \neq p$ $2^{2(l - \frac{l}{128})} < q < 2^{2l}$
$p^t \not\equiv 1 \pmod{q}$ $t = 1, \dots, B$	$B = 50$	$B_{l=128} = 31$ $B_{l=256} = 131$
$P, \text{ord}(P) = q$	$P = (0, y_P)$ $y_P \equiv b^{\frac{b+1}{4}} \pmod{p}$	случайна

Здесь l – уровень стойкости согласно СТБ 34.101.45-2013.



Прежде, чем начать

Предыдущие обзорные работы

- 1998 – Blake I., Seroussi G. Smart N. Elliptic Curves In Cryptology
- 2006 – Cohen H., H. Frey. Handbook of Elliptic and Hyperelliptic Curve Cryptography
- 2016 – Galbraith S. Gaudry P. Recent progress on the elliptic curve discrete logarithm problem
- 2025 – Hankerson D., Menezes A. Elliptic Curve Discrete Logarithm Problem в книге «Encyclopedia of Cryptography, Security and Privacy» (3е издание)



1. Универсальные методы

- Сведение к подгруппе простого порядка
- ρ -метод Полларда
- λ -метод Полларда
- Универсальные методы с ограничениями
- Теоретические результаты о минимальной сложности
- Рекорды



Сведение к подгруппе простого порядка

Метод согласования

Метод согласования найден² А.О. Гельфондом в 1962 г.

Неизвестное k ищется в виде

$$k = k_1 + k_2 h, \quad \text{где } h = \lceil \sqrt{m} \rceil \quad \text{и} \quad 0 \leq k_1, k_2 < h.$$

Тогда равенство $Q = [k]P$ принимает вид

$$Q - [k_1]P = [k_2]S, \quad \text{где } S = [h]P \in \mathcal{E}(\mathbb{F}_p), \quad (4)$$

Алгоритм: определить последовательности точек

$$\begin{aligned} Q_0 &= Q, & Q_{k_1} &= Q_{k_1-1} - P, & k_1 &= 1, 2, \dots, h-1, \\ R_0 &= \mathcal{O}, & R_{k_2} &= R_{k_2-1} + S, & k_2 &= 1, 2, \dots, h-1, \end{aligned}$$

найти совпадение $Q_{k_1} = R_{k_2}$ и определить k_1 и k_2 .

Память метода: h точек $Q_0, \dots, Q_{h-1}$. Трудоемкость метода: $\frac{3}{2} \lceil \sqrt{m} \rceil$ (в среднем).

Независимо предложен³ Д. Шенксом в 1971 г. (метод «больших и малых шагов»).

²Нечаев В.И. Элементы криптографии. М.:Высшая школа, 1999. 109 стр.

³Shanks D. Class number, a theory of factorization and genera // Proceedings Of Symposium Pure Mathematics. Providence, R.I., AMS. 1971. V. 20. pp. 415–440.



Сведение к подгруппе простого порядка

Метод В.И.Нечаева

Идея⁴ В.И.Нечаева, 1965 г.

Пусть $m = \prod_{i=1}^n q_i$ и $\text{НОД}(q_i, q_j) = 1$ для всех $i \neq j$, $n \in \mathbb{N}$. Тогда

$$\begin{cases} k \equiv k_1 \pmod{q_1}, \\ k \equiv k_2 \pmod{q_2}, \\ \dots \\ k \equiv k_n \pmod{q_n}, \end{cases}$$

в которой величины $k_i \in \mathbb{Z}_{q_i}$, $i = 1, \dots, n$ удовлетворяют равенствам

$$\left[\frac{m}{q_i} \right] Q = [k_i] S_i, \quad \text{где} \quad S_i = [q_i] P, \quad i = 1, \dots, n$$

Трудоёмкость решения исходной задачи $Q = [k]P$, в среднем, оценивается величиной

$$\frac{3}{2} \left(\sum_{i=1}^n \lceil \sqrt{q_i} \rceil \right).$$

⁴Нечаев В.И. Элементы криптографии. М.:Высшая школа, 1999. 109 стр.



Сведение к подгруппе простого порядка

Метод Поллига-Хеллмана⁵

Отдельно рассматривается случай $m = q^n$, где q – простое число.

Идея метода заключается в представлении k в виде

$$k = k_0 + k_1 q + k_2 q^2 + \dots + k_{n-1} q^{n-1} = \sum_{i=0}^{n-1} k_i q^i,$$

где величины $k_i \in \mathbb{F}_q$ и удовлетворяют равенствам

$$\begin{aligned} [q^{n-1}]Q &= [k_0]S, \\ [q^{n-2}](Q - [k_0]P) &= [k_1]S, \\ &\dots \\ [q^{n-1-i}]\left(Q - \left[\sum_{j=0}^{i-1} k_j q^j\right]P\right) &= [k_i]S, \quad \text{где } S = [q^{n-1}]P, \quad i = 1, \dots, n-1. \end{aligned}$$

Среди авторов, которые независимо предложили тот же алгоритм: Сильвер (R. Silver) и, немного позднее, Шрёппель (R. Schroepel) и Блок (H. Block).

⁵Pohlig S.C, Hellman M.E. An improved algorithm for computing logarithms over $GF(p)$ and its Cryptographic significance // IEEE. Trans. Information Theory. 1978. V. 24. pp. 106–110.



ρ -метод Полларда

Идея метода

Предложен⁶ Дж. Поллардом в 1978 году и основан на свойствах случайного отображения f подгруппы $\langle P \rangle = \{O, P, [2]P, \dots, [q-1]P\}$ в себя.

Пусть $h \in \mathbb{N}$. Рассмотрим случайное отображение $f: \langle P \rangle \rightarrow \langle P \rangle \subset \mathcal{E}(\mathbb{F}_p)$

$$f(R) = R + S_i, \quad \text{где } i \equiv x(R) \pmod{h},$$

$$S_i = [\gamma_i]P + [\omega_i]Q, \quad i = 0, \dots, h-1, \quad S_i \in \langle P \rangle, \gamma_i, \omega_i \in \mathbb{F}_q^*.$$

1. Выберем случайное значение γ_0 и построим последовательность точек $\{R_n\}_{n=0}^\infty$,

$$R_0 = [\gamma_0]P, \quad R_1 = f(R_0), \quad \dots, \quad R_{n+1} = f(R_n), \quad \dots$$

2. Поскольку $\langle P \rangle$ конечна и имеет порядок q , следовательно, найдется $\tau \in \mathbb{N}$, индексы $r, s \in \mathbb{N}$ такие, что $s > r$, $\tau | (s - r)$ и

$$[\alpha_r]P + [\beta_r]Q = R_r = R_s = [\alpha_s]P + [\beta_s]Q. \quad (5)$$

3. Определяем $k \equiv \frac{\alpha_r - \alpha_s}{\beta_s - \beta_r} \pmod{q}$.

⁶Pollard J.M. Monte Carlo methods for index computation (mod p) // Mathematics Of Computation. 1978. V. 32. № 143. pp. 918–924.



ρ -метод Полларда

Оптимизации и варианты

- Э.Теске⁷ в 2000 г. $h = \lceil \log_2 q \rceil$ (при малых значениях h нарушается свойство случайности отображения f),
- Способы поиска цикла⁸:

Автор	Память	Точное значение τ	Сложность
Флойд, 1965 г.	2 точки	нет	$\lambda + 2\tau$
Брент, 1969 г.	2 точки	нет	
Госпер, 1972 г.	$\lceil \log_2 q \rceil$	да	
Ниваш, 2004 г.	определяется вероятностью успеха	да	

- Использование автоморфизма $\pi : (x, y) \rightarrow -(x, y) = (x, -y)$ (существует всегда).
 $y^2 \equiv x^3 + ax \pmod{p}$ имеет $\pi_4 : (x, y) \rightarrow (x, \zeta_4 y)$ порядка 4, а $y^2 \equiv x^3 + b \pmod{p}$ имеет $\pi_3 : (x, y) \rightarrow (x, \zeta_3 y)$ порядка 6, где ζ_3, ζ_4 отличные от 1, -1 корни из 1 степени 3 и 4.

⁷Teske E. On Random Walks For Pollard's Rho Method // Mathematics of Computation. 2000. Vol. 70. pp. 809–825.

⁸Нестеренко А.Ю. Алгоритмы поиска длин циклов в последовательностях и их приложения // Фундаментальная и прикладная математика. 2010. Т. 16. № 6. стр. 109–122.



Оценка сложности сводится к определению значений математического ожидания $E_q(\lambda, f)$ и $E_q(\tau, f)$ для λ – длины подхода к циклу и τ – длины цикла, соответственно, при случайном выборе отображения f . Хорошо известно⁹, что

$$\lim_{q \rightarrow \infty} \frac{E_q(\lambda, f)}{\sqrt{q}} = \lim_{q \rightarrow \infty} \frac{E_q(\tau, f)}{\sqrt{q}} = \sqrt{\frac{\pi}{8}}.$$

Тогда, для эллиптических кривых таких, что $ab \not\equiv 0 \pmod{p}$, ρ -метод Полларда реализуется на множестве из $\frac{q-1}{2}$ классов (исключается точка $\mathcal{O}$), имеет трудоемкость, оцениваемую, в среднем, величиной

$$\sqrt{\frac{\pi(q-1)}{2}} = \frac{1}{2} \sqrt{\pi(q-1)}$$

и использует память, необходимую для хранения $2\lceil \log_2 q \rceil$ точек подгруппы $\langle P \rangle$.

⁹Flajolet P., Odlyzko A.M. Random mapping statistics // Advances in Cryptology: Proc. Eurocrypt'89. 1990. pp. 329–354.



Используется то же случайное отображение f , что и в ρ -методе Полларда.

1. Выбирается $\gamma_0 \in \mathbb{F}_q$ и строится посл-ть $R_{1,0} = [\gamma_0]P$, $R_{1,n+1} = f(R_{1,n})$.
2. Выбирается $\omega_0 \in \mathbb{F}_q$ и строится посл-ть $R_{2,0} = [\omega_0]P$, $R_{2,n+1} = f(R_{2,n})$.
3. Для некоторого $N \in \mathbb{N}$ ищется пересечение $R_{1,r} = R_{2,s}$ для всех $1 \leq r, s \leq N$.

Наивный способ пересечения памяти для хранения N точек эллиптической кривой, что делает его неприменимым на практике.



λ -метод Полларда

Метод параллельного поиска коллизий (метод выделенных точек)

Предложен¹⁰ ван Ооршотом и Винером в 1999 г. Действует на классах точек, порождаемых $\pi : (x, y) \rightarrow -(x, y) = (x, -y)$.

1. Выберем $w \in \mathbb{N}$, зафиксируем множество выделенных точек

$$M = \{R \in \mathcal{E}(\mathbb{F}_p) : x(R) \equiv 0 \pmod{2^w}\} \subset \mathcal{E}(\mathbb{F}_p), \quad |M| \sim \frac{1}{2^w} \cdot \frac{(q-1)}{2} = \frac{q-1}{2^{w+1}}.$$

и положим $L = \emptyset \subset M$ (L - множество найденных выделенных точек).

2. Рассмотрим $1 \leq r \leq 2^w$ параллельно работающих вычислителей, вычисляющих

$$R_{i,0} = [\gamma_i]P, \quad R_{i,n+1} = f(R_{i,n}), \quad \gamma_i \in \mathbb{F}_p^*.$$

3. Если $R_{i,n} \in M$, то ищется совпадение с $R_{i,n}$ в L .

3.1 Если совпадение не найдено, то точка $R_{i,n}$ добавляется в L .

3.2 Если совпадение найдено, то выполнено равенство $R_{i,n} = R_{j,s}$, которое позволяет найти неизвестное k аналогично ρ -методу Полларда.

¹⁰van Oorschot P.C., Wiener M.J. Parallel Collision Search with Cryptanalytic Applications // Journal of Cryptology. 1999. V. 12. pp. 1–28.



Кратко:

1. Для одного вычислительного средства $P(R_{i,n} \in M) = \frac{1}{2^w}$ и для r средств $P(R_{i,n} \in M) = \frac{r}{2^w}$, сл-но, для поиска одной выделенной точки требуется $\frac{2^w}{r}$ шагов.
2. Для поиска коллизии в M (с вероятностью более $\frac{1}{2}$) необходимо выполнить

$$\frac{2^w}{r} \sqrt{\frac{\pi}{2} |M|} = \frac{1}{2r} \sqrt{\pi(q-1)2^w}$$

3. Суммарная сложность по всем r вычислительным средствам $\sqrt{\pi(q-1)2^{w-2}}$.

Идея выбора множества M (П.А. Лебедев, 2018 г., неопубликовано). Для фиксированной точки $R_{i,n}$

$$R_{i,n} = R_{i,n-1} + S_j, \quad \text{где } j \equiv x(R_{i,n-1}) \pmod{h}, \quad i = 1, \dots, r,$$

опробовать $S_1, \dots, S_r$ и выбирать в M те, для которых указанное равенство выполняется более, чем для 2-х индексов j .

(Множество M существенно зависит от f и состоит из точек, которые заведомо принадлежат нескольким орбитам отображения f).



Теорема

Пусть M произвольное конечное подмножество в $\langle P \rangle$ такое, что ему принадлежат точки P и $Q = [k]P$. Обозначим $|M| = r$. Если найдутся эффективно вычислимые отображения

$$f: \mathbb{Z}_r \rightarrow M, \quad g: \mathbb{Z}_r \rightarrow \mathbb{F}_q$$

такие, что

1. $f(i) \neq f(j)$ при $i \neq j \in \mathbb{Z}_r$,
2. $f(i) = [g(i)]P$,

то найдется алгоритм, вычисляющий k со сложностью не более $2T_f\sqrt{r}$, где T_f сложность вычисления f .

В доказательстве применяется метод согласования.

¹¹Нестеренко А.Ю. Математические методы обеспечения защищенного взаимодействия средств защиты информации. Дисс. на соиск. д.ф.-м.н., МГУ им. М.В. Ломоносова, 2023.



Универсальные методы с ограничениями

Примеры

Наиболее известные примеры:

1. известен диапазон значений¹² неизвестного $A < k < B$,
2. известен мультипликативный порядок^{13 14} неизвестного $d = \text{ord}_q(k)$.
3. (возможно существуют еще)

Применимы методы

- согласования,
- ρ -Полларда,
- метод выделенных точек (в англ. литературе, метод Метод Гадри-Шоста^{15 16})

¹²Pollard J.M. Monte Carlo methods for index computation (mod p) // Math. Of Comp. 1978 (32).

¹³Cheon J.H. Security analysis of the strong Diffie-Hellman problem // EUROCRYPT 2006. pp. 1–11.

¹⁴Nesterenko A.Yu. Some remarks on the elliptic curve discrete logarithm problem // Матем. вопр. крипто. 2016 (2), стр. 115–120.

¹⁵Gaudry, P., Schost, E. A low-memory parallel version of Matsuo, Chao, and Tsujii's algorithm ANTS-2004 (2004).

¹⁶Galbraith S., Pollard J., Ruprai R., Computing discrete logarithms in an interval // Math. of Comp.



Теоретические результаты о минимальной сложности

Теорема В.И. Нечаева. Точные оценки

В 1994 г. для произвольной абелевой группы В.И. Нечаев рассмотрел¹⁷ модель вычислителя с доступными операциями:

- групповая операция,
- операция сравнения (сложность не учитывается)

Теорема

Пусть q нечетное простое число. Оптимальный алгоритм поиска неизвестного значения $k \in \mathbb{Z}_q$ удовлетворяющего равенству $Q = [k]P$ обладает сложностью не менее, чем $\sqrt{2(q-1)}$. При этом, объем используемой им памяти не менее $\frac{1}{2}\sqrt{m}$, где m – порядок группы точек эллиптической кривой $\mathcal{E}(\mathbb{F}_p)$.

Доказательство теоремы использует аппарат нормально ориентированных деревьев.

¹⁷В.И.Нечаев, “К вопросу о сложности детерминированного алгоритма для дискретного логарифма”, Матем. заметки, 55:2 (1994), 91–101.



Теоретические результаты о минимальной сложности

Теорема В. Шупа. Асимптотические оценки

В 1997 г. В. Шуп¹⁸ и, годом позднее, У. Маурер и Ш. Вольф¹⁹ расширили модель В.И. Нечаева. Пусть $\sigma : \mathcal{E}(\mathbb{F}_p) \rightarrow \mathbb{V}_{2^s}$ инъекция, т.ч. $m \leq 2^s$. Вычислителю доступны следующие операции:

- получение $\sigma(\mathcal{O})$,
- для $\sigma(P)$ возврат значения $\sigma(-P)$,
- групповая операция: для $\sigma(P_1), \sigma(P_2)$ возврат значения $\sigma(P_1 + P_2)$,
- возврат $\sigma(P)$ для случайной, равномерно распределенной на $\mathcal{E}(\mathbb{F}_p)$ точки P .

Теорема

Пусть $q \rightarrow \infty$. Тогда оптимальный вероятностный алгоритм поиска неизвестного значения $k \in \mathbb{Z}_q$ удовлетворяющего равенству $Q = [k]P$ обладает сложностью $T = \Omega(\sqrt{q})$, т.е. найдутся константы q_0 и C_0 такие, что для всех $q > q_0$ будет выполнено неравенство $T \geq C_0 \sqrt{q}$.

¹⁸Shoup, V., Lower bounds for discrete logarithms and related problems, EUROCRYPT'97, 1997.

¹⁹Maurer, U., Wolf, S. Lower bounds on generic algorithms in groups. EUROCRYPT'98. 1998.



Для кривых над полем $\mathbb{F}_{2^n}$:

Автор	Год	$\log_2 q$	n	Время
D. Bernstein etc. ²⁰	2016	117	127	200 дн.

Для кривых над полем $\mathbb{F}_p$:

$$p^* = 11957518425389075254535992784167879$$

Автор	Год	Кривая	$\log_2 q$	p	Время
T. Kusaka etc. ²¹	2017	$y^2 = x^3 + 3$ (с автоморфизмами)	114	p^*	81 дн.
J. Bos etc. ²²	2009	общий вид	112	$\frac{2^{128}-3}{11 \cdot 6949}$	180 дн.

Использовался метод параллельного поиска коллизий.

²⁰Bernstein D., Engles S., Lange T., Niederhagen R., Paar C., Schwabe P., Zimmermann R., Faster elliptic curve discrete logarithms on FPGAs, eprint Archive, 2016/382, 2016.

²¹Kusaka T., Joichi S., Ikuta K., Khandaker A., Nogami Y., Uehara S., Yamai N., Solving 114-bit ECDLP for a Barreto–Naehrig curve, Information Security and Cryptology – ICISC 2017, 2018, 231–244.

²²Bos J., Kaihara M., Kleinjung T., Lenstra A.K. Montgomery P., PlayStation 3 computing breaks 260 barrier, 112-bit ECDLP solved, EPFL Laboratory for Cryptologic Algorithms, 2009.



Алгоритмическая идея поиска: найти совпадающие значения функции $f(x_1, x_2) = [x_1]P + [x_2]Q$, у которой есть два периода (обзор и литература²³):

1. $f(x_1 + q, x_2) = [x_1 + q]P + [x_2]Q = f(x_1, x_2)$,
2. $f(x_1 + k, x_2 - 1) = [x_1 + k]P + [x_2 - 1]Q = [x_1]P + Q + [x_2 - 1]Q = f(x_1, x_2)$.

Для сравнения квантовые вычислители:

Автор	Год	$\log_2 q$	Время
S. Tappeconnic ²⁴	2025	6	
G. Lelli ²⁴	2026	15	45 мин.

²³Денисенко Д. Пример применения квантового алгоритма Шора для решения задачи дискретного логарифмирования в группе точек эллиптической кривой над конечным простым полем, РусКрипто25, 2025.

²⁴<https://www.mexc.io/news/1052339>



Методы логарифмирования на кривых, не удовлетворяющих ГОСТ Р 34.10-2001

- Аномальные кривые
- Сведение к конечному расширению поля
- Эллиптические кривые, определённые над $\mathbb{F}_{2^n}$ и $\mathbb{F}_{p^n}$



Определение

Эллиптическая кривая $\mathcal{E}(\mathbb{F}_p)$ называется аномальной, если $|\mathcal{E}(\mathbb{F}_p)| = m = p$.

Обозначим $\mathbb{Q}_p = \{x = \sum_{i=-k}^{\infty} a_i p^i\}$ поле p -адических чисел, $\mathbb{Z}_p$ кольцо целых p -адических чисел и $\pi : \mathcal{E}(\mathbb{Q}_p) \rightarrow \mathcal{E}(\mathbb{F}_p)$ - редукция по модулю p .

1. Точки $P, Q \in \mathcal{E}(\mathbb{F}_p)$ поднимаются до точек $\tilde{P}, \tilde{Q} \in \mathcal{E}(\mathbb{Q}_p)$ так, что $\tilde{P}, \tilde{Q} \in E_1(\mathbb{Q}_p)$, где $\forall S \in E_1(\mathbb{Q}_p)$ выполнено $\pi(S) = \mathcal{O} \in \mathcal{E}$, например

$$P(x, y) \longrightarrow (x + \alpha p, y + \beta p) \xrightarrow{[p]} \tilde{P}, \quad \alpha, \beta \in \{1, \dots, p-1\}.$$

2. Вычисляются эллиптические логарифмы $u = \log_E(\tilde{P}), v = \log_E(\tilde{Q})$, где $u, v \in p\mathbb{Z}_p$ и выполнено равенство $v = ku$, из которого находится k .

²⁵ Satoh T., Araki K., Fermat quotients and the polynomial time discrete log algorithm for anomalous curves // Comm. Math. University Sancti Pauli, 1998 (47), 81–92.

²⁶ Smart N., The discrete logarithm problem on elliptic curves of trace one // Journal of Cryptology, 1999 (12) 193–196.

²⁷ Semaev I. Evaluation of discrete logarithms in a group of p -torsion points of an elliptic curve in characteristic p // Math. Of Comp. V.67. 1998 (221), 353–356.



Сведение к конечному расширению поля $\mathbb{F}_p$

MOV-алгоритм²⁸ и работа И.А. Семаева²⁹

1. Определить t - порядок p по модулю q (существует всегда, $t|p(q) = q - 1$).
2. Поднять $P, Q \in \mathcal{E}(\mathbb{F}_p)$ на кривую $\mathcal{E}(\mathbb{F}_{q^t})$.
3. Найти точку $T \in \mathcal{E}[q](\mathbb{F}_{q^t})$ в группа кручения порядка q , т.е. $[q]T = \mathcal{O}$.
4. Используя спаривание Вейля

$$e_q(T, \cdot) : \mathcal{E}[q](\mathbb{F}_{q^t}) \times \mathcal{E}[q](\mathbb{F}_{q^t}) \rightarrow \mu_q \in \mathbb{F}_{q^t}^\times$$

отобразить точки P, Q в элементы ζ_P, ζ_Q группы корней из единицы степени q .

5. Решить задачу дискретного логарифмирования $(\zeta_P)^k = \zeta_Q$.

²⁸Menezes A., Vanstone S., Okamoto T. Reducing elliptic curve logarithms to logarithms in a finite field // Proc. 23rd ACM Symp. Theory of Computing. 1991. pp. 80–89.

²⁹И. А. Семаев, "К вопросу о сведении вычисления дискретных логарифмов на эллиптической кривой к вычислению дискретных логарифмов в конечном поле" // Дискрет. матем., 11:3 (1999), 24–28.



Сведение к конечному расширению поля $\mathbb{F}_p$

Дополнения

- Способы эффективного вычисления спариваний Вейля^{30 31}.
- Связь с аномальными кривыми:
 - Алгебраический подход (работа Ж.Волоха³²)
 - Эллиптические сети³³ и их частный случай – эллиптические последовательности деления (elliptic divisibility sequences)³⁴

$$h_{n+m}h_{n-m}h_r^2 = h_{n+r}h_{n-r}h_m^2 - h_{m+r}h_{m-r}h_n^2, \quad n \geq m \geq r, \quad h_0 = 0, h_1 = 1, h_2 | h_4.$$

$$x([n]P) = \frac{A_n(x(P))}{B_n^2(x(P))}, \quad h_n = \frac{B_n(x(P))}{B_1(x(P))} \in \mathbb{Z}.$$

³⁰ Miller S., Short Programs for functions on Curves, 1986.

³¹ О. Н. Василенко, О вычислении спариваний Вейля и Тейта, Труды по дискр. матем., 10 (2007), 18–46

³² J.F. Voloch, Relating the Smart-Satoh-Araki and Semaev approaches to the discrete logarithm problem on anomalous elliptic curves, 1999.

³³ Stange, K.E. The Tate Pairing Via Elliptic Nets // Pairing-Based Cryptography – Pairing 2007.

³⁴ Shipsey R. Elliptic Divisibility Sequences. PhD thesis, University of London, 2001.



Сведение к конечному расширению поля $\mathbb{F}_p$

Рекорды для логарифмирования в конечных расширениях простого поля

Автор	Год	Поле
R. Granger etc.	2014	$\mathbb{F}_{2^{9050}}$
R. Granger etc. ³⁵	2018	$\mathbb{F}_{2^{30750}}$
P. Gaudry etc. ³⁶	2021	$\mathbb{F}_{p^6}$, где $\lfloor 6 \cdot \log_2(p) \rfloor = 521$

³⁵Granger R., Kleinung T., Zumbragel J. On the discrete logarithm problem in finite fields of fixed characteristic // Transactions of the AMS, V. 370, N.5, 2018, 3129-3145.

³⁶De Micheli G., Gaudry P., Pierrot C. Lattice Enumeration and Automorphisms for Tower NFS: A 521-Bit Discrete Logarithm Computation. Journal Of Cryptology 37, 6 (2024)



Метод³⁷ работает для эллиптических кривых над полем $\mathbb{F}_{2^n}$ где $n = rs$ – составное число.
Идея метода³⁸:

1. Строится отображение из $\mathcal{E}(\mathbb{F}_{2^n})$ в якобиан $\text{Jac}(\mathcal{H}(\mathbb{F}_{2^r}))$ кривой

$$\mathcal{H}(\mathbb{F}_{2^r}) : y^2 = x^{2g+1} + f(x), \deg f(x) \leq 2g, \quad g \in \mathbb{N}.$$

2. Исходная задача дискретного логарифмирования сводится к задаче в $\text{Jac}(\mathcal{H}(\mathbb{F}_{2^r}))$.

Задача дискретного логарифмирования в якобиане решается с помощью индекс-метода (аналогично $\mathbb{F}_p^*$). Сложность метода зависит от g – рода гиперэллиптической кривой.

³⁷Gaudry P., Hess F., Smart N. Constructive and destructive facets of Weil descent on elliptic curves// Journal Of Cryptology, 2001 (15) N. 1, pp. 19-46.

³⁸Galbraith S., Hess F., Smart N. Extending the GHS Weil Descent Attack, EUROCRYPT 2002, 2002.



Теорема

Пусть $n \geq 2$ - натуральное число. Тогда существует алгоритм поиска неизвестного k удовлетворяющего равенству $Q = [k]P$, $P, Q \in \mathcal{E}(\mathbb{F}_{p^n})$, где p -просто нечетное со следующими свойствами, выполненными при $p \rightarrow \infty$

1. сложность алгоритма составляет $O(p^{c+\varepsilon})$,
2. объем используемой памяти составляет $O(p^{l-c+\varepsilon})$

для любой действительной константы c , удовлетворяющей неравенству $\frac{n^2}{(2n+1)} \leq c \leq \frac{n}{2}$ и некоторого $\varepsilon > 0$.

Для кривой над полем $\mathbb{F}_{p^2}$ и $c = 1$ получаем $O(p^{1+\varepsilon})$. При $c < 1$ – метод становится лучше, чем ρ -метод Полларда, но объем памяти больше, чем у «метода согласования».

³⁹Delaplace C., Fouque P.A., Kirchner P., May A.. Solving ECDLP over $\mathbb{F}_p$ with Precomputation via Representation Technique. 2020. (hal-02427655).



3. Методы, (пока) не реализуемые на практике

Подходы к построению субэкспоненциального алгоритма

- Индекс-метод
- Сведение к логарифмированию в расширениях поля рациональных чисел $\mathbb{Q}$
- Сведение к логарифмированию в поле p -адических чисел $\mathbb{Q}_p$
- Многочлены суммирования И.А. Семаева и сведение к решению систем нелинейных уравнений
- Сведение к другим сложным математическим задачам



Индекс-метод⁴⁰ поиска k , удовлетворяющего равенству $Q = [k]P$:

1. Фиксировать множество элементов $R_1, \dots, R_s \in \mathcal{E}(\mathbb{K})$ (факторная база).
2. Построить множество соотношений (более чем s):
 - 2.1 Выбрать случайные α_i, β_i и $S_i = [\alpha_i]P + [\beta_i]Q$.
 - 2.2 Найти $e_{i,1}, \dots, e_{i,s}$ такие, что $S_i = \sum_{j=1}^s [e_{i,j}]R_j = [\alpha_i]P + [\beta_i]Q$.
3. Используя найденные соотношения, определить λ, μ такие, что $[\lambda]P + [\mu]Q = \mathcal{O}$.
4. Определить $k = -\frac{\lambda}{\mu}$

Проблемы:

- Как выбрать поле, над которым рассматривать кривую?
- Как выбрать факторную базу?
- Как раскладывать точки в сумму элементов факторной базы?

⁴⁰ Для $\mathbb{F}_p^*$ индекс-метод хорошо известен и имеет субэкспоненциальную оценку $\mathcal{O}(\exp(c \log^\alpha p \log^{1-\alpha} p))$ при $p \rightarrow \infty$ и некоторых c и $0 < \alpha < 1$.



Кривые над конечными расширениями поля $\mathbb{Q}$

Пусть $\mathbb{K} = \mathbb{Q}(\zeta_1, \dots, \zeta_s)$, тогда $\mathcal{E}(\mathbb{K}) : \langle R_1, \dots, R_r \rangle \times \mathcal{E}(\mathbb{K})_{tors}$, где r – ранг кривой

- Результаты о ранге кривой
 - Гипотеза: ранг не ограничен, найденный максимум над $\mathbb{Q}$: $r = 28$ (Элкис, 2006).
 - Эффективный метод вычисления ранга не найден
 - Доказано: «средний ранг» (по всем кривым) $r = \frac{7}{6}$, (Шанкар, Бхаргава, 2015)
- Результаты о порядке группы кручения
 - Для $\mathbb{K} = \mathbb{Q}$ выполнено неравенство $|\mathcal{E}(\mathbb{Q})_{tors}| \leq 16$ (Мазур, 1977)
 - Существует функция $B(d)$ такая, что для любого числового поля $\mathbb{K}$ степени $d = [\mathbb{K} : \mathbb{Q}]$ и любой эллиптической кривой $\mathcal{E}(\mathbb{K})$, порядок группы кручения $\mathcal{E}(\mathbb{K})_{tors} \leq B(d)$. (Мерель, 1996)
 - Если l делит $\text{ord}(R) \in \mathcal{E}(\mathbb{K})_{tors}$ и l – простое, то $l < d^{3d^2}$ (Парен, 1999).



Подъем в поле $\mathbb{K} = \mathbb{Q}(\zeta_1, \dots, \zeta_s)$ «Простой» метод Сильвермена⁴²

Поднимаем в $\mathbb{K}$ и строим кривую $\mathcal{E}(\mathbb{K})$ по заданным точкам, используя редукцию

$$\pi : \mathbb{K} \rightarrow \mathbb{F}_p.$$

1. Записываем в неопределенной форме $\hat{a}, \hat{b} \in \mathbb{K}$ - коэффициенты кривой $\mathcal{E}(\mathbb{K})$ так, чтобы $\pi(\hat{a}) = a$, $\pi(\hat{b}) = b$.
2. Используя координаты точек $P(x_P, y_P)$ и $Q(x_Q, y_Q)$ как координаты в $\mathbb{K}$ находим параметры кривой $\hat{a}, \hat{b} \in \mathbb{K}$.
3. Если ранг кривой $\mathcal{E}(\mathbb{K})$ равен 1 или P, Q являются зависимыми, то используя каноническую высоту⁴¹ или индекс-метод для системы образующих, находим $\hat{k}$ такой, что $Q = [\hat{k}]P$ и, после, вычисляем $k = \pi(\hat{k})$.

Проблема метода - точки не являются зависимыми. Из результатов Массера (1989), следует, что зависимые точки образуют множество «меры ноль».

⁴¹Для точки $P \in \mathcal{E}(\mathbb{Q})$ каноническая высота определяется равенством $h(P) = \lim_{n \rightarrow \infty} \frac{\log \max(t, s)}{4^n}$, где $x([2^n]P) = \frac{t}{s}$, а также $h([n]P) = n^2 h(P)$.

⁴²Silverman J.H. Lifting and Elliptic Curve Discrete Logarithms // SAC 2008, pp. 82–102, 2009.



Подъем в поле $\mathbb{K} = \mathbb{Q}(\zeta_1, \dots, \zeta_s)$ «Сложный» метод Сильвермена

Поднимаем в $\mathbb{K}$ и строим кривую $\mathcal{E}(\mathbb{K})$ по коэффициентам кривой $\mathcal{E}(\mathbb{F}_p)$ и одной заданной точке.

1. Выбираем $\hat{a} = a, \hat{b} = b, \hat{P} = P$ (из оценки «среднего ранга» ранг построенной кривой, скорее всего, будет равен 1).
2. Находим $\hat{Q} \in \mathcal{E}(\mathbb{K})$ такую, что $\pi(\hat{Q}) = Q$.
3. Используя каноническую высоту и равенство $h(\hat{Q}) = h([k]\hat{P}) = k^2 h(\hat{P})$, находим k .

Проблема метода - как построить точку $\hat{Q}$?

Поскольку k велико, то числители и знаменатели координат точки $\hat{Q}$ – очень велики. Например⁴³, для $p \sim 2^{160}$ ожидаемый размер $\max\{|t|, |s|\} \sim 2^{16000}$, где $x(\hat{Q}) = \frac{t}{s}$.

⁴³Silverman J.H., Suzuki J. Elliptic Curve Discrete Logarithms and the Index Calculus // ASIACRYPT'98, pp. 110-125, 1998.



Подъем в поле $\mathbb{K} = \mathbb{Q}(\zeta_1, \dots, \zeta_s)$

Используем группу кручения

Идея метода:

1. Отображаем $P, Q \rightarrow \hat{P}, \hat{Q} \in \mathcal{E}(\mathbb{K})_{tors}$.
2. Находим $\hat{k}$ для которого $\hat{Q} = [\hat{k}]\hat{P}$.

Проблема – неизвестное $k \equiv \hat{k} \pmod{|\mathcal{E}(\mathbb{K})_{tors}|}$, а порядок группы кручения очень мал.

Теорема (Серр)

Существует константа $c = c(\mathcal{E}(\mathbb{Q})) > 0$ такая, что для всех натуральных $n \geq 2$ и любого числового поля $\mathbb{K}$ такого, что $\mathcal{E}(\mathbb{K})_{tors}$ содержит точку порядка n , будет выполнено

$$d = [\mathbb{K} : \mathbb{Q}] \geq cn^4.$$



Подъем в поле $\mathbb{Q}_p$

Используем $\mathbb{Z}_p$

Напомним, что $\mathbb{Q}_p = \{x = \sum_{i=-k}^{\infty} a_i p^i\}$ поле p -адических чисел (как для аномальных кривых). Кривая

$$\mathcal{E}(\mathbb{Q}_p) \cong \mathbb{Z}_p \times \mathcal{E}(\mathbb{Q}_p)_{tors}.$$

Подъём точки $P(x_p, y_p)$ из $\mathcal{E}(\mathbb{F}_p)$ в $\mathcal{E}(\mathbb{Q}_p)$:

- Строится $\hat{P} = (x_p + \alpha p, y_p + \beta p)$
- Подставляем в уравнение кривой

$$(y_p + \beta p)^2 \equiv (x_p + \alpha p)^3 + a(x_p + \alpha p) + b \pmod{p^2}$$

и находим $\alpha \equiv \omega_1 \beta + \omega_0 \pmod{p}$ для фиксированных ω_0, ω_1 и любого $\beta \in \mathbb{F}_p$.

Выполняем аналогичный подъем для точки Q из $\mathcal{E}(\mathbb{F}_p)$ до точки $\hat{Q}$ из $\mathcal{E}(\mathbb{Q}_p)$, после чего, используя эллиптический логарифм, определяем

$$\hat{k} = \frac{\log_E(\hat{Q})}{\log_E(\hat{P})} \in \mathbb{Q}_p, \quad k \equiv \hat{k} \pmod{p}.$$

Проблема – только для одного β из p возможных, выполнено равенство $\hat{Q} = [\hat{k}]\hat{P}$.



Подъем в поле $\mathbb{Q}_p$

Используем группу кручения

В случае подъема в группу кручения $\mathcal{E}(\mathbb{Q}_p)_{tors}$ подъем однозначный, т.е. для любой точки $P \in \mathcal{E}(\mathbb{F}_p)$ существует единственная точка $\hat{P}$: $[q]\hat{P} = \mathcal{O}$ и $\hat{P} \equiv P \pmod{p}$. Подъем точки $P(x_P, y_P)$:

- Строится $\hat{P} = (x_P + \alpha p, y_P + \beta p)$
- Подставляем в уравнение кривой

$$(y_P + \beta p)^2 \equiv (x_P + \alpha p)^3 + a(x_P + \alpha p) + b \pmod{p^2}$$

и находим $\alpha \equiv \omega_1 \beta + \omega_0 \pmod{p}$ для фиксированных ω_0, ω_1 и любого $\beta \in \mathbb{F}_p$.

- Используя равенство $[q]\hat{P} = \mathcal{O}$ находим единственное значение β .

Обозначим n – порядок точек $\hat{P}, \hat{Q}$ в $\mathcal{E}(\mathbb{Q}_p)_{tors}$. Из равенств

$$\hat{Q} - [k]\hat{P} \equiv Q - [k]P \equiv \mathcal{O} \pmod{p}, \quad n(\hat{Q} - [k]\hat{P}) = \mathcal{O}$$

следует равенство $\hat{Q} = [k]\hat{P}$.

Проблема – для эллиптического логарифма нужно использовать точки $[n]\hat{Q} = [n]\hat{P} = \mathcal{O}$.



Теорема

Пусть $\mathcal{E}(\mathbb{K})$ эллиптическая кривая и $\text{char}\mathbb{K} \neq 2, 3$. Многочлены суммирования задаются равенствами

$$\begin{cases} S_2(x_1, x_2) &= x_1 - x_2, \\ S_3(x_1, x_2, x_3) &= (x_1 - x_2)^2 x_3^2 - 2((x_1 x_2 + a)(x_1 + x_2) + 2b)x_3 + (x_1 x_2 - a)^2 - 4b(x_1 + x_2), \\ S_n(x_1, \dots, x_n) &= \text{Res}_X(S_{n-k}(x_1, \dots, x_{m-k-1}, X), S_{k+2}(x_{nk}, \dots, x_n, X)), \end{cases}$$

для всех $n \geq 4$ и $m - 3 \geq k \geq 1$, где Res_X результат двух многочленов от переменной X . Более того, для каждого $n \geq 2$ найдутся точки $R_1, \dots, R_n \in \mathcal{E}(\mathbb{K})$ такие, что

$$f(x(R_1), \dots, x(R_n)) = 0, \quad \text{и} \quad R_1 + \dots + R_n = \mathcal{O}.$$

Метод ускоренного вычисления и явные формулы для $n \leq 10$ получены в 2014 г.⁴⁴

⁴⁴Faugère J.C., Huot L., Joux A., Renault R., Vitse V. Symmetrized summation polynomials: Using small order torsion points to speed up elliptic curve index calculus, EUROCRYPT 2014, pp. 40–57, 2014.

⁴⁵Semaev I. Summation polynomials and the discrete logarithm problem on elliptic curves. Cryptology ePrint Archive, Report 2004/031, 2004.



Многочлены суммирования

Индекс-метод дискретного логарифмирования

Шаг индекс-метода ($R_1, \dots, R_s$ – факторная база):

$$[\alpha_i]P + [\beta_i]Q = [e_{i,1}]R_1 + \dots + [e_{i,s}]R_s,$$

Пусть $\mathbb{V} \subset \mathbb{F}_p$ т.ч. для любого $\gamma \in \mathbb{V}$ существует $R \in \mathcal{E}(\mathbb{F}_p)$: $x(R) = \gamma$ и $|\mathbb{V}| = s$.
Тогда, для некоторого n

1. выберем случайные α_i, β_i .
2. составим систему уравнений

$$\begin{cases} S_{n+1}(x_1, \dots, x_n, x([\alpha_i]P + [\beta_i]Q)) & = 0, \\ F(x_1) & = 0, \\ \dots & \\ F(x_n) & = 0 \end{cases}$$

где $F(x) = \prod_{\gamma \in \mathbb{V}} (x - \gamma)$ и $F(x) | x^p - x = \prod_{\gamma \in \mathbb{F}_p} (x - \gamma)$.

Проблема – решить указанную систему.



Многочлены суммирования

Методы решения нелинейных системы уравнений

Основной аппарат: построение базисов Грёбнера.

Методы:

- алгоритмы Фужера F_4 (обоснованная оценка сложности) и F_5
- учет специального вида нелинейных систем

Результаты:⁴⁶

- оценка поиска корней для одной системы: ns^{n-1} .
- общая оценка метода логарифмирования: $n!q$ (с вероятностью близкой к единице)
- оптимистичные предположения о снижении сложности решения в силу специального вида системы - не верны

Результаты подтверждены экспериментально для $n = 2, 3, 4$ и малых значений $p \leq 23$.

⁴⁶Yokoyama K., Yasuda M., Takahashi Y., Kogure J. Complexity bounds on Semaev's naive index calculus method for ECDLP // J. Math. Cryptol. 2020 (14), pp. 460–485.



Подходы, которые (возможно) требуют дополнительного рассмотрения

- Методы, использующие информацию о кольце эндоморфизмов кривой $\mathcal{E}(\mathbb{F}_p)$
 - метод, использующий отображение кривой $\mathcal{E}(\mathbb{F}_p)$ на изогенную кривую, на которой решение «может быть несколько проще»⁴⁷,
 - утверждение о том, что явно заданный эндоморфизм $Q = \pi(P)$ или $\phi(Q) = P$ позволяет найти решение задачи дискретного логарифмирования.
- метод сведения дискретного логарифмирования на эллиптической кривой к вычислению сигнатур в дуальностях Понтрягина⁴⁸
- подъем кривой в поле $\mathbb{F}_{p^n}$ и последующее применение многочленов Семаева (метод Пети-Мессенга)⁴⁹. Необходимое условие: существование такого $k \in \mathbb{F}_p$, что $p^k - 1$ является гладким.

⁴⁷Jao D., Miller S.D., Venkatesan R. Do all elliptic curves of the same order have the same difficulty of discrete log? In: Roy B.K. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 21–40. Springer, Berlin (2005)

⁴⁸Huang M.D., Raskind W.: Global duality, signature calculus and the discrete logarithm problem. LMS J. Comput. Math. 12, 228–263 (2009).

⁴⁹Petit C., Kisters M., Messeng A. Algebraic Approaches for the Elliptic Curve Discrete Logarithm Problem over Prime Fields // PKC 2016, Part II, LNCS 9615, pp. 3–18, 2016.



Закключение

Временная шкала

1990 – 2000 гг.	Поиск частных случаев
2000 – 2018 гг.	Метод параллельного поиска коллизий
2004 – 2020 гг.	Методы с использованием многочленов суммирования
2020 – н/вр.	Применение квантовых вычислителей

СПАСИБО ЗА ВНИМАНИЕ!