МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА
факультет вычислительной математики и кибернетики

На правах рукописи

Николаев Максим Владимирович

О сложности решения некоторых обобщений задачи дискретного логарифмирования

05.13.19 - Методы и системы защиты информации, информационная безопасность

ДИССЕРТАЦИЯ

на соискание ученой степени
кандидата физико-математических наук

Научный руководитель:
кандидат физико-математических наук
Матюхин Д.В.

Москва — 2018

Оглавление

Введение

Актуальность темы исследования. Задача дискретного логарифмирования является одной из важнейших в области информационной безопасности. Предположение о вычислительной трудности ее решения является обоснованием стойкости большинства используемых на практике механизмов защиты информации с открытым ключом, включая различные варианты схемы (протокола) выработки общего ключа Диффи-Хеллмана [17] и схем шифрования и электронной подписи Эль-Гамаля [22]. В ряде случаев задачу определения ключа указанных схем удается свести к одному из обобщений задачи дискретного логарифмирования, которые могут быть решены с меньшей трудоемкостью. В работе рассматриваются следующие из них.

- Задача дискретного логарифмирования в интервале.
  В данном случае известно, что решение лежит в наперед заданном интервале, размер которого заведомо меньше порядка исходной группы. Необходимость решения задачи в такой формулировке естественным образом возникает в задаче нахождения c-битной экспоненты [31, 52, 50], атаках, использующих информацию из побочных каналов утечки, и атаках по маленькой подгруппе [34, 42], при расшифровании в схеме гомоморфного шифрования Бонэ-Го-Ниссима [10], подсчете числа точек эллиптических кривых [30], оценке трудоемкости решения сильной задачи Диффи-Хеллмана [14, 37].

- Двумерная задача дискретного логарифмирования.
  В этом случае требуется найти два неизвестных параметра, при-

надлежащих наперед заданным интервалам. Задача в такой формулировке возникает, например, при подсчете количества элементов многообразия Якоби, анализе трудоемкости решения классической задачи дискретного логарифмирования в случае подгруппы простого порядка группы точек эллиптической кривой, обладающей эффективным автоморфизмом, которые позволяют заменять вычисление кратной точки вычислением суммы кратных точек (метод Галланта-Ламберта-Ванстоуна) [29], анализе трудоемкости решения задачи дискретного логарифмирования для экспонент ограниченной высоты [8].

Таким образом, существует обширный список задач, трудоемкость решения которых может быть оценена с помощью трудоемкости решения указанных обобщений задачи дискретного логарифмирования. Однако до настоящего времени задача поиска наилучших методов их решения относительно слабо изучена, что наделяет проводимое исследование не только теоретической, но и существенной практической значимостью. Действительно, национальные и международные стандарты, определяющие рекомендации по использованию параметров механизмов защиты информации, должны в полной мере учитывать последние результаты в данной области. Огромный интерес к этому вопросу подтверждает также растущее от года к году количество публикаций по исследуемой тематике.

Степень научной разработанности темы исследования. Двумерная задача дискретного логарифмирования в конечной группе G (без ограничения общности, с аддитивной записью операции) является обобщением классической задачи дискретного логарифмирования и заключается в поиске для заданных $P_1,\ P_2,\ Q \in G,\ 0 < N_1, N_2 < \sqrt{|G|}$ значений n_1, n_2 таких, что $Q = n_1P_1 + n_2P_2$, в предположении, что при условии $-N_1 \leq n_1 \leq N_1,\ -N_2 \leq n_2 \leq N_2$ эти значения существуют. В 2004 году Годри и Шост предложили алгоритм решения этой задачи, средняя трудоемкость которого при стандартных эвристических пред-

положениях не превосходит $(c + o(1))\sqrt{N}$ групповых операций в G, где $c \approx 2.43, N = 4N_1N_2, o(1) \to 0$ при $N \to \infty$. В 2009 году Гэлбрайт и Рупраи усовершенствовали алгоритм Годри-Шоста, получив $c \approx 2.36$.

Как и в случае классической задачи, для ускорения поиска решения двумерной задачи можно использовать наличие у группы G автоморфизма, для которого орбита любого элемента группы вычисляется существенно быстрее групповой операции (такой автоморфизм называют эффективным). Например, группа точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов

1) всегда обладает эффективным автоморфизмом порядка 2 (операция взятия обратного элемента $\varphi(x, y) = (x, -y)$);

2) если $B = 0$ и $p \equiv 1 \bmod 4$ — эффективным автоморфизмом порядка 4: $\varphi(x, y) = (-x, \alpha y)$, где α — элемент порядка 4 по модулю p;

3) если $A = 0$ и $p \equiv 1 \bmod 3$ — эффективным автоморфизмом порядка 6: $\varphi(x, y) = (\beta x, -y)$, где $\beta \neq 1$ — кубический корень из 1 по модулю p.

В 2010 году Лиу показал, что в первом случае значение c в оценке трудоемкости алгоритма Годри-Шоста может быть снижено до 1.4503, а во втором при $P_2 = \varphi(P_1)$ и $N_1 = N_2$ — до 1.0255.

Задача дискретного логарифмирования в интервале заключается в поиске для заданной конечной группы G (с аддитивной записью операции), заданных $P, Q \in G, N < |G| - 1$ такого значения n (в предположении, что оно существует), что $Q = nP, 0 \leq n \leq N$. В 2010 году Гэлбрайт и Рупраи адаптировали алгоритм Годри-Шоста к решению указанной задачи для групп с эффективным инвертированием. Оценка средней трудоемкости решения задачи составила $(1.36 + o(1))\sqrt{N}$ групповых операций в G при $N \to \infty$.

Целью исследования является усовершенствование известных методов решения двумерной задачи дискретного логарифмирования и задачи дискретного логарифмирования в интервале для групп с

эффективными автоморфизмами.

Основные задачи исследования.

- Разработать алгоритм решения двумерной задачи дискретного логарифмирования в подгруппе группы точек эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов при $P_2 = \varphi(P_1)$ и $N_1 = N_2$, где φ — эффективный автоморфизм порядка 6. Оценить среднюю трудоемкость полученного алгоритма.

- Провести анализ возможности оптимизации наилучших известных методов решения двумерной задачи дискретного логарифмирования для групп с эффективными автоморфизмами, а именно для подгрупп группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов в перечисленных ранее случаях 1), 2), 3).

- Провести анализ возможности оптимизации наилучших известных методов решения задачи дискретного логарифмирования в интервале для групп с эффективным инвертированием.

Область исследования. Содержание диссертации соответствует паспорту специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность», область исследования соответствует п. 1 «Теория и методология обеспечения информационной безопасности и защиты информации».

Краткое содержание работы.

- Глава 1 содержит обзор наиболее значимых результатов в области решения задачи дискретного логарфмирования и некоторых ее обобщений, а также формулировку теоремы Гэлбрайта-Холмса, используемой при получении оценок трудоемкости рассматриваемых

в диссертации алгоритмов. В параграфе 1.1 приводится формулировка классической задачи дискретного логарифмирования, описание наиболее эффективных методов ее решения, а также варианты сведения к двумерной задаче. Параграф 1.2 содержит описание классического алгоритм Годри-Шоста решения двумерной задачи дискретного логарифмирования. Далее излагаются теоретические факты, необходимые для оценки среднего количества шагов, выполняемых алгоритмом, и описываются основные идеи использования автоморфизмов, допускающих эффективную реализацию, для оптимизации алгоритма Годри-Шоста в случае решения двумерной задачи дискретного логарифимирвания. И, наконец, приводятся наилучшие известные оценки средней трудоемкости решения двумерной задачи дискретного логарифмирования в случае групп с эффективными автоморфизмами порядка 2 и 4. В параграфе 1.3 рассматривается задача дискретного логарифмирования в интервале. Приводятся наилучшие известные оценки средней трудоемкости решения задачи дискретного логарифмирования в интервале в случае групп с эффективным инвертированием. Параграф 1.4 содержит анализ возможности достижения теоретических оценок средней трудоемкости алгоритмов решения обобщений задачи дискретного логарифмирования на практике с учетом принятых допущений при их получении.

- В главе 2 рассматривается двумерная задача дискретного логарифмирования для эллиптической кривой E, заданной над конечным простым полем $GF(p)$ уравнением $y^2 = x^3 + B$ при $p \equiv 1 \pmod 3$, обладающей эффективным автоморфизмом φ порядка 6 ($\varphi(x, y) = (\beta x, -y)$, где $\beta \neq 1$ — кубический корень из 1 по модулю p). Для данной эллиптической кривой E конструктивно доказывается существование (при $P_2 = \varphi(P_1)$ и $N_1 = N_2$) более эффективного алгоритма решения двумерной задачи дискретного логарифмирования, а также приводится и доказывается оценка средней трудоемкости алгоритма.

- Глава 3 посвящена исследованию возможностей оптимизации алгоритма Годри-Шоста для решения двумерной задачи дискретного логарифмирования и задачи дискретного логарифмирования в интервале. В параграфе 3.1 рассматривается двумерная задача дискретного логарифмирования в конечных циклических группах с эффективным автоморфизмом. Предлагается способ параметризации соответствующих модификаций алгоритма Годри-Шоста. Приводятся описание разработанного программного средства и результаты выполненных с помощью него расчетов константы при главном члене в оценке средней трудоемкости модифицированных алгоритмов для различных значений параметра. Далее приводится конструктивное доказательство существования оптимального (в смысле использования рассматриваемых параметров) алгоритма решения двумерной задачи дискретного логарифмирования в группе с автоморфизмом порядка 6. Демонстрируется, как полученный результат можно обобщить для случаев групп с эффективными автоморфизмами порядка 2 и 4. В параграфе сравнивается трудоемкость решения классической задачи дискретного логарифмирования алгоритмом Полларда и разработанным алгоритмом в случае сведения классической задачи к двумерной, анализируются условия, при которых такое сведение целесообразно. В параграфе 3.2 результаты, полученные в параграфе 3.1, используются для конструктивного доказательства существования оптимальной (с точки зрения рассматриваемых параметров) модификации алгоритма Годри-Шоста решения задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием.

- Глава 4 содержит описание и результаты численных экспериментов для вариантов алгоритма Годри-Шоста, изложенных в главе 3, а именно, алгоритмов решения двумерной задачи дискретного логарифмирования в конечных циклических группах с эффективными автоморфизмами (параграф 3.1), а также задачи дискретного логарифмирования в интервале для группы с эффективным инвер-

тированием (параграф 3.2). Выполнено сравнение теоретических и экспериментальных результатов, полученных реализациями алгоритма Годри-Шоста, для ряда эллиптических кривых, стандартизованных NIST, SECG и ECC Brainpool.

- Заключение содержит краткий перечень полученных результатов, а также описание возможных перспектив дальнейшей разработки темы.

Научная новизна полученных результатов.

- Автором впервые предложена модификация алгоритма Годри-Шоста решения двумерной задачи дискретного логарифмирования в случае подгруппы группы точек эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов при $P_2 = \varphi(P_1)$ и $N_1 = N_2$, где φ — эффективный автоморфизм порядка 6. Автором получена также оценка средней трудоемкости разработанного алгоритма, составляющая $(c+o(1))\sqrt{N}$ групповых операций, где $c \approx 0.9781$, что меньше, чем в случае эллиптической кривой общего вида.

- Автором разработаны модификации алгоритма Годри-Шоста решения двумерной задачи дискретного логарифмирования и получены оценки средней трудоемкости:

  – для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов при $N_1 = N_2$ с оценкой средней трудоемкости $(1+\varepsilon)\sqrt{\frac{\pi N}{2}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций;

  – для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax$ над конечным простым полем из $p \equiv 1 \bmod 4$ элементов при $P_2 = \varphi(P_1)$ и $N_1 = N_2$, где φ — эффективный автоморфизм порядка 4, с оценкой средней трудоемкости $(1+\varepsilon)\sqrt{\frac{\pi N}{4}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций;

– для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов при $P_2 = \varphi(P_1)$ и $N_1 = N_2$, где φ — эффективный автоморфизм порядка 6, с оценкой средней трудоемкости $(1+\varepsilon)\sqrt{\frac{\pi N}{4}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций.

С помощью разработанной программной реализации алгоритмов продемонстрирована также согласованность теоретических оценок средней трудоемкости с экспериментальными. Таким образом, получены наиболее эффективные в настоящее время алгоритмы решения указанных задач.

- Автором предложена модификация алгоритма Годри-Шоста для решения задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием, и получена оценка средней трудоемкости, составляющая $(1+\varepsilon)\sqrt{\frac{\pi N}{2}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций в G. Разработанный алгоритм в настоящее время является наиболее эффективным алгоритмом решения указанной задачи.

Теоретическая и практическая значимость работы. Получены наиболее эффективные (на момент написания работы) алгоритмы решения некоторых обобщений задачи дискретного логарифмирования. Работа имеет теоретический характер, однако полученные результаты могут применяться для обоснования стойкости конкретных реализаций математических методов защиты информации, что указывает на практическую значимость.

Методология и методы исследования. Проводимые исследования базируются на известных теоретических положениях алгебраической геометрии, дискретной математики, теории вероятностей, математического анализа, вычислительной математики. Достоверность полученных результатов обоснована строгим математическим доказательством.

Положения, выносимые на защиту.

- Модификация алгоритма Годри-Шоста решения двумерной задачи дискретного логарифмирования при $P_2 = \varphi(P_1)$ и $N_1 = N_2$ в случае эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов, где φ — эффективный автоморфизм порядка 6. Оценка средней трудоемкости нового алгоритма.

- Оптимальные (с точки зрения используемых параметров алгоритма Годри-Шоста) оценки средней трудоемкости решения двумерной задачи дискретного логарифмирования для групп с эффективными автоморфизмами, а именно для подгрупп группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов в рассмотренных ранее случаях 1), 2), 3).

- Модификация алгоритма Годри-Шоста решения задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием, а также оценка средней трудоемкости нового алгоритма.

Апробация результатов. Основные результаты работы опубликованы в следующих изданиях.

1. М. В. Николаев, Д. В. Матюхин. О сложности двумерной задачи дискретного логарифмирования в конечной циклической группе с эффективным автоморфизмом порядка 6. Дискретная математика, том 25 (2013), стр. 54–65.

2. М. В. Николаев. On the complexity of two-dimensional discrete logarithm problem in a finite cyclic group with efficient automorphism. Математические вопросы криптографии, том 6 выпуск 2 (2015), стр. 45–57.

3. М. В. Николаев. О сложности задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием. Прикладная дискретная математика, №2 (2015), стр. 97–102.

Первая работа выполнена в соавторстве с научным руководителем. Д. В. Матюхину принадлежит постановка задачи; решение поставленной задачи полностью принадлежит М. В. Николаеву.

Результаты работы докладывались на семинарах, всероссийских и международных конференциях:

1) на XV международной научно-практической конференции «РусКрипто», 2013 год, с 27 по 30 марта, с.п. Смирновское, Солнечногорский район, Московская область;

2) на III симпозиуме «Современные тенденции в криптографии» (CTCrypt' 2014), 2014 год, с 5 по 6 июня, Москва;

3) на XVI международной научно-практической конференции «РусКрипто», 2014 год, с 25 по 28 марта, с.п. Смирновское, Солнечногорский район, Московская область;

4) на XIV всероссийской конференции «Сибирская научная школа-семинар с международным участием Компьютерная безопасность и криптография» (SIBECRYPT'15), 2015 год, с 7 по 12 сентября, Новосибирск;

5) на семинаре «Арифметические вопросы криптографии» под руководством д.ф.-м.н., проф. В.Н. Чубарикова (Механико-математический факультет Московского государственного университета имени М.В. Ломоносова, г. Москва), 2017 год.

Благодарности. Автор выражает искреннюю благодарность своему научному руководителю кандидату физико-математических наук Матюхину Дмитрию Викторовичу за постановку задач, постоянное внимание к работе и ценные советы. Автор выражает признательность коллективу кафедры информационной безопасности факультета ВМК МГУ имени М.В. Ломоносова.

Глава 1

Обзор результатов по теме исследования и вспомогательные утверждения

Настоящая глава является введением в проблематику дискретного логарифмирования и содержит обзор наиболее значимых в настоящее время результатов по теме исследования.

1.1 Задача дискретного логарифмирования

Безопасность многих механизмов защиты информации с открытым ключом основывается на предположении о вычислительной трудности решения задачи дискретного логарифмирования. Этот факт демонстрирует практическую значимость анализа трудоемкости решения этой задачи.

Определение 1. *Задача дискретного логарифмирования.*

Дано: группа $G = \langle P \rangle$, $Q \in G$.
Найти: $n \in \{0, \ldots, |G| - 1\}$ *такое, что* $Q = nP$.

Хотя в частном случае использования в качестве группы G мультипликативной группы конечного поля, для решения классической задачи дискретного логарифмирования предложены алгоритмы с субэкспоненциальной оценкой трудоемкости (см., например, [6]), в общем случае такие алгоритмы неизвестны. Особый интерес представляет использование в качестве группы G подгруппы большого простого порядка группы точек эллиптической кривой, определенной над конечным простым полем.

Определение 2. *[1] Пусть* $\mathbb{K}$ *- поле,* $\operatorname{char}\mathbb{K} \neq 2, 3$. *Эллиптическая кривая задается над* $\mathbb{K}$ *уравнением*

$$y^2 = x^3 + Ax + B,$$

где $A, B \in \mathbb{K}$, $4A^3 + 27B \neq 0$. *Она обозначается символом* E *или* $E_{A,B}$. *Множество точек кривой обозначается через*

$$E_{A,B}(\mathbb{K}) = E(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 : y^2 = x^3 + Ax + B\} \cup \mathcal{O}.$$

Здесь $\mathcal{O}$ *- «ноль» кривой, или «бесконечно удаленная точка».*

Для превращения множества точек эллиптической кривой в абелеву группу вводится операция сложения, удовлетворяющая следующим правилам (см., например, [1, 3]).

1. Сложение с нейтральным элементом
   $(x, y) + \mathcal{O} = (x, y),\ \mathcal{O} + \mathcal{O} = \mathcal{O}$.

2. Сложение с противоположным элементом
   $(x, y) + (x, -y) = \mathcal{O}$.

3. Сложение точек
   Пусть $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$, $x_P \neq x_Q$. Тогда

$R = P + Q = (x_R, y_R)$ и

$$\begin{aligned} x_R &= \lambda^2 - x_P - x_Q, \\ y_R &= -y_P + \lambda(x_P - x_R), \text{ где} \\ \lambda &= \frac{y_Q - y_P}{x_Q - x_P}. \end{aligned} \tag{1.1}$$

4. Удвоение точки
   Пусть $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$, $P = Q$. Тогда $R = P + Q = 2P = (x_R, y_R)$ и

$$\begin{aligned} x_R &= \lambda^2 - 2x_P, \\ y_R &= -y_P + \lambda(x_P - x_R), \text{ где} \\ \lambda &= \frac{3x_P^2 + A}{2y_P}. \end{aligned} \tag{1.2}$$

В настоящее время наиболее эффективным в общем случае методом решения классической задачи дискретного логарифмирования в подгруппе большого простого порядка группы точек эллиптической кривой, определенной над конечным простым полем, является параллельный метод Полларда [51]. Основная идея метода заключается в следующем. Вычисляется псевдослучайная последовательность

$$a_i P + b_i Q,\ a_i, b_i \in_R \{0, \ldots, |G| - 1\},\ i = 1, 2, \ldots \tag{1.3}$$

до тех пор, пока в ней не найдутся два одинаковых элемента:

$$a_k P + b_k Q = a_l P + b_l Q,\ k \neq l, \tag{1.4}$$

откуда находим $n = (a_k - a_l)(b_l - b_k)^{-1}$.

Анализ средней трудоемкости параллельного метода Полларда основывается на использовании парадокса задачи о днях рождения. В работе [51] показано, что средняя трудоемкость метода не превосходит по порядку величины $\sqrt{\frac{\pi|G|}{2}}$ групповых операций.

Предположим теперь, что группа G — циклическая простого порядка и обладает автоморфизмом φ, для которого орбиту любого элемента

можно вычислить за время, существенно меньшее необходимого для выполнения групповой операции, и для которого легко вычислить такое $\lambda \in \{1, \ldots, |G|-1\}$, что φ действует в группе G как умножение на λ. Тогда группа G распадается на непересекающиеся классы эквивалентности (орбиты) относительно действия группы $\langle\varphi\rangle$, и как показано в работах [19, 64], метод Полларда может быть оптимизирован за счет перехода от поиска совпадающих элементов последовательности (1.3) к поиску совпадающих классов эквивалентности этих элементов. Действительно, в этом случае вместо равенства (1.4) имеем равенство

$$\varphi^s(a_k P + b_k Q) = a_l P + b_l Q,$$

для некоторого s, откуда

$$(\lambda^s a_k - a_l)P = (b_l - \lambda^s b_k)Q,$$

т. е. $n = (\lambda^s a_k - a_l)(b_l - \lambda^s b_k)^{-1}$. Средняя трудоемкость соответствующей модификации параллельного метода Полларда не превосходит по порядку величины $\sqrt{\frac{\pi|G|}{2|\langle\varphi\rangle|}}$ групповых операций ([19], [64]).

Примеры групп *с эффективными автоморфизмами* будут рассмотрены в § 1.2 и § 2.1.

Автоморфизмы, допускающие эффективную реализацию, в целях оптимизации вычислений широко используются в программном обеспечении, реализующем механизмы защиты информации на основе эллиптических кривых [15, 36]. Получить прирост производительности позволяет использование таких методов, как GLV [29] и GLS [26], суть которых заключается в замене вычисления кратной точки эллиптической кривой kP вычислением суммы $k_1 P + k_2\varphi(P)$, где φ — автоморфизм эллиптической кривой, а k_1, k_2 — порядка $\sqrt{|G|}$. Описанный подход используется в некоторых эффективных реализациях (см., например [63]) и позволяет получить значительный прирост производительности (до 1.7 раза).

Для получения кратной точки kP для случайного $0 < k < |G|$ с использованием методов GLV, GLS используется один из следующих подходов [33].

1. Сначала выбираются параметры $k_1, k_2 \in_R [0, \sqrt{|G|}) \cap \mathbb{Z}$, после чего вычисляется кратная точка $kP = k_1 P + k_2 \varphi(P)$, где $k \equiv k_1 + \lambda k_2 \bmod |G|$. Такой подход называется *рекомпозицией*.

2. Сначала выбирается случайный параметр k, после чего определяются соответствующие k_1, k_2 для вычисления кратной точки. Такой подход *декомпозиции* является более ресурсоемким.

При использовании как рекомпозиции, так и декомпозиции, задача нахождения дискретного логарифма k может быть сведена к нахождению значений k_1, k_2, удовлетворяющих уравнению

$$kP = k_1 P + k_2 \varphi(P),$$

т. е. решению двумерной задачи дискретного логарифмирования. Следующий параграф содержит обзор наиболее важных результатов анализа трудоемкости решения двумерной задачи дискретного логарифмирования.

1.2 Двумерная задача дискретного логарифмирования

Определение 3. *Двумерная задача дискретного логарифмирования.*
Дано: группа G; $P_1, P_2, Q \in G$, $N_1, N_2 \in \mathbb{N}$, $Q = n_1 P_1 + n_2 P_2$ *для некоторых (неизвестных)* $n_1 \in \{-N_1, \ldots, N_1\}$, $n_2 \in \{-N_2, \ldots, N_2\}$.
Найти: $n_1', n_2' \in \mathbb{Z}$ *такие, что* $Q = n_1' P_1 + n_2' P_2$.

Двумерная задача дискретного логарифмирования, помимо случаев, описанных в конце § 1.1, имеет и другие важные приложения. Одним из них является вычисление порядка *многообразия Якоби* [45] гиперэллиптической кривой.

Определение 4. *[21] Гиперэллиптическая кривая C рода $g \geq 1$ над полем $GF(q)$ задается уравнением вида*

$$C : v^2 + h(u)v = f(u),$$

где $h(u) \in GF(q)[u]$ — полином степени не выше g, $f(u) \in GF(q)[u]$ — нормированный полином степени $2g+1$, и не существует пары (u, v), одновременно удовлетворяющей уравнениям

$$\begin{cases} v^2 + h(u)v = f(u), \\ 2v + h(u) = 0, \\ h'(u)v - f'(u) = 0. \end{cases}$$

Вычислительная трудность решения классической задачи дискретного логарифмирования в подгруппе многообразия Якоби гипперэллиптических кривых делает их привлекательными для использования в системах защиты информации [39]. Обязательным условием стойкости таких систем является наличие больших простых делителей у порядка многообразия Якоби. Таким образом, подсчет числа точек подгрупп многообразия Якоби является обязательным шагом для выработки параметров систем, использующих гиперэллиптические кривые.

Пусть $\mathfrak{J}_C$ — многообразие Якоби гиперэллиптической кривой C рода 2, $\mathfrak{J}_C(GF(q))$ — множество $GF(q)$-рациональных точек, представляющих собой конечную абелеву группу. Характеристический многочлен автоморфизма Фробениуса степени q для $\mathfrak{J}_C(GF(q))$ задается следующим образом [59, 44, 41]:

$$\chi_q(X) = X^4 - s_1X^3 + s_2X^2 - s_1qX + q^2,$$

где $s_1, s_2 \in \mathbb{Z}$ и

$$|s_1| \leq 4\sqrt{q},$$

$$2|s_1|\sqrt{q} - 2q \leq s_2 \leq \frac{s_1^2}{4} + 2q.$$

Тогда порядок $\mathfrak{J}_C(GF(q))$ может быть вычислен следующим образом [59]:

$$|\mathfrak{J}_C(GF(q))| = \chi_q(1) = q^2 + 1 - s_1(q+1) + s_2.$$

Используя модификацию алгоритма Шуфа [9], можно вычислить $|\mathfrak{J}_C(GF(q))| \bmod m$, $\overline{s_1} = s_1 \bmod m$, $\overline{s_2} = s_2 \bmod m$ для некоторого $m \in \mathbb{N}$. Следуя работе [30], предположим, что

$$s_1 = \overline{s_1} + m\widetilde{s_1},\ s_2 = \overline{s_2} + m\widetilde{s_2},\ \text{где}$$

$$0 \leq \overline{s_1}, \overline{s_2} < m.$$

Тогда

$$\begin{aligned} |\widetilde{s_1}| &\leq \frac{4\sqrt{q}}{m}, \\ |\widetilde{s_2}| &\leq \frac{6q}{m}. \end{aligned} \tag{1.5}$$

Для того, чтобы найти неизвестные $\widetilde{s_1}, \widetilde{s_2}$, выберем $\mathfrak{D} \in_R \mathfrak{J}_C(GF(q))$. Так как $\chi_q(1)\mathfrak{D} = \mathcal{O}$, то справедливо равенство

$$(q^2 + 1 - \overline{s_1}(q+1) + \overline{s_2})\mathfrak{D} + (-\widetilde{s_1}(q+1) + \widetilde{s_2})m\mathfrak{D} = \mathcal{O}.$$

Значение $q^2+1-\overline{s_1}(q+1)+\overline{s_2}$ известно. Обозначив его через K, получаем

$$\widetilde{s_1}\mathfrak{D}_1 + \widetilde{s_2}\mathfrak{D}_2 = \mathfrak{D}_3,$$

где

$$\mathfrak{D}_1 = -(q+1)m\mathfrak{D},$$

$$\mathfrak{D}_2 = m\mathfrak{D},$$

$$\mathfrak{D}_3 = -K\mathfrak{D}.$$

Таким образом, нахождение значений $\widetilde{s_1}, \widetilde{s_2}$ (с учетом неравенств (1.5)) сводится к решению двумерной задачи дискретного логарифмирования. Значения $\widetilde{s_1}, \widetilde{s_2}$ позволяют выполнить проверку, является ли порядок элемента $\mathfrak{D}$ достаточно большим простым числом.

Еще одной областью применения алгоритмов решения двумерной задачи дискретного логарифмирования является решение задачи дискретного логарифмирования для экспонент ограниченной высоты. Задача дискретного логарифмирования для экспонент ограниченной высоты предполагает для $P_1, P_2 \in G, n \in \mathbb{N}$ нахождение таких $0 < a, b \leq n$, что

$$aP_1 = bP_2.$$

Пусть высота h рационального числа a/b определена следующим образом

$$h(a/b) = \max\{|a|, |b|\}.$$

Тогда для решения задачи дискретного логарифмирования для экспонент высоты n необходимо найти такое q, что

$$qP_1 = P_2,\ h(q) \leq n.$$

Как показано в работе [8], задача в такой постановке возникает при оценке стойкости протокола установления защищенного соединения [24] между EMV-картами и банковскими терминалами. Одним из требований к протоколу является обеспечение защиты от трекинга карт, т. е. отслеживания операций, выполненных с конкретной EMV-картой. Дизайн протокола позволяет нарушить конфиденциальность данных в предположении возможности решения задачи дискретного логарифмирования для экспонент ограниченной высоты.

Основная идея протокола может быть сформулирована следующим образом. Пусть G — подгруппа группы точек эллиптической кривой, $2^{255} < |G| < 2^{256}$, P — образующий элемент G. EMV-карта обладает секретным (d_c) и открытым ($Q = d_cP$) ключами, а также сертификатом, соответствующим ключу Q.

1. Карта вырабатывает k-битное случайное число r (для повышения эффективности k рекомендуется установить равным 32) и отправляет терминалу $W = rQ$.

2. Терминал вырабатывает 256-битное случайное число d_t и отправляет карте d_tP.

3. И карта, и терминал вырабатывают общий секретный параметр rd_cd_tP:
$$rd_cd_tP = rd_c(d_tP) = d_tW.$$

4. И карта, и терминал на основе значения rd_cd_tP вырабатывают секретный ключ K.

5. Используя шифрование с аутентификацией и ключ K, карта отправляет терминалу открытый ключ Q, сертификат, а также значение r.

6. Терминал выполняет проверку $W = rQ$ и аутентифицирует открытый ключ карты, используя сертификат.

Следуя [8], обозначим P_1, P_2 значения W, перехваченные при двух различных сеансах выполнения протокола (шаг 1) для одной и той же карты. Тогда $P_1 = aQ, P_2 = bQ$ для некоторых k-битных a, b. Значение $q = b/a$ является решением задачи дискретного логарифмирования для экспонент ограниченной высоты 2^k и позволяет с достаточно большой вероятностью вычислить открытый ключ Q, что делает возможным отслеживание операций с использованием данной карты.

Пусть $\overline{P}_1 = P_1,\ \overline{P}_2 = -P_2,\ v = \beta 2^k$ для некоторого $\beta > 1,\ \beta \in \mathbb{R}$, r_1, r_2 — случайные целые числа, $0 \le r_1, r_2 < v$, $\overline{P}_3 = r_1\overline{P}_1 + r_2\overline{P}_2$, а x_1, x_2 — решение двумерной задачи дискретного логарифмирования

$$x_1\overline{P}_1 + x_2\overline{P}_2 = \overline{P}_3.$$

Тогда $(x_1 - r_1, x_2 - r_2) = (db, da)$ для некоторого целого d, и, если $d \neq 0$, с некоторой фиксированной вероятностью

$$b = \frac{x_1 - r_1}{\text{НОД}(x_1 - r_1, x_2 - r_2)},$$

$$a = \frac{x_2 - r_2}{\text{НОД}(x_1 - r_1, x_2 - r_2)}.$$

В общем случае наиболее эффективным алгоритмом решения двумерной задачи дискретного логарифмирования является алгоритм Годри-Шоста, предложенный в 2004 году в работе [30]. Основная идея алгоритма может быть сформулирована следующим образом. Сначала выбираются так называемые «домашнее» (tame) и «дикое» (wild) множества:

$$T = \{-N_1, \ldots, N_1\} \times \{-N_2, \ldots, N_2\},$$

$$W = \{-N_1 + n_1, \ldots, N_1 + n_1\} \times \{-N_2 + n_2, \ldots, N_2 + n_2\}.$$

Затем параллельно вычисляются псевдослучайные последовательности

$$x_i P_1 + y_i P_2, (x_i, y_i) \in T, i = 1, 2, \ldots, \tag{1.6}$$

$$Q + z_j P_1 + w_j P_2, (n_1 + z_j, n_2 + w_j) \in W, j = 1, 2, \ldots \tag{1.7}$$

до тех пор, пока в них не найдутся два одинаковых элемента:

$$x_k P_1 + y_k P_2 = Q + z_l P_1 + w_l P_2, \tag{1.8}$$

откуда находим $n'_1 = x_k - z_l, n'_2 = y_k - w_l$.

Процесс выработки элементов последовательностей (1.6) и (1.7) осуществляется псевдослучайным блужданием, определяемым следующим образом. Пусть для группы G заданы $m_s \in \mathbf{N}, m_s > 1$, хэш-функция $\psi : G \to \{1, ..., m_s\}$, а также функции $F, F_1, ..., F_{m_s} : G \to G$ такие, что

$$F(u) = \begin{cases} F_1(u), \text{ если } \psi(u) = 1 \\ F_2(u), \text{ если } \psi(u) = 2 \\ \vdots \\ F_{m_s}(u), \text{ если } \psi(u) = m_s \end{cases}$$

Для начального элемента $u_0 \in_R G$ последовательность $u_0, u_1 = F(u_0), ..., u_{i+1} = F(u_i), ...$ называется *псевдослучайным блужданием.* Важно заметить, что параметры псевдослучайного блуждания m_s, ψ, F выбираются таким образом, чтобы действие F было максимально похоже на случайный равновероятный выбор элементов. В качестве хэш-функции возможно использование, например,

$$\psi(u) = \lfloor \psi^*(u) \cdot m_s \rfloor + 1, \tag{1.9}$$

где $\psi^*(u) = A \cdot b(u) - \lfloor A \cdot b(u) \rfloor$, $b(u) : G \to \mathbf{N}$ — представление натуральным числом двоичной записи элемента G, A — рациональная аппроксимация золотого сечения $\frac{\sqrt{5}-1}{2}$. Как показано в работе Кнута [2], при достаточно большом значении знаменателя в аппроксимации золотого сечения распределение $\psi(u)$ получается достаточно близким к равномерному. На практике также могут использоваться другие функции ψ,

допускающие эффективную реализацию. Кроме того, в работе [60] показано, что для получения функции F, действие которой максимально похоже на случайный равновероятный выбор элементов в G, параметр m_s достаточно выбирать равным 20. Функции псевдослучайного блуждания, следуя работе [28], могут быть заданы следующим образом:

$$F_i(u) = u + \gamma_{\psi(u)},$$

где

$$\gamma_i = \zeta_i^{'} P_1 + \zeta_i^{''} P_2,\ 1 \le i \le m_s,$$
$$\zeta_i^{'}, \zeta_i^{''} \in_R \{-2M, ..., 2M\}, M \in \mathbf{N}.$$

Так как значения $\gamma_{\psi(u)}$ могут быть предвычислены, а трудоемкость вычисления $\psi(u)$ пренебрежимо мала по сравнению с трудоемкостью групповой операции в G, то трудоемкость вычисления очередного элемента псевдослучайного блуждания сравнима с трудоемкостью групповой операции в G. Поэтому в литературе средняя трудоемкость алгоритма Годри-Шоста традиционно измеряется количеством групповых операций в G и равна среднему значению количества элементов последовательностей (1.6) и (1.7), вычисляемых до появления совпадающих элементов (равенство (1.8)), в предположении, что значения (n_1, n_2), (x_i, y_i) и (z_j, w_j) выбираются случайно равновероятно и независимо из соответствующих множеств.

Средняя трудоемкость алгоритма Годри-Шоста определяется с использованием следующего результата Гэлбрайта и Холмса, являющегося обобщением парадокса дней рождения.

Теорема 1. *[25, Theorem 1] Предположим, что выполнены следующие условия.*

1. *В случайной последовательности шаров каждый шар имеет один из C цветов; j-й шар независимо от остальных имеет цвет $c \in \{1, \dots, C\}$ с вероятностью $r_{j,c}$, $j = 1, 2, \dots$ Для любого $c \in \{1, \dots, C\}$, существует*

$$p_c = \lim_{n \to \infty} n^{-1} \sum_{k=1}^{n} r_{j,c}$$

и $p_1 \geq p_2 \geq \cdots \geq p_C > 0$. *Пусть* $b_{n,c} = p_c - n^{-1}\sum_{k=1}^{n} r_{j,c}$ *и существует константа* K *такая, что для любого* $c \in \{1, \ldots, C\}$, $n > 1$ *выполняется неравенство* $|b_{n,c}| \leq K/n$.

2. *Имеется* $N' \in \mathbb{N}$ *различных урн. Если* j*-й шар имеет цвет* c, *то он попадает в урну с номером* i *с вероятностью* $q_{c,i}(N')$ *независимо от цветов и размещений остальных шаров. Существует такое* $d > 0$, *не зависящее от* N' *и* c, *что для любых* $c = 1, \ldots, C$ *и* $i = 1, \ldots, N'$,

$$0 \leq q_{c,i} \leq d/N'.$$

Существуют такие константы $\alpha, \mu > 0$, *что*

$$|\{i \in \{1, \ldots, N'\} : q_{1,i}, q_{2,i} \geq \mu/N'\}| \geq \alpha N'.$$

Тогда математическое ожидание числа $Z_{N'}$ *шаров, размещенных до первого появления двух шаров разных цветов в одной урне, равно*

$$\mathbf{M}(Z_{N'}) = \sqrt{\frac{\pi}{2A_{N'}}} + O(N'^{1/4}),$$

где

$$A_{N'} = \sum_{c=1}^{C} p_c \left(\sum_{c'=1, c \neq c'}^{C} p_{c'} \left(\sum_{i=1}^{N'} q_{c,i} q_{c',i} \right) \right)$$

и константа в O *зависит от* $C, p_c, d, K, \alpha, \mu$, *но не зависит от* N' *и* $q_{c,i}$.

Средняя трудоемкость алгоритма Годри-Шоста вычислена Гэлбрайтом и Рупраи в работе [27] и составляет $(2.43+o(1))\sqrt{N}$, где $N = 4N_1N_2$, $o(1) \to 0$ при $N_1, N_2 \to \infty$. В той же работе предложена усовершенствованная версия алгоритма с трудоемкостью $(2.36 + o(1))\sqrt{N}$.

Пусть группа G — циклическая простого порядка и обладает эффективным автоморфизмом φ, действующим в группе G как умножение на $\lambda \in \{1, \ldots, |G|-1\}$. Тогда, подобно тому, как это делается для классической задачи дискретного логарифмирования, можно ускорить алгоритм, если искать не совпадающие элементы последовательностей (1.6) и (1.7),

а совпадающие классы эквивалентности этих элементов. Действительно, в этом случае вместо равенства (1.8) имеем равенство

$$\varphi^s(x_kP_1 + y_kP_2) = Q + z_lP_1 + w_lP_2, \tag{1.10}$$

для некоторого s, откуда

$$Q = (\lambda^s x_k - z_l)P_1 + (\lambda^s y_k - w_l)P_2,$$

т. е. $n_1' = \lambda^s x_k - z_l, n_2' = \lambda^s y_k - w_l$.

При практической реализации алгоритма в этом случае можно сохранять не сами элементы последовательностей (1.6) и (1.7), а лишь представителей соответствующих классов эквивалентности, порожденных ими, например, элементы с меньшей x-координатой в лексикографическом порядке. Так как вычислительная сложность определения представителя класса эквивалентности существенно меньше вычислительной сложности групповой операции, то средняя трудоемкость алгоритма попрежнему может измеряться количеством групповых операций в G и сопоставима с количеством элементов последовательностей, вычисляемых до появления совпадающих.

Примерами групп *с эффективными автоморфизмами* являются подгруппы групп точек эллиптических кривых над конечным простым полем $GF(p)$.

1. Подгруппа G группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов, очевидно, обладает автоморфизмом порядка 2 с $\lambda = -1$ (операция взятия обратного элемента $\varphi(x, y) = (x, -y)$), тогда

   $$\varphi(aP_1 + bP_2) = -aP_1 - bP_2,$$

   и класс эквивалентности точки $aP_1 + bP_2$ относительно действия группы $\langle\varphi\rangle$ состоит из $aP_1 + bP_2$ и $\varphi(aP_1 + bP_2)$. Каждому такому классу эквивалентности соответствует множество (класс) пар

   $$C(a, b) = \{(a, b), (-a, -b)\}.$$

В работе Лиу [43] для этого случая предложена соответствующая модификация алгоритма Годри-Шоста, имеющая при $N \to \infty$ трудоемкость $(1.45 + o(1))\sqrt{N}$ групповых операций. Для получения этого результата Лиу использует «домашнее» множество

$$T = \{C(a,b) : -\frac{17}{20}N_1 \le a \le \frac{17}{20}N_1, \\ -\frac{17}{20}N_1 \le b \le \frac{17}{20}N_1\}, \quad (1.11)$$

и «дикое» множество

$$W = \{\{(n_1 + a, n_2 + b), (-n_1 - a, -n_2 - b)\} : \\ -\frac{N_1}{2} \le a \le \frac{N_1}{2}, -\frac{N_1}{2} \le b \le \frac{N_1}{2}\}. \quad (1.12)$$

Используя описанный автоморфизм φ, получаем, что множество «представителей» для каждого класса $C(a,b) \in T$ равно

$$\widetilde{T} = \{(a,b) : -\frac{17}{20}N_1 \le a \le \frac{17}{20}N_1, -a \le b \le \frac{17}{20}N_1\}. \quad (1.13)$$

На Рис. 1.1 изображены «дикое» множество, множество T_0 — объединение классов из множества T, а также пересечение $U = \widetilde{W} \cap \widetilde{T}$, где

$$\widetilde{W} = \{(n_1 + a, n_2 + b) : -\frac{N_1}{2} \le a \le \frac{N_1}{2}, -\frac{N_1}{2} \le b \le \frac{N_1}{2}\}$$

2. Подгруппа G простого порядка q группы точек эллиптической кривой, заданной уравнением $y^2 = x^3 + Ax$, при $p \equiv 1 \bmod 4$ и $q^2 \nmid \#E$ обладает эффективным автоморфизмом порядка 4: $\varphi(x,y) = (-x, \alpha y)$, где α — элемент порядка 4 по модулю p, λ — корень уравнения $\lambda^2 \equiv -1 \pmod q$. Если $P_2 = \varphi(P_1)$, то

$$\varphi(aP_1 + bP_2) = a(\lambda P_1) + b(\lambda^2)P_1 = -bP_1 + aP_2,$$

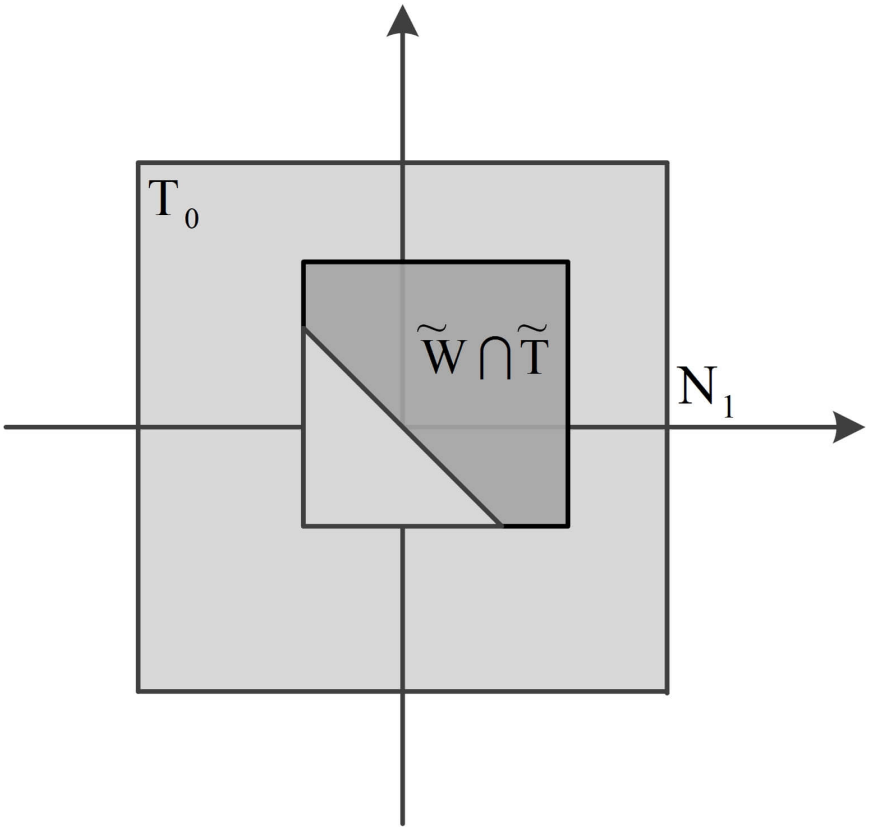

Рис. 1.1.

откуда

$$\varphi^2(aP_1 + bP_2) = -aP_1 - bP_2,$$
$$\varphi^3(aP_1 + bP_2) = bP_1 - aP_2,$$

и класс эквивалентности точки $aP_1 + bP_2$ относительно действия группы $\langle\varphi\rangle$ включает 4 указанные точки. Каждому такому классу эквивалентности соответствует множество (класс) пар

$$C(a, b) = \{(a, b), (-a, b), (-a, -b), (a, -b)\}.$$

В той же работе Лиу [43] для этого случая получена трудоемкость (при $N_1 = N_2$) $(1.0255 + o(1))\sqrt{N}$ групповых операций. Для получения этого результата Лиу использует в качестве «домашнего»

множества [1]

$$T = \{C(a,b) : \\ -(1-\tau)N_1 \le a \le (1-\tau)N_1, -(1-\tau)N_1 \le b \le (1-\tau)N_1\},$$

где $\tau = 0.1467$, а также «дикое» множество

$$W = \{C(n_1 + a, n_2 + b) : \\ -\frac{N_1}{2} \le a \le \frac{N_1}{2}, -\frac{N_1}{2} \le b \le \frac{N_1}{2}\}. \quad (1.14)$$

Используя описанный автоморфизм φ, получаем, что множество «представителей» для каждого класса $C(a,b) \in T$ равно

$$\widetilde{T} = \{(a,b) : 0 \le a \le (1-\tau)N_1, 0 \le b \le (1-\tau)N_1\}.$$

На рис. 1.2 изображены «дикое» множество, множество T_0 — объединение классов из множества T, а также пересечение $U = \widetilde{W} \cap \widetilde{T}$, где

$$\widetilde{W} = \{(n_1 + a, n_2 + b) : -\frac{N_1}{2} \le a \le \frac{N_1}{2}, -\frac{N_1}{2} \le b \le \frac{N_1}{2}\}.$$

1.3 Задача дискретного логарифмирования в интервале

Определение 5. *Задача дискретного логарифмирования в интервале.*
Дано: группа $G = \langle P \rangle$, $Q \in G$, $N \in \mathbb{N}$, $2|N$, $N < |G| - 1$, $Q = nP$ *для некоторого (неизвестного)* $n \in \{-\frac{N}{2}, \ldots, \frac{N}{2}\}$.
Найти: n.

Одним из возможных вариантов увеличения производительности практических реализаций методов защиты информации, основанных на

[1] для получения значения τ в работе Лиу рассматриваются различные значения «сжатия» домашнего множества и «растяжения» дикого множества

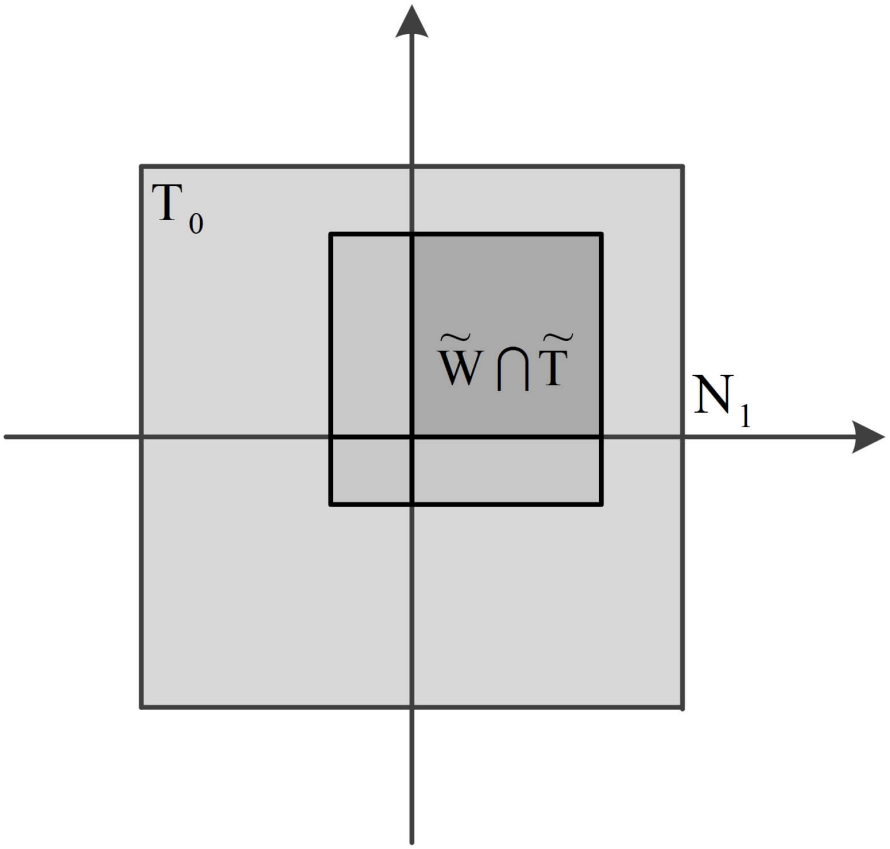

Рис. 1.2.

вычислении кратной точки (в мультипликативной записи — возведении в степень) aP в циклической группе G простого порядка, где a — секретное значение, является введение ограничений на параметр a. Примеры использования таких ограничений описаны в работах [50, 52, 31].

С другой стороны, дополнительная информация о секретном значении a дает возможность использовать алгоритмы решения задачи дискретного логарифмирования в интервале, которые при определенных границах на значение a оказываются эффективнее алгоритмов решения классической задачи дискретного логарифмирования.

Кроме того, для двоичного представления секретной экспоненты

$$a = (a_u, \ldots, a_0),$$

$$u = \lceil \log_2 |G| \rceil,$$

в ряде случаев удается получить значения некоторых бит, используя утечки по побочным каналам [34]. Если $a = a' 2^{\overline{u}} + \overline{a}$, где $\overline{a}$ известно,

$\overline{a} < 2^{\overline{u}} < 2^u$, то для вычисления значения a по $aP = Q$ достаточно найти такое a', что:

$$\begin{cases} a'(2^{\overline{u}}P) = Q - \overline{a}P, \\ 0 < a' < 2^{u-\overline{u}} \end{cases}$$

В этом случае решение задачи дискретного логарифмирования в интервале также может оказаться более эффективным способом нахождения значения a.

Одним из методов решения задачи дискретного логарифмирования в интервале является метод Шенкса [56], требующий в среднем $2\sqrt{N}$ групповых операций и размещения в памяти $O(\sqrt{N})$ элементов группы.

Другим методом решения задачи дискретного логарифмирования в интервале, лишенным недостатка необходимости большого количества памяти, является разработанный Поллардом метод Кенгуру [53, 54]. При использовании техники отмеченных (distinguished) точек [51] оценка средней трудоемкости решения задачи методом Кенгуру составляет $2\sqrt{N}$ групповых операций, при этом требуется размещение в памяти лишь $O(\theta\sqrt{N})$ элементов группы, где θ — вероятность, что случайно выбранный элемент группы является отмеченным.

Еще одним эффективным алгоритмом решения задачи дискретного логарифмирования в интервале является алгоритм Годри-Шоста [28, 30]. Как и для двумерной задачи, алгоритм Годри-Шоста требует выбора «домашнего» и «дикого» множеств:

$$T = \{-\frac{N}{2}, \ldots, \frac{N}{2}\},$$

$$W = \{-\frac{N}{2} + n, \ldots, \frac{N}{2} + n\}.$$

Затем параллельно вычисляются псевдослучайные последовательности

$$x_i P, x_i \in T, i = 1, 2, \ldots, \tag{1.15}$$

$$Q + z_j P, n + z_j \in W, j = 1, 2, \ldots \tag{1.16}$$

до тех пор, пока в них не найдутся два одинаковых элемента:

$$x_k P = Q + z_l P, \tag{1.17}$$

откуда находим $n = x_k - z_l$.

Как и в случае классической и двумерной задач дискретного логарифмирования, для оптимизации методов решения задачи дискретного логарифмирования в интервале можно использовать наличие у исходной группы эффективного автоморфизма. Но в случае задачи дискретного логарифмирования в интервале подойдут только автоморфизмы, дающие такие классы эквивалентности, все элементы которых лежат в том же интервале, что и решение задачи. Итак, предположим теперь, что группа G обладает эффективно вычислимой операцией взятия обратного элемента, т. е. время, необходимое для вычисления обратного элемента, существенно меньше времени, необходимого для выполнения одной групповой операции. Тогда можно модифицировать алгоритм Годри-Шоста, учитывая обратные элементы при поиске совпадающих элементов последовательностей (1.15) и (1.16). Это можно сделать, изменив равенства (1.17):

$$(-1)^s(x_kP) = Q + z_lP, \tag{1.18}$$

для некоторого $s \in \{0, 1\}$, откуда

$$Q = ((-1)^s x_k - z_l)P, s \in \{0, 1\},$$

т. е. $n = (-1)^s x_k - z_l$, $s \in \{0, 1\}$.

При практической реализации алгоритма в этом случае можно сохранять не сами элементы последовательностей (1.15) и (1.16), а лишь представителей соответствующих классов эквивалентности, порожденных ими, например, наименьший элемент в лексикографическом порядке. Примером такой группы *с эффективным инвертированием* является группа точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов, действительно,

$$-(x, y) = (x, -y),$$

и класс эквивалентности точки aP, порожденный действием операции взятия обратного элемента группы, состоит из aP и $-aP$. Каждому такому классу эквивалентности соответствует множество (класс) пар

$$C(a) = \{a, -a\}.$$

В работе [28] для этого случая предложена соответствующая модификация алгоритма Годри-Шоста, имеющая при $N \to \infty$ трудоемкость $(1.36 + o(1))\sqrt{N}$ групповых операций. Для получения этого результата использовались «домашнее» множество вида

$$T = \{C(a) : -\frac{N}{2} \le a \le \frac{N}{2}\},$$

а также «дикое» множество

$$W = \{C(n + a) : -\frac{N}{4} \le a \le \frac{N}{4}\}$$

Используя описанный автоморфизм, получим, что множество «представителей» для каждого класса $C(a) \in T$ равно

$$\widetilde{T} = \{a : 0 \le a \le \frac{N}{2}\}$$

На Рис. 1.3 изображены множества T_0 (объединение классов из множества T), $\widetilde{T}$, $\widetilde{W}$, $\widetilde{W} \cap \widetilde{T}$, где

$$\widetilde{W} = \{(n + a) : -\frac{N}{4} \le a \le \frac{N}{4}\}$$

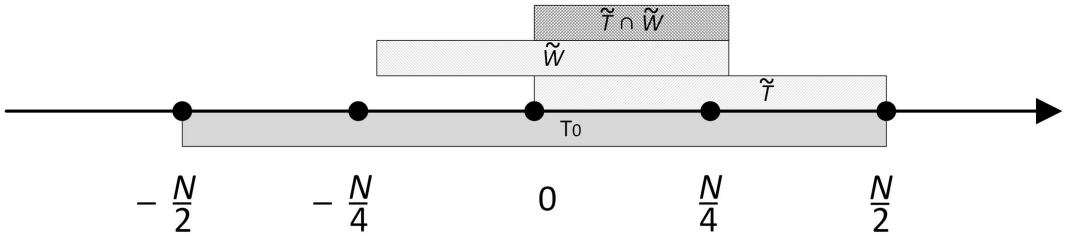

Рис. 1.3.

1.4 О достижимости теоретических оценок средней трудоемкости

Как было отмечено в § 1.2, § 1.3, для групп с эффективными автоморфизмами возможно получение модификаций алгоритма Годри-Шоста,

обладающих сравнительно меньшей трудоемкостью, которая достигается за счет того, что работа производится не с элементами исходных групп, а с представителями соответствующих классов эквивалентности. При этом трудоемкость вычисления представителя класса эквивалентности, порожденного действием эффективного автоморфизма, в литературе принято считать пренебрежимо малой по отношению к трудоемкости групповой операции и не учитывать в теоретических оценках ([64, 43, 28, 19]). В этом параграфе мы оценим погрешность оценок трудоемкости различных модификаций алгоритма Годри-Шоста при использовании такого допущения и покажем, что оно является вполне адекватным.

Справедливы следующие оценки трудоемкости вычисления представителя класса эквивалентности, порожденного действием эффективного автоморфизма.

1) В случае подгруппы G группы точек эллиптической кривой E, заданной уравнением $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов, рассмотрим эффективный автоморфизм порядка 2 с $\lambda = -1$ (операция взятия обратного элемента $\varphi(x, y) = (x, -y)$). Класс эквивалентности точки $P' = (x, y)$ состоит из двух элементов: $\{P', -P'\} = \{(x, y), (x, -y)\}$. Представителем такого класса может служить элемент с нечетной $y-$координатой, для вычисления которого в худшем случае требуется 1 операция взятия противоположного элемента в $GF(p)$. Однако, в среднем половина элементов псевдослучайного блуждания уже будут обладать нечетной $y-$координатой, т. е. будут являться представителями соответствующих классов.

2) В случае подгруппы G порядка q группы точек эллиптической кривой E, заданной уравнением $y^2 = x^3 + Ax$ над конечным простым полем из $p \equiv 1 \bmod 4$ элементов, $q^2 \nmid \#E$, рассмотрим эффективный автоморфизм порядка 4: $\varphi(x, y) = (-x, \alpha y)$, где α — элемент порядка 4 по модулю p, λ — корень уравнения $\lambda^2 \equiv -1 \pmod q$. Класс эквивалентности точки $P' = (x, y)$ состоит из четырех элементов $\{P', -P', \varphi(P'), -\varphi(P')\} = \{(x, y), (x, -y), (-x, \alpha y), (-x, -\alpha y)\}$.

Представителем такого класса может служить элемент с нечетной $x-$координатой и нечетной $y-$координатой, для его вычисления в худшем случае требуется 1 операция умножения на константу и 2 операции взятия противоположного элемента в $GF(p)$.

3) В случае подгруппы G порядка q группы точек эллиптической кривой E, заданной уравнением $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов, $q^2 \nmid \#E$, рассмотрим эффективный автоморфизм порядка 6: $\varphi(x, y) = (\beta x, -y)$, где $\beta \neq 1$ — кубический корень из 1 по модулю p, λ — корень уравнения $\lambda^2 - \lambda + 1 \equiv 0 \pmod{q}$. Класс эквивалентности точки $P' = (x, y)$ состоит из шести элементов $\{P', -P', \varphi(P'), -\varphi(P'), \varphi^2(P'), -\varphi^2(P')\} = \{(x, y), (x, -y), (\beta x, -y), (\beta x, y), (\beta^2 x, y), (\beta^2 x, -y)\}$. Представителем такого класса может служить элемент с меньшей $x-$координатой и нечетной $y-$координатой. В силу того, что $\beta^2 x = (\beta - 1)x$, для вычисления представителя класса в худшем случае требуется 1 операция умножения на константу, 1 операция сложения и 2 операции взятия противоположного элемента в поле $GF(p)$.

С другой стороны, трудоемкость групповой операции сложения точек эллиптической кривой в аффинных координатах (см. (1.1)) может быть оценена [35, 18, 62] трудоемкостью 1 операции взятии обратного элемента, 2 операций умножения и 1 операции возведения в квадрат в поле $GF(p)$. Трудоемкость операции удвоения точек эллиптической кривой в аффинных координатах (см. (1.2)) может быть оценена [35, 18, 62] трудоемкостью 1 операции взятия обратного элемента, 2 операций умножения и 2 операций возведения в квадрат в поле $GF(p)$. Стоит заметить, что использование проективных координат позволяет применять формулы сложения и удвоения точек эллиптической кривой, не содержащие операции взятия обратного элемента, и, тем самым, существенно сократить трудоемкость групповой операции. Однако, в настоящее время нет известных эффективных методов работы с псевдослучайными блужданиями в проективных координатах [11]. Это связано с тем, что

в проективных координатах одновременно несколько элементов могут соответствовать единственному элементу в аффинных.

Трудоемкость операции взятия обратного элемента может сильно варьироваться в зависимости от характеристики и размера поля, а при практической реализации — также от архитектуры используемого вычислителя. Ряд практических экспериментов [57, 35] показывает, что для многих используемых на практике конечных простых полей трудоемкость операции получения обратного элемента превышает трудоемкость умножения в среднем в 80 раз.

На основании вышесказанного можно сделать вывод, что в рассматриваемых случаях трудоемкость определения представителя класса эквивалентности, порожденного эффективным автоморфизмом, меньше трудоемкости групповой операции в среднем более чем в 83 раза. Тогда дополнительные вычисления, требуемые для определения представителя класса эквивалентности, при практической реализации (без распараллеливания) модификаций алгоритма Годри-Шоста, использующих эффективные автоморфизмы, увеличивают теоретическую оценку средней трудоемкости не более, чем на 1.2%.

В случае параллельной реализации вариантов алгоритма Годри-Шоста одновременно выполняется множество псевдослучайных блужданий, что допускает использование метода *одновременного инвертирования Монтогомери* [46]. В этом случае, при достаточно большом количестве одновременно выполняемых псевдослучайных блужданий, среднее время выполнения операции инвертирования сопоставимо с трудоемкостью выполнения 3 умножений в $GF(p)$. Тогда трудоемкость определения представителя класса эквивалентности, порожденного эффективным автоморфизмом, меньше трудоемкости групповой операции в среднем более чем в 6 раз, а дополнительные вычисления, требуемые для определения представителя класса эквивалентности, при практической реализации такого алгоритма увеличивают теоретическую оценку средней трудоемкости не более, чем в $\frac{7}{6}$ раз [11].

Необходимо заметить, что для получения представителя класса эк-

вивалентности, порожденного эффективным автоморфизмом, выполняется умножение на константу, а не на произвольный элемент $GF(p)$. Этот факт позволяет оптимизировать практическую реализацию. Действительно, пусть α — константа, умножение на которую выполняется при вычислении автоморфизма, $0 < w < \log_2 p, w \in \mathbb{N}$, тогда можно предвычислить таблицу M:

$$M[v,i] = v \cdot 2^{iw} \cdot \alpha \mod p,$$

$$\text{для } v = 0, \ldots, 2^w - 1,\ i = 0, \ldots, \left\lfloor \frac{\log_2 p}{w} \right\rfloor.$$

Тогда для любого $x \in GF(p)$ справедливо следующее равенство:

$$x \cdot \alpha = \sum_{i=0}^{\left\lfloor \frac{\log_2 p}{w} \right\rfloor} M \left[\frac{x}{2^{iw}} \mod 2^w,\ i \right] \mod p. \tag{1.19}$$

Используя представление (1.19), операцию умножения на α в $GF(p)$ можно заменить на $\left\lfloor \frac{\log_2 p}{w} \right\rfloor$ операций сложения.

Эффективность использования представления (1.19) и соответствующих предвычислений зависит от характеристики и размера поля. Например, для $GF(2^{521}-1)$, входящего в состав стандартизованного NIST [38] набора параметров *P-521*, трудоемкость операции сложения в среднем в 29 раз меньше трудоемкости операции умножения [57]. Тогда, при использовании $w = 32$ и предвычисленного M, трудоемкость определения представителя класса эквивалентности, порожденного эффективным автоморфизмом соответствующей эллиптической кривой, при реализации параллельного алгоритма становится меньше трудоемкости групповой операции в среднем в 10.9 раз, и в 150.4 раз — при реализации классического алгоритма. Таким образом, дополнительные вычисления, требуемые для определения представителя класса эквивалентности, при реализации параллельного алгоритма увеличивают теоретическую оценку средней трудоемкости менее, чем на 10%, а при реализации классического алгоритма — менее, чем на 0.66%.

Исходя из вышесказанного, в настоящей работе **трудоемкость** алгоритма Годри-Шоста решения двумерной задачи дискретного логарифми-

рования (задачи дискретного логарифмирования в интервале) и его различных модификаций измеряется в групповых операциях в G и равна количеству элементов последовательностей (1.6) и (1.7) ((1.15) и (1.16) соответственно), вычисляемых до появления совпадающих элементов (равенство (1.8) ((1.17) соответственно)) или классов эквивалентности (равенство (1.10) ((1.18) соответственно)).

1.5 Выводы

К основным выводам главы 1 относятся следующие.

1. Оценка трудоемкости решения различных обобщений задачи дискретного логарифмирования должна учитываться при анализе стойкости ряда механизмов защиты информации на основе эллиптических кривых.

2. Для решения некоторых обобщений задачи дискретного логарифмирования в случае эллиптических кривых, обладающих эффективным автоморфизмом, возможно использование алгоритмов, обладающих меньшей средней трудоемкостью по сравнению с классическим алгоритмом Годри-Шоста.

В силу того, что для двумерной задачи дискретного логарифмирования получены модификации алгоритма Годри-Шоста лишь для случая эллиптических кривых, обладающих эффективными автоморфизмами порядка 2 и 4, научный интерес представляет получение соответствующих модификаций алгоритма для других классов эллиптических кривых. Следующая глава посвящена построению модификации алгоритма Годри-Шоста для класса эллиптических кривых, обладающих эффективным автоморфизмом порядка 6.

Глава 2

Алгоритм решения двумерной задачи дискретного логарифмирования в конечной циклической группе с эффективным автоморфизмом порядка 6

В настоящей главе конструктивно доказывается возможность снижения трудоемкости решения двумерной задачи дискретного логарифмирования для класса эллиптических кривых, обладающих эффективным автоморфизмом порядка 6, а также приводится оценка средней трудоемкости соответствующего алгоритма.

2.1 Описание автоморфизма порядка 6 для некоторого класса эллиптических кривых

Как показано в главе 1, для эллиптических кривых, обладающих эффективными автоморфизмами порядка 2 и 4, существуют алгоритмы решения двумерной задачи дискретного логарифмирования, обладающие меньшей оценкой средней трудоемкости по сравнению с классическим алгоритмом Годри-Шоста. Кроме того, работа Лиу [43] позволяет предположить, что использование автоморфизмов более высоких порядков позволит получить еще более эффективные алгоритмы.

Подгруппа G простого порядка q группы точек эллиптической кривой E, заданной над $GF(p)$ уравнением $y^2 = x^3 + B$ при $p \equiv 1 \pmod 3$, $q^2 \nmid \#E$ обладает эффективным автоморфизмом φ порядка 6, $\varphi(x, y) = (\beta x, -y)$, где $\beta \neq 1$ — кубический корень из 1 по модулю p, λ — корень уравнения $\lambda^2 - \lambda + 1 \equiv 0 \pmod q$. Для точки $P = (x, y)$ класс эквивалентности представлен шестью элементами:

$$\{(x, y), (\beta x, -y), (\beta^2 x, y), (x, -y), (\beta x, y), (\beta^2 x, -y)\}.$$

Если $P_2 = \varphi(P_1)$, то

$$\varphi(aP_1 + bP_2) = a(\lambda P_1) + b(\lambda - 1)P_1 = -bP_1 + (a + b)P_2,$$

откуда

$$\begin{gathered}
\varphi^2(aP_1 + bP_2) = -(a + b)P_1 + aP_2, \\
\varphi^3(aP_1 + bP_2) = -aP_1 - bP_2, \\
\varphi^4(aP_1 + bP_2) = bP_1 - (a + b)P_2, \\
\varphi^5(aP_1 + bP_2) = (a + b)P_1 - aP_2,
\end{gathered}$$

т. е. класс эквивалентности точки $aP_1 + bP_2$ относительно действия группы $\langle\varphi\rangle$ включает также указанные пять точек. Каждому такому классу

эквивалентности соответствует множество (класс) пар

$$C(a,b) = \{(a,b), (-b, a+b), (-(a+b), a), \\ (-a,-b), (b, -(a+b)), (a+b, -a)\}. \quad (2.1)$$

Полученное описание класса эквивалентности точек $aP_1 + bP_2$ относительно действия группы $\langle\varphi\rangle$ используется в дальнейшей части работы для оценки средней трудоемкости модификации алгоритма Годри-Шоста.

2.2 Алгоритм и оценка средней трудоемкости

Для класса эллиптических кривых, описанного в § 2.1, автором получена наиболее эффективная модификация алгоритма Годри-Шоста решения двумерной задачи дискретного логарифмирования. Следующая теорема конструктивно доказывает существование такой модификации, а также оценивает ее среднюю трудоемкость.

Теорема 2. *[5] Пусть G — подгруппа простого порядка q группы точек эллиптической кривой E, заданной над конечным простым полем $GF(p)$ уравнением $y^2 = x^3 + B$ при $p \equiv 1 \pmod 3$, $q^2 \nmid \#E$; φ — автоморфизм группы G, $\varphi(x,y) = (\beta x, -y)$, где $\beta \neq 1$ — кубический корень из 1 по модулю p; λ — корень уравнения $\lambda^2 - \lambda + 1 \equiv 0 \pmod q$ такой, что $\varphi(x,y) = \lambda(x,y)$. Тогда средняя трудоемкость решения двумерной задачи дискретного логарифмирования в группе G при $N_1 = N_2$, $P_2 = \varphi(P_1)$ и случайном равновероятном выборе (n_1, n_2) не превосходит $(0.97811 + o(1))\sqrt{N}$ групповых операций, где $N = 4N_1N_2, N \to \infty$.*

Доказательство. В качестве «домашнего» множества T возьмем

$$T = \{C(a,b) : -N_1 \leq a \leq N_1, -N_1 \leq b \leq N_1\}.$$

Заметим, что элементы множества T находятся во взаимно однозначном соответствии с элементами множества представителей классов

$$\widetilde{T} = \{0, \ldots, N_1\} \times \{1, \ldots, N_1\} \cup \{(0,0)\}^{(1)}$$

(в работах [28, 43] такое множество называется фундаментальной областью «домашнего» множества). На рисунке 2.1 изображено объединение классов из множества T (обозначим его T_0), множество $\widetilde{T}$ — часть изображения, ограниченная первым квадрантом плоскости.

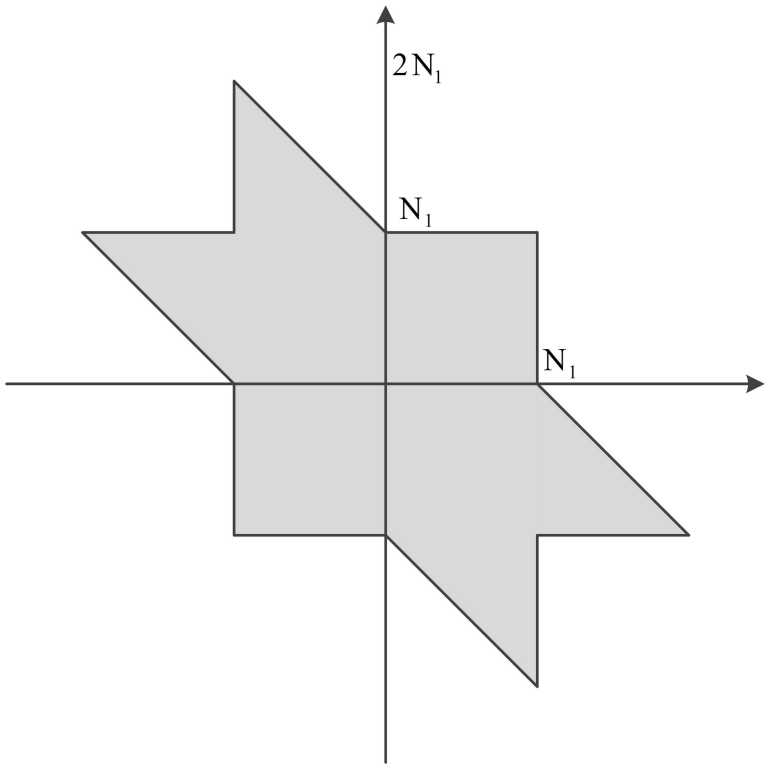

Рис. 2.1.

Определим «дикое» множество

$$W = \{C(n_1 + a, n_2 + b) : -\frac{N_1}{2} \le a \le \frac{N_1}{2}, -\frac{N_1}{2} \le b \le \frac{N_1}{2}\}$$

и множество

$$\widetilde{W} = \{-\frac{N_1}{2} + n_1, \ldots, \frac{N_1}{2} + n_1\} \times \{-\frac{N_1}{2} + n_2, \ldots, \frac{N_1}{2} + n_2\}$$

[(1)] в множество $\widetilde{T}$ не включены элементы вида $\{(a,0)|a > 0\}$, так как в соответствии с (2.1) такой элемент принадлежит классу $C(0,a)$

(при $n_1 = n_2 = 0$ множество $\widetilde{W}$ изображено на рисунке 2.2 — выделено темно серым цветом).

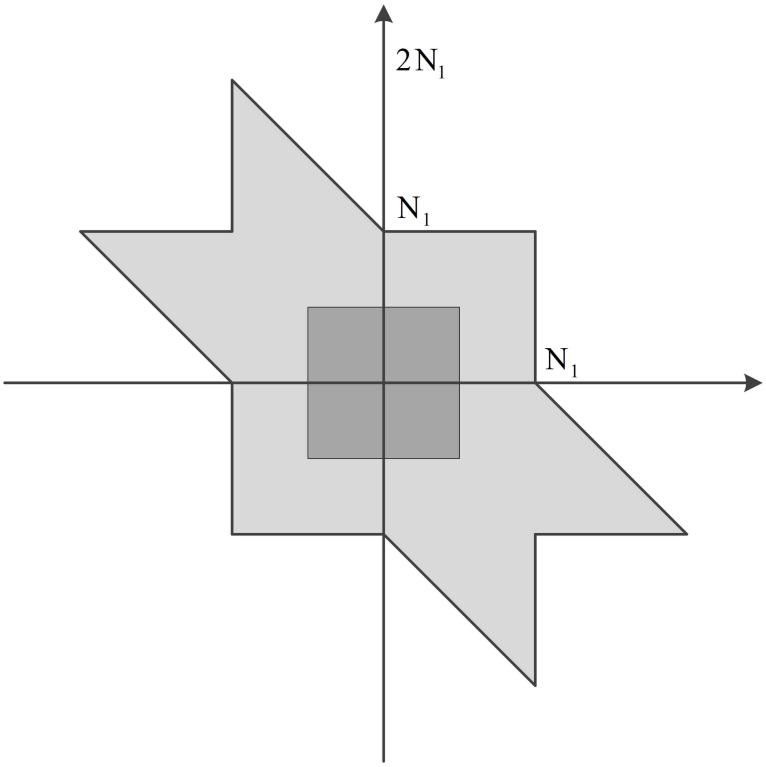

Рис. 2.2.

Как и в алгоритме Годри-Шоста, будем параллельно вычислять последовательности точек

$$x_i P_1 + y_i P_2, (x_i, y_i) \in \widetilde{T}, i = 1, 2, \ldots, \tag{2.2}$$

$$Q + z_j P_1 + w_j P_2, (z_j, w_j) \in \widetilde{W}, j = 1, 2, \ldots \tag{2.3}$$

до тех пор, пока в них не найдутся две точки из одного класса эквивалентности, после чего находим решение задачи как показано в § 1.2. (При этом предполагается, что значения (x_i, y_i) и (z_j, w_j) выбираются случайно равновероятно и независимо из соответствующих множеств.)

Для определения средней трудоемкости алгоритма воспользуемся теоремой 1. В обозначениях теоремы в нашем случае $C = 2$: шары цвета 1 — это элементы множества $\widetilde{T}$, а шары цвета 2 — элементы множества $\widetilde{W}$. Так как вычисление последовательностей (2.2) и (2.3) происходит параллельно, мы можем считать, что $r_{j,1} = r_{j,2} = \frac{1}{2}$ для всех $j = 1, 2, \ldots,$

откуда $p_1 = p_2 = \frac{1}{2}$. Множество урн в нашем случае — это $T \cup W$, и шар (a, b) попадает в урну $C(a, b)$. Ясно, что $N' = O(N)$.

Очевидно, что интересующая нас средняя трудоемкость, выраженная в количестве групповых операций, не превосходит математического ожидания суммарного числа $Z_{N'}$ значений (x_i, y_i) и $(n_1 + z_j, n_2 + w_j)$, выбираемых до появления значений (x_k, y_k) и $(n_1 + z_l, n_2 + w_l)$ таких, что $C(x_k, y_k) = C(n_1 + z_l, n_2 + w_l)$. Вычислим условное математическое ожидание $\mathbf{M}(Z_{N'}|(n_1, n_2))$ случайной величины $Z_{N'}$ при фиксированных n_1, n_2.

В целях упрощения записи, далее величины $o(N)$ при $N \to \infty$ будут опускаться. Тогда имеем: $|T| = |\widetilde{T}| = |\widetilde{W}| = \frac{N}{4}$ и

$$q_{1,i} = \begin{cases} \frac{4}{N}, & \text{если } i \in T \\ 0, & \text{в противном случае} \end{cases}.$$

С учетом последнего равенства и утверждения теоремы 1 нас интересуют значения $q_{2,i}$ только для $i \in T \cap W$. Поскольку каждый класс $C(a, b)$ содержит не более 6 элементов, то $T \cap W$ разбивается на 6 непересекающихся подмножеств $U_j, j = 1, \ldots, 6$, таких, что в каждый класс из U_j попадает ровно j элементов из $\widetilde{W}$, т. е.

$$q_{2,i} = \frac{4j}{N}, i \in U_j.$$

Из двух последних равенств получаем:

$$A_{N'} = 2 \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{4}{N} \cdot \frac{4}{N} \cdot \sum_{j=1}^{6} j \cdot |U_j| = \frac{8}{N^2}|U|,$$

где $U = \widetilde{W} \cap T_0$, и по теореме 1 при $N \to \infty$

$$\mathbf{M}(Z_{N'}|(n_1, n_2)) \sim \sqrt{\frac{\pi}{2A_{N'}}} = \frac{N}{4}\sqrt{\frac{\pi}{|U|}}.$$

Следуя работам [28, 43], положим $n_1 = xN_1, n_2 = yN_1, |x|, |y| \leq 1$ и рассмотрим различные случаи расположения множества U в зависимости от значений x и y.

1) $(n_1, n_2) \in B_1 = \{(xN_1, yN_1) : y > \frac{1}{2}, |x| \le \frac{1}{2}, x < 1 - y\}$. Множество значений (x, y) изображено на рисунке 2.3.

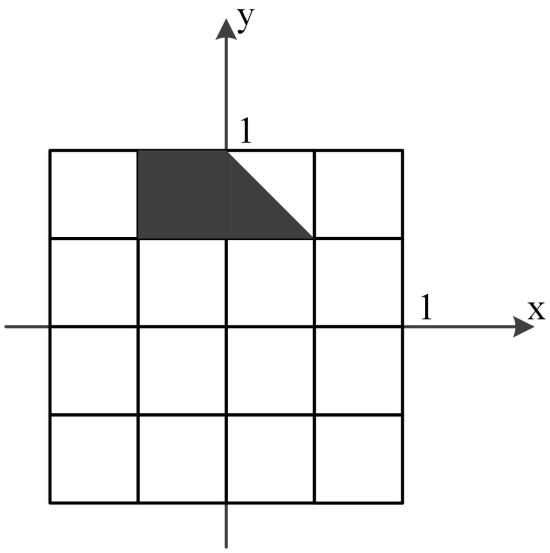

Рис. 2.3.

Вероятность события $(n_1, n_2) \in B_1$ равна $\frac{3}{32}$. Множества $\widetilde{W}$ и T_0 изображены на рисунке 2.4. Имеем:

$$|S_1| = \left(\frac{1}{2} + y - 1\right)\left(\frac{1}{2} + x\right)\frac{N}{4} = \left(y - \frac{1}{2}\right)\left(x + \frac{1}{2}\right)\frac{N}{4},$$

$$|S_2| = \left(y - \frac{1}{2}\right)\left(y - \frac{1}{2}\right) \cdot \frac{1}{2} \cdot \frac{N}{4},$$

$$|U| = |\widetilde{W}| - |S_1| - |S_2| = \frac{N}{4} - \left(y - \frac{1}{2}\right)\left(\frac{y}{2} + x + \frac{1}{4}\right)\frac{N}{4}$$

$$= \frac{N}{8}\left(\frac{9}{4} + x - y^2 - 2xy\right).$$

Тогда условное математическое ожидание величины $Z_{N'}$ при условии $(n_1, n_2) \in B_1$ и $N \to \infty$ имеет вид

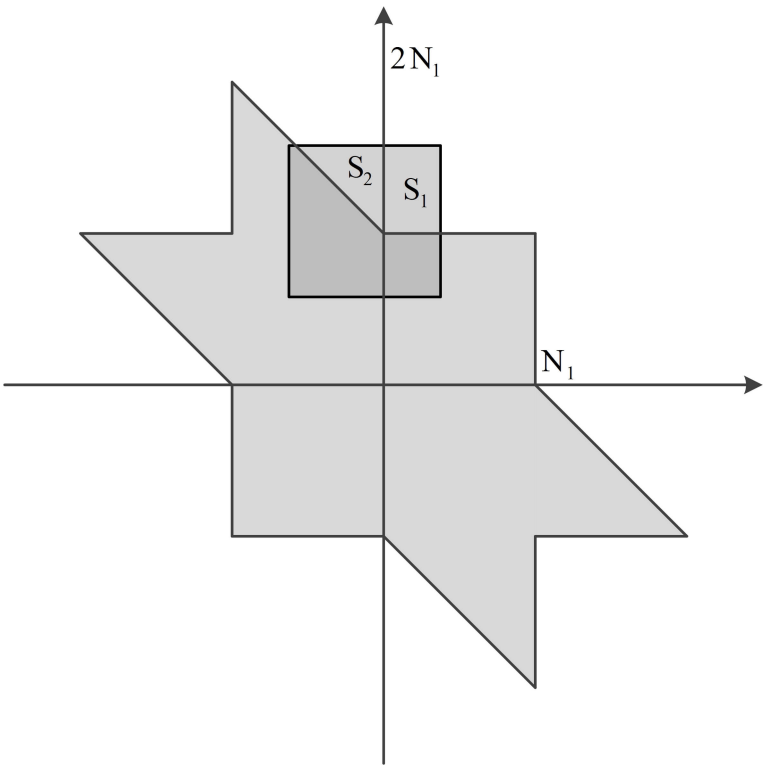

Рис. 2.4.

$$\begin{aligned}
\mathbf{M}(Z_{N'}|(n_1,n_2)\in B_1) &= \frac{1}{|B_1|}\sum_{(n_1,n_2)\in B_1}\mathbf{M}(Z_{N'}|(n_1,n_2)) \\
&\sim \frac{32}{3N}\sum_{(xN_1,yN_1)\in B_1\cap\mathbb{Z}^2}\frac{N}{4}\sqrt{\frac{\pi}{\frac{N}{8}\left(\frac{9}{4}+x-y^2-2xy\right)}} \\
&= \frac{16}{3}\sqrt{\frac{2\pi}{N}}\sum_{(xN_1,yN_1)\in B_1\cap\mathbb{Z}^2}\frac{1}{\sqrt{\left(\frac{9}{4}+x-y^2-2xy\right)}} \\
&\sim \frac{16}{3}\sqrt{\frac{2\pi}{N}}\int_{\frac{N_1}{2}}^{N_1}\int_{-\frac{N_1}{2}}^{(1-\eta)N_1}\frac{d(\xi N_1)d(\eta N_1)}{\sqrt{\left(\frac{9}{4}+\xi-\eta^2-2\xi\eta\right)}} \\
&= \frac{16}{3}\sqrt{\frac{2\pi}{N}}\cdot\frac{N}{4}\int_{\frac{1}{2}}^{1}\int_{-\frac{1}{2}}^{(1-\eta)}\frac{d\xi d\eta}{\sqrt{\left(\frac{9}{4}+\xi-\eta^2-2\xi\eta\right)}} \\
&\approx \frac{8}{3}\cdot 0.282323\cdot\sqrt{\frac{\pi N}{2}}.
\end{aligned}$$

Осталось заметить, что, в силу симметричности отображения φ, есть еще 3 случая с таким же значением условного математического ожи-

дания, т. е. общее количество аналогичных случаев здесь $K_1 = 4$.

2) $(n_1, n_2) \in B_2 = \{(xN_1, yN_1) : y > \frac{1}{2}, |x| \le \frac{1}{2}, x \ge 1 - y\}$. Множество значений (x, y) изображено на рисунке 2.5.

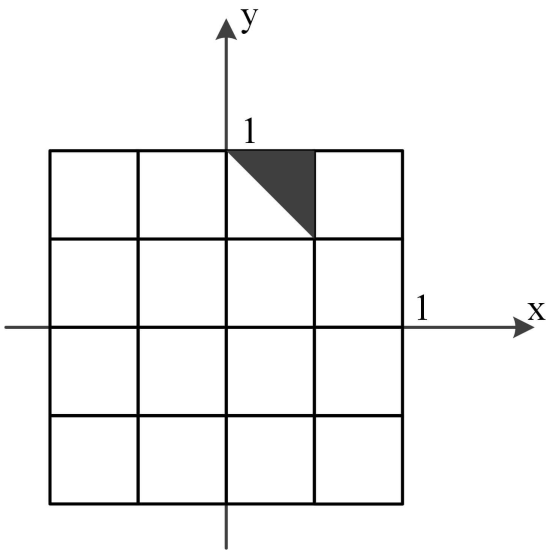

Рис. 2.5.

Вероятность события $(n_1, n_2) \in B_2$ равна $\frac{1}{32}$. Множества $\widetilde{W}$ и T_0 изображены на рисунке 2.6. Имеем:

$$|S_1| = \left(y - \frac{1}{2}\right)\left(x + \frac{1}{2}\right) \cdot \frac{N}{4},$$

$$|S_2| = \frac{\frac{1}{2} + y - 1 + \frac{1}{2} + y - 1 - \frac{1}{2} + x}{2} \cdot \left(\frac{1}{2} - x\right) \cdot \frac{N}{4}$$

$$= \left(\frac{1}{2} - x\right)\left(\frac{x}{2} + y - \frac{3}{4}\right) \cdot \frac{N}{4},$$

$$|U| = |\widetilde{W}| - |S_1| - |S_2|$$

$$= \frac{N}{4} - \left(\left(y - \frac{1}{2}\right)\left(x + \frac{1}{2}\right) + \left(\frac{1}{2} - x\right)\left(\frac{x}{2} + y - \frac{3}{4}\right)\right) \cdot \frac{N}{4} =$$

$$= \frac{N}{8} \cdot \left(x^2 - x - 2y + \frac{13}{4}\right).$$

Тогда условное математическое ожидание величины $Z_{N'}$ при условии

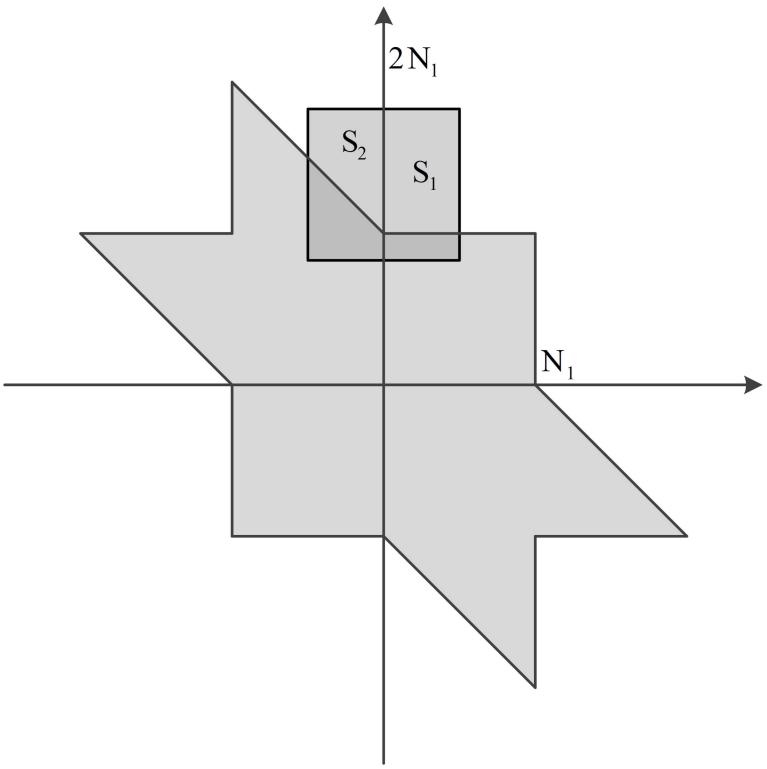

Рис. 2.6.

$(n_1, n_2) \in B_2$ и $N \to \infty$ имеет вид

$$\begin{aligned}
\mathbf{M}(Z_{N'}|(n_1,n_2) \in B_2) &= \frac{1}{|B_2|} \sum_{(n_1,n_2)\in B_2} \mathbf{M}(Z_{N'}|(n_1,n_2)) \\
&\sim \frac{32}{N} \sum_{(xN_1,yN_1)\in B_2\cap\mathbb{Z}^2} \frac{N}{4} \sqrt{\frac{\pi}{\frac{N}{8}\cdot\left(x^2-x-2y+\frac{13}{4}\right)}} \\
&= 16\sqrt{\frac{2\pi}{N}} \sum_{(xN_1,yN_1)\in B_2\cap\mathbb{Z}^2} \frac{1}{\sqrt{\left(x^2-x-2y+\frac{13}{4}\right)}} \\
&\sim 16\sqrt{\frac{2\pi}{N}} \int\limits_{\frac{N_1}{2}}^{N_1} \int\limits_{(1-\eta)N_1}^{\frac{N_1}{2}} \frac{d(\xi N_1)d(\eta N_1)}{\sqrt{\left(\xi^2-\xi-2\eta+\frac{13}{4}\right)}} \\
&= 16\sqrt{\frac{2\pi}{N}} \cdot \frac{N}{4} \int\limits_{\frac{1}{2}}^{1} \int\limits_{(1-\eta)}^{\frac{1}{2}} \frac{d\xi d\eta}{\sqrt{\left(\xi^2-\xi-2\eta+\frac{13}{4}\right)}} \\
&\approx 8 \cdot 0.1075 \cdot \sqrt{\frac{\pi N}{2}}
\end{aligned}$$

Осталось заметить, что, в силу симметричности отображения φ, есть еще 3 случая с таким же значением условного математического ожидания, т. е. общее количество аналогичных случаев здесь $K_2 = 4$.

3) $(n_1, n_2) \in B_3 = \{(xN_1, yN_1) : y > \frac{1}{2}, x < -\frac{1}{2}, x > -y\}$. Множество значений (x, y) изображено на рисунке 2.7.

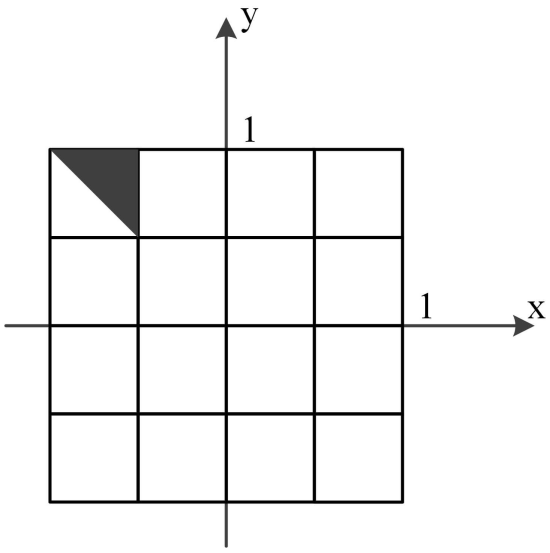

Рис. 2.7.

Вероятность события $(n_1, n_2) \in B_3$ равна $\frac{1}{32}$. Множества $\widetilde{W}$ и T_0 изображены на рисунке 2.8. Имеем:

$$|S_1| = \frac{1}{2} \cdot (x+y)^2 \cdot \frac{N}{4},$$

$$|S_2| = \left(\frac{1}{2} + x\right)\left(\frac{1}{2} - y\right) \cdot \frac{N}{4},$$

$$|U| = |\widetilde{W}| - |S_1| - |S_2|$$

$$= \frac{N}{4} - \left(\frac{1}{2} \cdot (x+y)^2 + \left(\frac{1}{2} + x\right)\left(\frac{1}{2} - y\right)\right) \cdot \frac{N}{4} =$$

$$= \frac{N}{8}\left(\frac{3}{2} - x^2 - y^2 - x + y\right).$$

Тогда условное математическое ожидание величины $Z_{N'}$ при условии

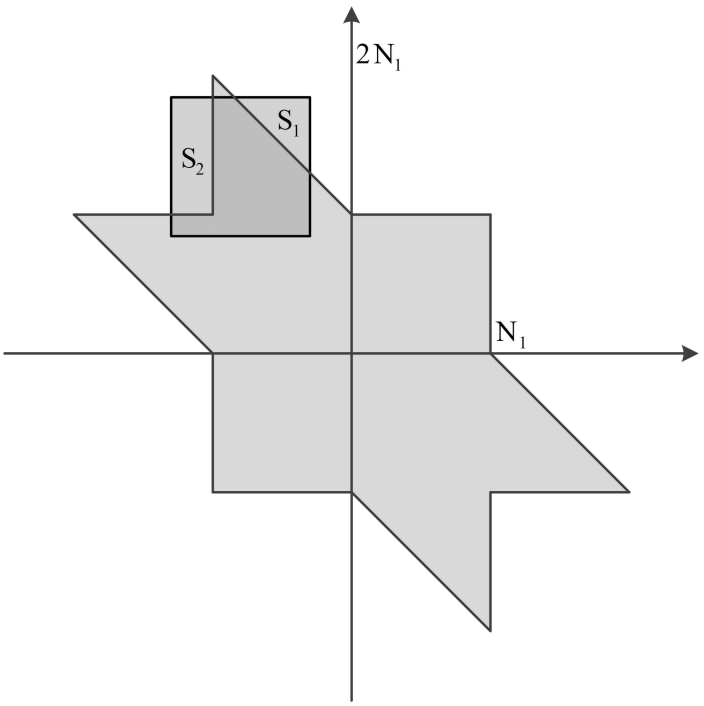

Рис. 2.8.

$(n_1, n_2) \in B_3$ и $N \to \infty$ имеет вид

$$\begin{aligned}
\mathbf{M}(Z_{N'}|(n_1,n_2) \in B_3) &= \frac{1}{|B_3|} \sum_{(n_1,n_2)\in B_3} \mathbf{M}(Z_{N'}|(n_1,n_2)) \\
&\sim \frac{32}{N} \sum_{(xN_1,yN_1)\in B_3\cap\mathbb{Z}^2} \frac{N}{4} \sqrt{\frac{\pi}{\frac{N}{8}\cdot\left(\frac{3}{2}-x^2-y^2-x+y\right)}} \\
&= 16\sqrt{\frac{2\pi}{N}} \sum_{(xN_1,yN_1)\in B_3\cap\mathbb{Z}^2} \frac{1}{\sqrt{\left(\frac{3}{2}-x^2-y^2-x+y\right)}} \\
&\sim 16\sqrt{\frac{2\pi}{N}} \int\limits_{\frac{N_1}{2}}^{N_1} \int\limits_{-\eta N_1}^{-\frac{N_1}{2}} \frac{d(\xi N_1)d(\eta N_1)}{\sqrt{\left(\frac{3}{2}-\xi^2-\eta^2-\xi+\eta\right)}} \\
&= 16\sqrt{\frac{2\pi}{N}} \cdot \frac{N}{4} \int\limits_{\frac{1}{2}}^{1} \int\limits_{-\eta}^{-\frac{1}{2}} \frac{d\xi d\eta}{\sqrt{\left(\frac{3}{2}-\xi^2-\eta^2-\xi+\eta\right)}} \\
&\approx 8 \cdot 0.092436 \cdot \sqrt{\frac{\pi N}{2}}
\end{aligned}$$

Осталось заметить, что, в силу симметричности отображения φ, есть еще 3 случая с таким же значением условного математического ожи-

дания, т. е. общее количество аналогичных случаев здесь $K_3 = 4$.

4) $(n_1, n_2) \in B_4 = \{(xN_1, yN_1) : |y| \le \frac{1}{2}, |x| \le \frac{1}{2}\}$. Множество значений (x, y) изображено на рисунке 2.9.

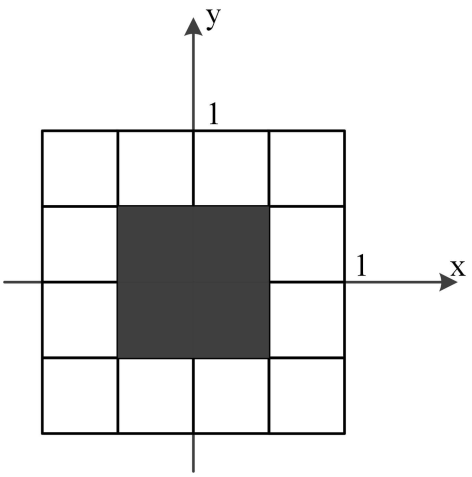

Рис. 2.9.

Вероятность события $(n_1, n_2) \in B_4$ равна $\frac{1}{4}$. Множества $\widetilde{W}$ и T_0 изображены на рисунке 2.10. Имеем:

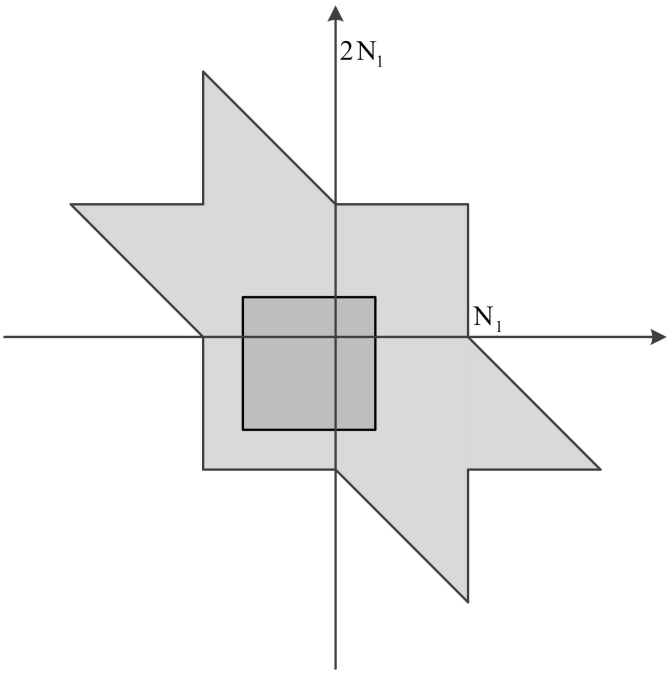

Рис. 2.10.

$$|U| = \frac{N}{4}.$$

Тогда условное математическое ожидание величины $Z_{N'}$ при условии $(n_1, n_2) \in B_4$ и $N \to \infty$ имеет вид

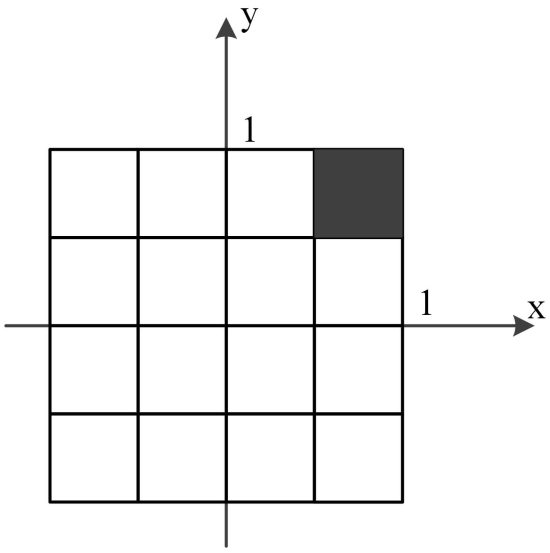

Рис. 2.11.

$$\mathbf{M}(Z_{N'}|(n_1, n_2) \in B_4) = \frac{1}{|B_4|} \sum_{(n_1,n_2)\in B_4} \mathbf{M}(Z_{N'}|(n_1, n_2))$$

$$\sim \frac{4}{N} \sum_{(xN_1,yN_1)\in B_4\cap\mathbb{Z}^2} \frac{N}{4}\sqrt{\frac{\pi}{\frac{N}{4}}} = \frac{N}{4}\sqrt{\frac{\pi}{\frac{N}{4}}} \approx \sqrt{\frac{\pi N}{2}} \cdot 0.7071067$$

Общее количество аналогичных случаев здесь $K_4 = 1$.

5) $(n_1, n_2) \in B_5 = \{(xN_1, yN_1) : y > \frac{1}{2}, x > \frac{1}{2}\}$. Множество значений (x, y) изображено на рисунке 2.11. Вероятность события $(n_1, n_2) \in B_5$ равна $\frac{1}{16}$. Множества $\widetilde{W}$ и T_0 изображены на рисунке 2.12. Имеем:

$$|U| = \frac{N}{4} \cdot \left(\frac{3}{2} - x\right)\left(\frac{3}{2} - y\right).$$

Тогда условное математическое ожидание величины $Z_{N'}$ при условии $(n_1, n_2) \in B_5$ и $N \to \infty$ имеет вид

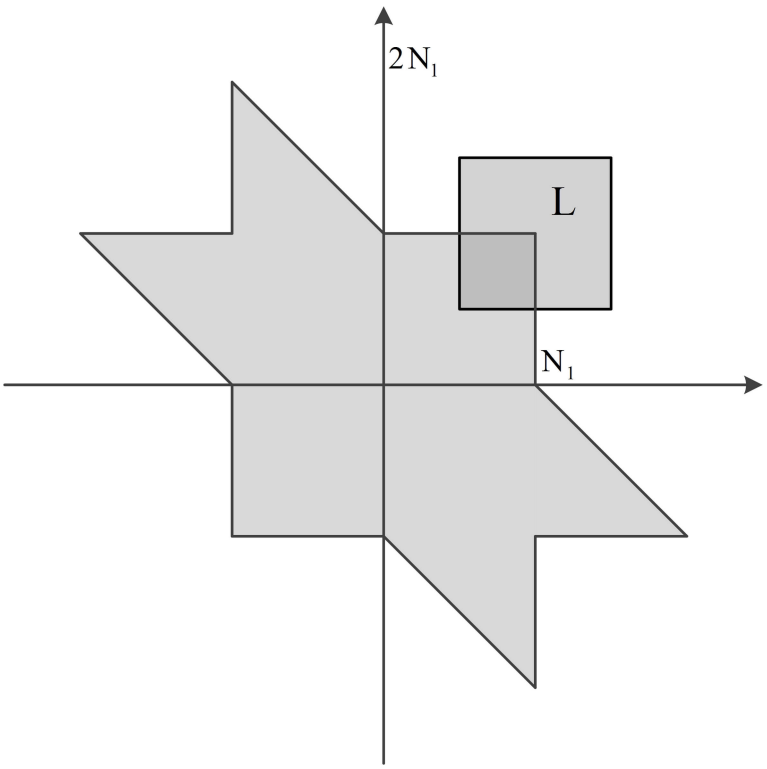

Рис. 2.12.

$$\mathbf{M}(Z_{N'}|(n_1,n_2)\in B_5)=\frac{1}{|B_5|}\sum_{(n_1,n_2)\in B_5}\mathbf{M}(Z_{N'}|(n_1,n_2))$$

$$\sim\frac{16}{N}\sum_{(xN_1,yN_1)\in B_5\cap\mathbb{Z}^2}\frac{N}{4}\sqrt{\frac{\pi}{\frac{N}{4}\cdot\left(\frac{3}{2}-x\right)\left(\frac{3}{2}-y\right)}}$$

$$=8\sqrt{\frac{\pi}{N}}\sum_{(xN_1,yN_1)\in B_5\cap\mathbb{Z}^2}\frac{1}{\sqrt{\left(\frac{3}{2}-x\right)\left(\frac{3}{2}-y\right)}}$$

$$\sim 8\sqrt{\frac{\pi}{N}}\int\limits_{\frac{N_1}{2}}^{N_1}\int\limits_{\frac{N_1}{2}}^{N_1}\frac{d(\xi N_1)d(\eta N_1)}{\sqrt{\left(\frac{3}{2}-\xi\right)\left(\frac{3}{2}-\eta\right)}}$$

$$=8\sqrt{\frac{\pi}{N}}\cdot\frac{N}{4}\int\limits_{\frac{1}{2}}^{1}\int\limits_{\frac{1}{2}}^{1}\frac{d\xi d\eta}{\sqrt{\left(\frac{3}{2}-\xi\right)\left(\frac{3}{2}-\eta\right)}}\approx 4\cdot\sqrt{\frac{\pi N}{2}}\cdot 0.2426406871$$

Осталось заметить, что, в силу симметричности отображения φ, есть еще 1 случай с таким же значением условного математического ожидания, т. е. общее количество аналогичных случаев здесь $K_5=2$.

В итоге получаем

$$\mathbf{M}(Z_{N'}) = \sum_{i=1}^{5} \Pr((n_1, n_2) \in B_i) \cdot M(Z_{N'} | (n_1, n_2) \in B_i) \cdot K_i$$

$$\approx 0.97811 \cdot \sqrt{N}.$$

Теорема доказана. □

2.3 Выводы

К основным выводам главы 2 относятся следующие.

1. Для класса эллиптических кривых, заданных над $GF(p)$ уравнением $y^2 = x^3 + B$ при $p \equiv 1 \pmod 3$, приведено описание орбиты точки (a, b), соответствующей классу эквивалентности точки кривой $aP_1 + bP_2$ под действием эффективного автоморфизма φ порядка 6.

2. Автором впервые предложена модификация алгоритма Годри-Шоста решения двумерной задачи дискретного логарифмирования в случае подгруппы группы точек эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов при $P_2 = \varphi(P_1)$ и $N_1 = N_2$, где φ — эффективный автоморфизм порядка 6, а также получена оценка средней трудоемкости разработанного алгоритма, составляющая $(c + o(1))\sqrt{N}$ групповых операций, где $c \approx 0.9781$, что меньше, чем в случае эллиптической кривой общего вида.

Существенное влияние на эффективность различных модификаций алгоритма Годри-Шоста оказывает выбор начальных параметров, а именно «дикого» и «домашнего» множеств. В следующей главе будет проведен анализ возможности оптимизации (путем выбора подходящих начальных параметров) модификаций алгоритмов Годри-Шоста для решения некоторых обобщений задачи дискретного логарифмирования.

Глава 3

О сложности решения двумерной задачи дискретного логарифмирования и задачи дискретного логарифмирования в интервале

В настоящей главе исследуется возможность оптимизации алгоритма Годри-Шоста для решения некоторых обобщений задачи дискретного логарифмирования. Для двумерной задачи дискретного логарифмирования в конечных циклических группах, обладающих эффективным автоморфизмом порядка 2, 4 или 6, получены модификации алгоритма Годри-Шоста, а также оценки их средней трудоемкости. Для задачи дискретного логарифмирования в интервале получена модификация алгоритма Годри-Шоста для конечных циклических групп с эффективным

инвертированием, а также оценка средней трудоемкости такого алгоритма.

3.1 О сложности решения двумерной задачи дискретного логарифмирования в конечной циклической группе с эффективным автоморфизмом

В настоящем параграфе рассматривается двумерная задача дискретного логарифмирования в конечных циклических группах с эффективным автоморфизмом, а именно:

1) случай подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов;

2) случай подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax$ над конечным простым полем из $p \equiv 1 \bmod 4$ элементов;

3) случай подгруппы группы точек эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов.

Для указанных групп приводятся результаты расчетов константы при главном члене в оценке средней трудоемкости решения двумерной задачи дискретного логарифмирования алгоритмом Годри-Шоста для различных размеров «дикого» множества, а также полученные модификации алгоритма Годри-Шоста.

3.1.1 Оценка средней трудоемкости для некоторых значений параметров алгоритма

Для оптимизации алгоритма Годри-Шоста можно варьировать размеры «домашнего» и «дикого» множеств. В целях определения характера влияния размера и формы этих множеств на константу при главном члене в оценке средней трудоемкости рассматриваются три описанных выше случая: в каждом из них используются «дикие» и «домашние» множества, однако размер «дикого» множества варьируется.

Определим «домашнее» множество T и множество $\widetilde{T}$ представителей классов T классическим образом:

$$T = \{C(a,b) : -N_1 \le a \le N_1, -N_1 \le b \le N_1\},$$

1) для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов
$$\widetilde{T} = \{(a,b) : -N_1 \le a \le N_1, -a \le b \le N_1\};$$

2) для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax$ над конечным простым полем из $p \equiv 1 \bmod 4$ элементов
$$\widetilde{T} = \{0, \ldots, N_1\} \times \{0, \ldots, N_1\};$$

3) для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов
$$\widetilde{T} = \{0, \ldots, N_1\} \times \{1, \ldots, N_1\} \cup \{(0,0)\}.$$

Обозначим через T_0 объединение классов из множества T. Для «дикого» множества W введем параметр k — коэффициент сжатия, а также обозначим

$$W_k = \{C(n_1 + a, n_2 + b) : -\frac{kN_1}{2} \le a \le \frac{kN_1}{2}, -\frac{kN_1}{2} \le b \le \frac{kN_1}{2}\}$$

и

$$\widetilde{W}_k = \{-\frac{kN_1}{2} + n_1, \ldots, \frac{kN_1}{2} + n_1\} \times \{-\frac{kN_1}{2} + n_2, \ldots, \frac{kN_1}{2} + n_2\}.$$

Как и в алгоритме Годри-Шоста, будем параллельно вычислять последовательности точек

$$x_i P_1 + y_i P_2, (x_i, y_i) \in \widetilde{T}, i = 1, 2, \ldots, \tag{3.1}$$

$$Q + z_j P_1 + w_j P_2, (z_j, w_j) \in \widetilde{W}_k, j = 1, 2, \ldots \tag{3.2}$$

до тех пор, пока в них не найдутся две точки из одного класса эквивалентности, после чего находим решение задачи как показано в § 1.2 (при этом предполагается, что значения (x_i, y_i) и (z_j, w_j) выбираются случайно равновероятно и независимо из соответствующих множеств).

Для определения средней трудоемкости воспользуемся теоремой 1, как это делается в главе 2. Тогда в обозначениях теоремы $C = 2$: шары цвета 1 — это элементы множества $\widetilde{T}$, а шары цвета 2 — элементы множества $\widetilde{W}_k$. Вычисление последовательностей (3.1) и (3.2) происходит параллельно, поэтому мы можем считать, что $r_{j,1} = r_{j,2} = \frac{1}{2}$ для всех $j = 1, 2, \ldots$, откуда $p_1 = p_2 = \frac{1}{2}$. Множество урн в нашем случае — это $T \cup W_k$, и шар (a, b) попадает в урну $C(a, b)$. Ясно, что $N' = O(N)$.

Очевидно, что интересующая нас средняя трудоемкость, выраженная в количестве групповых операций, не превосходит математического ожидания суммарного числа $Z_{N'}$ значений (x_i, y_i) и $(n_1 + z_j, n_2 + w_j)$, выбираемых до появления значений (x_k, y_k) и $(n_1 + z_l, n_2 + w_l)$ таких, что $C(x_k, y_k) = C(n_1 + z_l, n_2 + w_l)$. Согласно теореме 1,

$$\begin{gathered} \mathbf{M}(Z_{N'}|(n_1,n_2)) = \sqrt{\frac{\pi}{2A_{N'}}} + O(N^{\frac{1}{4}}), \\ A_{N'} = \frac{|U|}{2 \cdot |\widetilde{T}| \cdot |\widetilde{W}_k|}, \end{gathered} \tag{3.3}$$

где $U = \widetilde{W}_k \cap T_0$. Тогда для фиксированных $(n_1, n_2) \in \{-N_1, \ldots, N_1\} \times \{-N_1, \ldots, N_1\}$ может быть вычислена мощность множества U и получена оценка средней трудоемкости алгоритма.

На множестве $\{-N_1, \ldots, N_1\} \times \{-N_1, \ldots, N_1\}$ введем двумерную равномерную сетку:

$$\Omega_m = \{(n_1^i, n_2^j) = (-N_1 + ih, -N_1 + jh), i, j = 0, \ldots, m; h = \frac{N_1}{m}\}.$$

Выбор параметра сетки позволяет получать достаточно точные приближения среднего значения площади пересечения двух многоугольников. Для проведения расчетов был реализован скрипт на языке python (листинг приведен в приложении А). Таким образом для различных значений параметра k с использованием математического пакета shapely [32] по формулам (3.3) была вычислена оценка средней трудоемкости алгоритма в каждом узле сетки Ω_m, а также усредненное значение по всем узлам.

Результаты проведенного расчета с $m = 200$ согласуются со всеми известными ранее оценками средней трудоемкости алгоритма. Таблица 3.1 показывает результаты для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов. Таблица 3.2 показывает результаты для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax$ над конечным простым полем из $p \equiv 1 \bmod 4$ элементов. Таблица 3.3 показывает результаты для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов.

Из расчетов видно, что наименьшее значение коэффициента в асимптотической оценке средней трудоемкости алгоритма во всех трех случаях достигается при наименьшей площади пересечения $U = \widetilde{W_k} \cap T_0$. Строгое доказательство этого факта, а также определение связи между оценкой средней трудоемкости и размером «дикого» множества приводится в дальнейшей части работы.

3.1.2 Алгоритм и оценка средней трудоемкости

Первоначальный выбор «дикого» и «домашнего» множеств оказывает влияние не оценку средней трудоемкости различных вариантов алго-

Таблица 3.1: оценка средней трудоемкости для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов

Коэффициент сжатия «дикого» множества, k	Константа при главном члене в оценке средней трудоемкости
0.1	1.27510178675
0.2	1.29678705843
0.3	1.31871993702
0.4	1.34085315566
0.5	1.36317720124
0.6	1.38568889736
0.7	1.40838688171
0.8	1.43127047289
0.9	1.45433929223
1.0	1.47759311251 [1]
1.1	1.50103178912
1.2	1.52465522563

[1] результат получен в работе Лиу [43]

ритма Годри-Шоста. Так, в работе Лиу [43] рассматриваются оптимизации алгоритма Годри-Шоста решения двумерной задачи дискретного логарифмирования, предполагающие варьирование размера «домашнего» множества. В настоящей работе автором рассматриваются модификации алгоритма Годри-Шоста с измененным размером «дикого» множества. Расчеты (таблицы 3.1, 3.2, 3.3) демонстрируют возможность получения таким способом наиболее эффективных оптимизаций алгоритма Годри-Шоста для двумерной задачи дискретного программирования. Для каждого из трех рассмотренных классов эллиптических кривых, обладающих эффективными автоморфизмами порядка $2, 4$ и 6, автором сформулированы и доказаны теоремы, определяющие явным образом связь между оценкой средней трудоемкости соответствующих алгоритмов и размером «дикого» множества.

Следующая теорема конструктивно доказывает возможность снижения трудоемкости решения двумерной задачи дискретного логарифмирования для случая подгруппы группы точек эллиптической кривой

Таблица 3.2: оценка средней трудоемкости для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax$ над конечным простым полем из $p \equiv 1 \bmod 4$ элементов

Коэффициент сжатия «дикого» множества, k	Константа при главном члене в оценке средней трудоемкости
0.1	0.901633120116
0.2	0.916966922771
0.3	0.932475809951
0.4	0.948126358941
0.5	0.963911842953
0.6	0.979830015935
0.7	0.995879914594
0.8	1.01206105709
0.9	1.02837317568
1.0	1.04481610969 [1]
1.1	1.06138975686
1.2	1.07809404902

[1] результат получен в работе Лиу [43]

$y^2 = x^3 + B$ над конечным простым полем из $p > 3$ элементов, а также определяет оценку средней трудоемкости соответствующего алгоритма.

Теорема 3. *[49] Пусть G — подгруппа простого порядка q группы точек эллиптической кривой E, заданной над конечным простым полем $GF(p)$ уравнением $y^2 = x^3 + B$ при $p \equiv 1 \pmod 3$, $q^2 \nmid \#E$; φ — автоморфизм группы G, $\varphi(x, y) = (\beta x, -y)$, где $\beta \neq 1$ — кубический корень из 1 по модулю p; λ — корень уравнения $\lambda^2 - \lambda + 1 \equiv 0 \pmod q$ такой, что $\varphi(x, y) = \lambda(x, y)$. Тогда для любого $\varepsilon > 0$ существует такой алгоритм решения двумерной задачи дискретного логарифмирования (см. определение 3) в группе G, что при $N_1 = N_2$, $P_2 = \varphi(P_1)$ и случайном равновероятном выборе (n_1, n_2), его средняя трудоемкость не превосходит $(1 + \varepsilon)\sqrt{\frac{\pi N}{4}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций[(1)], где $N = 4N_1N_2, N \to \infty$.*

Доказательство. Определим «домашнее» множество T и множество $\widetilde{T}$

[(1)]запись O_ε означает, что константа, скрывающаяся под символом O, зависит от ε

Таблица 3.3: оценка средней трудоемкости для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов

Коэффициент сжатия «дикого» множества, k	Константа при главном члене в оценке средней трудоемкости
0.1	0.894066878098
0.2	0.90210923268
0.3	0.910489432021
0.4	0.919190764618
0.5	0.928209867054
0.6	0.937545616299
0.7	0.947197533218
0.8	0.957167061124
0.9	0.967468355894
1.0	0.978132200326 [1]
1.1	0.989193563032
1.2	1.00065213859

[1] результат получен в главе 2

представителей классов из T

$$T = \{C(a, b) : -N_1 \leq a \leq N_1, -N_1 \leq b \leq N_1\},$$

где $C(a, b)$ — множество (класс) пар, соответствующее классу эквивалентности точки вида $aP_1 + bP_2$ эллиптической кривой E, определенный в § 2.1,

$$\widetilde{T} = \{0, \ldots, N_1\} \times \{1, \ldots, N_1\} \cup \{(0, 0)\}$$

(в работах [28, 43] такое множество называется фундаментальной областью «домашнего» множества). Обозначим T_0 объединение классов из множества T. Введем параметр $k \in (0, 2)$ — коэффициент сжатия «дикого» множества W, такой, что $\frac{kN_1}{2} \in \mathbb{Z}$. Обозначим

$$W_k = \{C(n_1 + a, n_2 + b) : -\frac{kN_1}{2} \leq a \leq \frac{kN_1}{2}, -\frac{kN_1}{2} \leq b \leq \frac{kN_1}{2}\}$$

и

$$\widetilde{W}_k = \{-\frac{kN_1}{2} + n_1, \ldots, \frac{kN_1}{2} + n_1\} \times \{-\frac{kN_1}{2} + n_2, \ldots, \frac{kN_1}{2} + n_2\}.$$

Тогда

$$|\widetilde{W}_k| = (kN_1 + 1)^2$$

Аналогично тому, как это делается в § 3.1.1, будем параллельно вычислять последовательности точек (3.1) и (3.2) до тех пор, пока в них не найдутся две точки из одного класса эквивалентности. Также определим $Z_{N'}$ — суммарное число значений (x_i, y_i) и $(n_1 + z_j, n_2 + w_j)$, выбираемых до появления значений (x_k, y_k) и $(n_1 + z_l, n_2 + w_l)$ таких, что $C(x_k, y_k) = C(n_1 + z_l, n_2 + w_l)$.

Найдем условное математическое ожидание $\mathbf{M}(Z_{N'}|(n_1, n_2))$ случайной величины $Z_{N'}$ при фиксированных n_1, n_2. Согласно теореме 1, имеем:

$$q_{1,i} = \begin{cases} \frac{1}{N_1^2+N_1+1}, & \text{если } i \in T \\ 0, & \text{в противном случае} \end{cases}.$$

С учетом последнего равенства и утверждения теоремы 1 нас интересуют значения $q_{2,i}$ только для $i \in T \cap W_k$. Поскольку каждый класс $C(a, b)$ содержит не более 6 элементов, то $T \cap W_k$ разбивается на 6 непересекающихся подмножеств $U_j, j = 1, \ldots, 6$ таких, что в каждый класс из U_j попадает ровно j элементов из $\widetilde{W}_k$, т. е.

$$q_{2,i} = \frac{j}{(kN_1 + 1)^2}, i \in U_j.$$

Из двух последних равенств получаем:

$$A_{N'} = 2 \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{N_1^2 + N_1 + 1} \cdot \frac{1}{(kN_1 + 1)^2} \cdot \sum_{j=1}^{6} j \cdot |U_j| = \frac{1}{2 \cdot |\widetilde{T}| \cdot |\widetilde{W}_k|}|U|,$$

где $U = \widetilde{W}_k \cap T_0$, и по теореме 1

$$\mathbf{M}(Z_{N'}|(n_1, n_2)) = \sqrt{\frac{\pi}{2A_{N'}}} + O(N^{\frac{1}{4}}).$$

Следуя работам [28, 43], положим $n_1 = xN_1, n_2 = yN_1, |x|, |y| \leq 1$. Оценим мощность множества U в зависимости от значений x и y.

1) $(n_1, n_2) \in B_1 = \{(xN_1, yN_1) : |x| \le 1 - \frac{k}{2}, |y| \le 1 - \frac{k}{2}\}$ (см. рис. 3.1) Вероятность события $(n_1, n_2) \in B_1$ равна $\left(\frac{(2-k)N_1+1}{2N_1+1}\right)^2$. В этом случае множество $\widetilde{W}_k$ полностью содержится в T_0, т. е.

$$|U| = |\widetilde{W}_k|$$

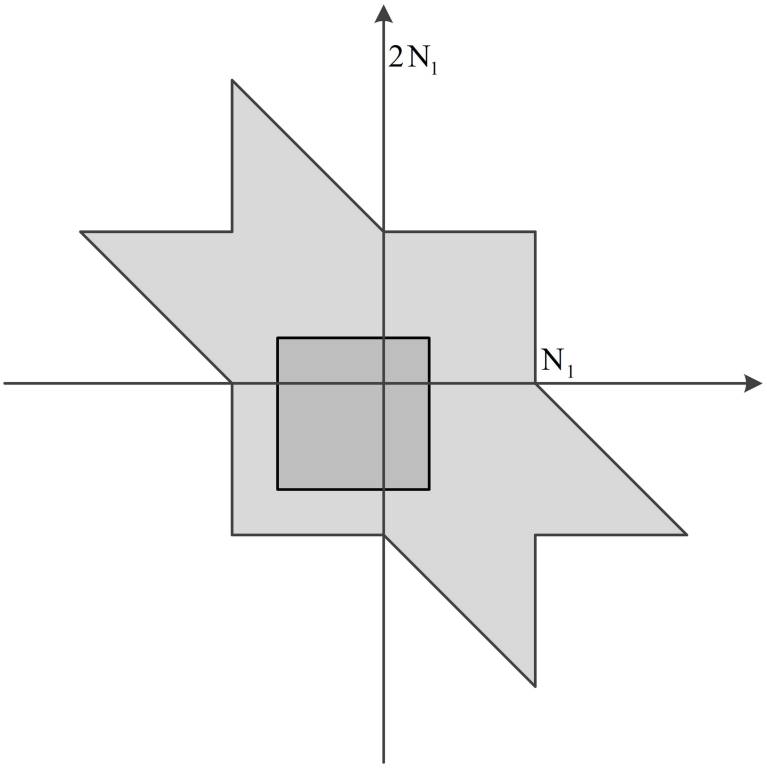

Рис. 3.1.

2) $(n_1, n_2) \in B_2 = \{(xN_1, yN_1) : |x| > 1 - \frac{k}{2}\} \cup \{(xN_1, yN_1) : |y| > 1 - \frac{k}{2}\}$ (см. рис. 3.2) Вероятность события $(n_1, n_2) \in B_2$ равна $1 - \left(\frac{(2-k)N_1+1}{2N_1+1}\right)^2$. В этом случае можно сделать оценку

$$|U| \ge \frac{|\widetilde{W}_k|}{4}$$

Теперь можем оценить математическое ожидание

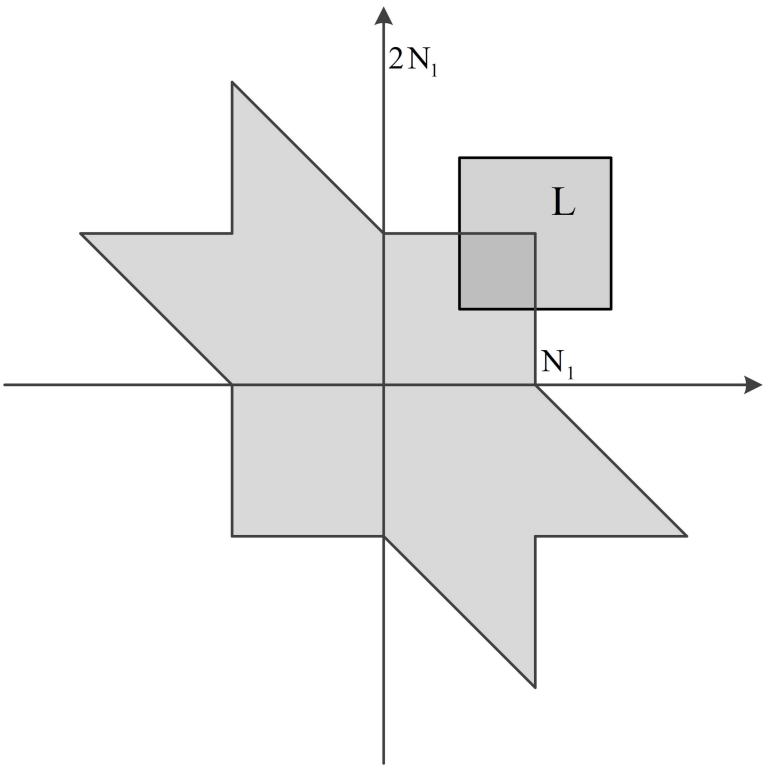

Рис. 3.2.

$$\mathbf{M}(Z_{N'}) = \left(\frac{(2-k)N_1+1}{2N_1+1}\right)^2 \mathbf{M}(Z_{N'}|(n_1,n_2)\in B_1)$$
$$+ (1-\left(\frac{(2-k)N_1+1}{2N_1+1}\right)^2)\mathbf{M}(Z_{N'}|(n_1,n_2)\in B_2)$$
$$\leq \left(\frac{(2-k)N_1+1}{2N_1+1}\right)^2 \sqrt{\pi\cdot|\widetilde{T}|}+(1-\left(\frac{(2-k)N_1+1}{2N_1+1}\right)^2)\sqrt{4\pi\cdot|\widetilde{T}|}+O_k(N^{\frac{1}{4}})$$
$$\leq (2-\left(\frac{(2-k)N_1+1}{2N_1+1}\right)^2)\sqrt{\pi\cdot|\widetilde{T}|}+O_k(N^{\frac{1}{4}})$$
$$\leq \left(\frac{(4+4k-k^2)N_1^2+(4+2k)N_1+1}{4N_1^2+4N_1+1}\right)\sqrt{\pi}\cdot(N_1+1)+O_k(N^{\frac{1}{4}}) \quad (3.4)$$

Т.е. при $N=4N_1^2, N\to\infty$

$$\mathbf{M}(Z_{N'}) \leq (1+k-\frac{k^2}{4})\sqrt{\frac{\pi N}{4}}+O_k(N^{\frac{1}{4}}). \quad (3.5)$$

Тогда при $k\to 0$, получаем утверждение теоремы.

Теорема доказана. □

Оценка (3.5) позволяет определить значения коэффициента сжатия «дикого» множества k, при которых, в условиях теоремы 3, средняя трудоемкость модификации алгоритма Годри-Шоста решения двумерной задачи дискретного логарифмирования не превосходит $(1+\varepsilon)\sqrt{\frac{\pi N}{4}}+O_\varepsilon(N^{\frac{1}{4}})$ групповых операций. Для любого $0<\varepsilon<1$ необходимо выбрать значение k:

$$k-\frac{k^2}{4}<\varepsilon,\ k>0,$$

$$0<k<2(1-\sqrt{1-\varepsilon}). \tag{3.6}$$

Следующая теорема конструктивно доказывает возможность снижения трудоемкости решения двумерной задачи дискретного логарифмирования для случая подгруппы группы точек эллиптической кривой $y^2=x^3+Ax$ над конечным простым полем из $p\equiv 1 \bmod 4$ элементов, а также определяет оценку средней трудоемкости соответствующего алгоритма.

Теорема 4. *[49] Пусть G — подгруппа простого порядка q группы точек эллиптической кривой E, заданной над конечным простым полем $GF(p)$ уравнением $y^2=x^3+Ax$ при $p\equiv 1\pmod 4$, $q^2\nmid \#E$; φ — автоморфизм группы G, $\varphi(x,y)=(-x,\alpha y)$, где α — элемент порядка 4 по модулю p; λ — корень уравнения $\lambda^2\equiv -1 \pmod q$ такой, что $\varphi(x,y)=\lambda(x,y)$. Тогда для любого $\varepsilon>0$ существует такой алгоритм решения двумерной задачи дискретного логарифмирования в группе G, что при $N_1=N_2$, $P_2=\varphi(P_1)$ и случайном равновероятном выборе (n_1,n_2), его средняя трудоемкость не превосходит $(1+\varepsilon)\sqrt{\frac{\pi N}{4}}+O_\varepsilon(N^{\frac{1}{4}})$ групповых операций, где $N=4N_1N_2$, $N\to\infty$.*

Доказательство. Определим «домашнее» множество T и множество $\widetilde{T}$ представителей классов T

$$T=\{C(a,b):-N_1\le a\le N_1,-N_1\le b\le N_1\},$$

где $C(a,b)$ — множество (класс) пар, соответствующее классу эквивалентности точки вида aP_1+bP_2 эллиптической кривой E, определенный

в § 1.2,

$$\widetilde{T} = \{0, \ldots, N_1\} \times \{0, \ldots, N_1\}$$

Введем параметр $k \in (0, 2)$ — коэффициент сжатия «дикого» множества W, такой, что $\frac{kN_1}{2} \in \mathbb{Z}$.

$$W_k = \{C(n_1 + a, n_2 + b) : -\frac{kN_1}{2} \leq a \leq \frac{kN_1}{2}, -\frac{kN_1}{2} \leq b \leq \frac{kN_1}{2}\}$$

тогда

$$\widetilde{W_k} = \{-\frac{kN_1}{2} + n_1, \ldots, \frac{kN_1}{2} + n_1\} \times \{-\frac{kN_1}{2} + n_2, \ldots, \frac{kN_1}{2} + n_2\}$$

и

$$|\widetilde{W_k}| = (kN_1 + 1)^2$$

Аналогично доказательству теоремы 3,

$$A_{N'} = 2 \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{N_1^2 + N_1 + 1} \cdot \frac{1}{(kN_1 + 1)^2} \cdot \sum_{j=1}^{6} j \cdot |U_j| = \frac{1}{2 \cdot |\widetilde{T}| \cdot |\widetilde{W_k}|}|U|,$$

В таком случае остается справедливой оценка (3.5). □

Следующая теорема конструктивно доказывает возможность снижения трудоемкости решения двумерной задачи дискретного логарифмирования для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов, а также определяет оценку средней трудоемкости соответствующего алгоритма.

Теорема 5. *[49] Пусть G — подгруппа простого порядка q группы точек эллиптической кривой E, заданной над конечным простым полем $GF(p)$ уравнением $y^2 = x^3 + Ax + B$; φ — автоморфизм группы G, $\varphi(x, y) = (x, -y)$, Тогда для любого $\varepsilon > 0$ существует такой алгоритм решения двумерной задачи дискретного логарифмирования в группе G, что при $N_1 = N_2$ и случайном равновероятном выборе (n_1, n_2), его средняя трудоемкость не превосходит $(1+\varepsilon)\sqrt{\frac{\pi N}{2}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций, где $N = 4N_1N_2, N \to \infty$.*

Доказательство. Определим «домашнее» множество T и множество $\widetilde{T}$ представителей классов T

$$T = \{C(a,b) : -N_1 \le a \le N_1, -N_1 \le b \le N_1\},$$

где $C(a,b)$ — множество (класс) пар, соответствующее классу эквивалентности точки вида $aP_1 + bP_2$ эллиптической кривой E, определенный в § 1.2,

$$\widetilde{T} = \{(a,b) : -N_1 \le a \le N_1, -a \le b \le N_1\}.$$

Введем параметр $k \in (0,2)$ — коэффициент сжатия «дикого» множества W, такой, что $\frac{kN_1}{2} \in \mathbb{Z}$.

$$W_k = \{C(n_1 + a, n_2 + b) : -\frac{kN_1}{2} \le a \le \frac{kN_1}{2}, -\frac{kN_1}{2} \le b \le \frac{kN_1}{2}\}$$

тогда

$$\widetilde{W_k} = \{-\frac{kN_1}{2} + n_1, \ldots, \frac{kN_1}{2} + n_1\} \times \{-\frac{kN_1}{2} + n_2, \ldots, \frac{kN_1}{2} + n_2\}$$

и

$$|\widetilde{W_k}| = (kN_1 + 1)^2$$

Аналогично доказательству теоремы 3,

$$A_{N'} = 2 \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{2}{(2N_1+1)(2N_1+2)} \cdot \frac{1}{(kN_1+1)^2} \cdot \sum_{j=1}^{2} j \cdot |U_j| = \frac{4}{k^2N^2}|U|.$$

Легко убедиться, что в этом случае оценка (3.5) принимает вид

$$\mathbf{M}(Z_{N'}) \le (1 + k - \frac{k^2}{4})\sqrt{\frac{\pi N}{2}}$$

□

Теоремы 3, 4, 5 позволяют привести в явном виде модификацию алгоритма Годри-Шоста для решения двумерной задачи дискретного логарифмирования в каждом из описанных случаев.

Алгоритм 1.

Вход. Группа G*:*

$$G = \begin{cases} \mathcal{E}_1, \text{ подгруппа группы точек эллиптической кривой} \\ y^2 = x^3 + Ax + B \text{ над конечным простым полем из } p > 3 \text{ элементов}, \\ \mathcal{E}_2, \text{ подгруппа группы точек эллиптической кривой} \\ y^2 = x^3 + Ax \text{ над конечным простым полем из } p \equiv 1 \bmod 4 \text{ элементов}, \\ \mathcal{E}_3, \text{ подгруппа группы точек эллиптической кривой} \\ y^2 = x^3 + B \text{ над конечным простым полем из } p \equiv 1 \bmod 3 \text{ элементов}. \end{cases}$$

$P_1, P_2, Q \in G$*,* $N_1 \in \mathbb{N}$*,* $Q = n_1 P_1 + n_2 P_2$ *для некоторых (неизвестных)* $n_1 \in \{-N_1, \ldots, N_1\}$*,* $n_2 \in \{-N_1, \ldots, N_1\}$*,* k *— коэффициент сжатия «дикого» множества.*

Выход: $n_1', n_2' \in \mathbb{Z}$ *такие, что* $Q = n_1' P_1 + n_2' P_2$*.*

1. *Инициализировать множества*

$$\widetilde{T} = \begin{cases} \{(a, b) : -N_1 \le a \le N_1, -a \le b \le N_1\}, \text{ в случае } G = \mathcal{E}_1, \\ \{0, \ldots, N_1\} \times \{0, \ldots, N_1\}, \text{ в случае } G = \mathcal{E}_2, \\ \{0, \ldots, N_1\} \times \{1, \ldots, N_1\} \cup \{(0, 0)\}, \text{ в случае } G = \mathcal{E}_3, \end{cases}$$

$$W_0 = \{(a, b) : -\frac{kN_1}{2} \le a \le \frac{kN_1}{2}, -\frac{kN_1}{2} \le b \le \frac{kN_1}{2}\},$$

а также множества

$$S_{\widetilde{T}} = \varnothing, \ S_{\widetilde{W}} = \varnothing.$$

2. *Инициализировать счетчик шагов*

$$i = 1.$$

3. *Выполнить вычисление и сохранение очередного элемента «домашнего» множества.*

(a) *выбрать элемент* $(x_i, y_i) \in_R \widetilde{T}$;

(b) *вычислить* $P_{\widetilde{T}} = x_i P_1 + y_i P_2$;

(c) *вычислить представитель* $P'_{\widetilde{T}}$ *класса эквивалентности точки* $P_{\widetilde{T}}$, *порожденного действием эффективного автоморфизма группы* G.

(d) *добавить* $P'_{\widetilde{T}}$ *в множество* $S_{\widetilde{T}}$: $S_{\widetilde{T}} = S_{\widetilde{T}} \cup \{P'_{\widetilde{T}}\}$.

4. *Если* $S_{\widetilde{T}} \cap S_{\widetilde{W}} \neq \varnothing$, *перейти на шаг 8.*

5. *Выполнить вычисление и сохранение очередного элемента «дикого» множества.*

(a) *выбрать элемент* $(z_i, w_i) \in_R W_0$;

(b) *вычислить* $P_{\widetilde{W}} = Q + z_i P_1 + w_i P_2$;

(c) *вычислить представитель* $P'_{\widetilde{W}}$ *класса эквивалентности точки* $P_{\widetilde{W}}$, *порожденного действием эффективного автоморфизма группы* G.

(d) *добавить* $P'_{\widetilde{W}}$ *в множество* $S_{\widetilde{W}}$: $S_{\widetilde{W}} = S_{\widetilde{W}} \cup \{P'_{\widetilde{W}}\}$.

6. *Если* $S_{\widetilde{T}} \cap S_{\widetilde{W}} \neq \varnothing$, *перейти на шаг 8.*

7. *Увеличить значение счетчика* i, *перейти на шаг 3.*

8. *Используя* $S_{\widetilde{W}} \cap S_{\widetilde{T}}$, *вычислить* n'_1, n'_2.

3.1.3 Двумерная и классическая задачи дискретного логарифмирования

Как показано в § 1.1, в случае использования методов рекомпозиции и декомпозиции для повышения эффективности реализаций операции вычисления кратной точки эллиптической кривой, возможно сведение классической задачи дискретного логарифмирования к двумерной.

Пусть G — подгруппа большого простого порядка группы точек эллиптической кривой E, обладающей эффективным автоморфизмом, действующим в группе G как умножение на $\lambda \in \{1, \ldots, |G|-1\}$, и заданной одним из следующих уравнений:

- $y^2 = x^3 + Ax$ над конечным простым полем из $p \equiv 1 \bmod 4$ элементов,
- $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов.

Тогда, согласно работе [29], существует полиномиальный алгоритм, который для любой точки kP, $k \in \{1, \ldots, |G| - 1\}$ позволяет выполнить разложение

$$kP = (k_1 + k_2\lambda)P,$$

причем $k_1, k_2 \leq C_{GLV}\sqrt{|G|}$, а C_{GLV} — константа, не зависящая от $|G|$. В таком случае задачу дискретного логарифмирования на E можно свести к двумерной с неизвестными параметрами k_1, k_2.

Определение 6. *Пусть алгоритмы $\mathfrak{A}_1, \mathfrak{A}_2$ решения классической задачи дискретного логарифмирования в группе G при $|G| \to \infty$ имеют средние трудоемкости $(c_1 + o(1))\sqrt{|G|}$ и $(c_2 + o(1))\sqrt{|G|}$ групповых операций, соответственно. Тогда алгоритм $\mathfrak{A}_1$ называется более эффективным по сравнению с алгоритмом $\mathfrak{A}_2$, если $\frac{c_1}{c_2} < 1$.*

Следующее утверждение описывает, в каких случаях сведение классической задачи к двумерной имеет смысл с точки зрения наличия наиболее эффективного алгоритма (по количеству групповых операций).

Утверждение 1. *Пусть G — циклическая группа, обладающая эффективным автоморфизмом φ. В G задана классическая задача дискретного логарифмирования (см Определение 1). Пусть также для Q справедливо GLV-разложение*

$$Q = (k_1 + k_2\varphi)P, |k_1|, |k_2| \leq C_{GLV}\sqrt{|G|}.$$

Тогда модифицированный алгоритм Годри-Шоста эффективнее параллельного метода Полларда, если

1) G *— подгруппа группы точек эллиптической кривой* $y^2 = x^3 + Ax$ *над конечным простым полем из* $p \equiv 1 \bmod 4$ *элементов и* $C_{GLV} < \frac{1}{2\sqrt{2}(1+\varepsilon)}$*;*

2) G *— подгруппа группы точек эллиптической кривой* $y^2 = x^3 + B$ *над конечным простым полем из* $p \equiv 1 \bmod 3$ *элементов и* $C_{GLV} < \frac{1}{2\sqrt{3}(1+\varepsilon)}$.

Доказательство. Оценка средней трудоемкости алгоритма Полларда составляет $\sqrt{\frac{\pi|G|}{2|\langle\varphi\rangle|}}$ групповых операций ([19], [64]). В терминах алгоритма Годри-Шоста $N_1 = N_2 = C_{GLV}\sqrt{|G|}$, тогда

$$N = 4N_1N_2 \leq 4C_{GLV}^2|G|.$$

Рассмотрим случай кривой $y^2 = x^3 + B$, при $p \equiv 1 \pmod 3$, обладающей эффективным автоморфизмом порядка 6, и сравним оценки средней трудоемкости решения задачи дискретного логарифмирования алгоритмом Годри-Шоста и алгоритмом Полларда. Имеем

$$(1+\varepsilon)\sqrt{\frac{\pi N}{4}} = (1+\varepsilon)\sqrt{\frac{\pi}{4}} \cdot 2C_{GLV}\sqrt{|G|} < \sqrt{\frac{\pi}{12}}\sqrt{|G|}$$

Таким образом, при

$$C_{GLV} < \frac{1}{2\sqrt{3}(1+\varepsilon)}$$

главный член в теоретической оценке среднего количества групповых операций алгоритма Годри-Шоста оказывается меньше.

Аналогично рассматривается случай кривой $y^2 = x^3 + Ax$.

□

Для случая эллиптической кривой, заданной уравнением $y^2 = x^3 + B$ над полем $GF(p),\ p > 3$, используя утверждение 1 и оценку (3.6), можно рассчитать для заданного значения константы C_{GLV} значение коэффициента «сжатия» дикого множества, при котором сведение классической

Таблица 3.4: расчет коэффициента «сжатия» дикого множества для заданной константы C_{GLV}

Значение C_{GLV}	Значение ε	Коэффициент сжатия «дикого» множества, k
менее 0.2	0.75	1
0.225	0.571348403	0.690570204
0.25	0.414213562	0.469266271
0.275	0.285648693	0.309613882
0.3	0.178511302	0.187279726
0.325	0.087856586	0.089876011
0.35	0.010152545	0.010178445

задачи к двумерной и использование модификации алгоритма Годри-Шоста (Алгоритм 1) является оправданным с точки зрения минимизации трудоемкости поиска решения. Пример такого расчета приведен в таблице 3.4.

В следующем параграфе будет рассмотрена возможность получения оптимизированной версии алгоритма Годри-Шоста для задачи дискретного логарифмирования в интервале в случае группы с эффективным инвертированием.

3.2 О сложности решения задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием

В настоящем параграфе доказывается возможность снижения трудоемкости решения задачи дискретного логарифмирования в интервале для группы с эффективным инвертированием, а также приводится оценка трудоемкости соответствующего алгоритма.

Оценка средней трудоемкости вариантов алгоритма Годри-Шоста решения задачи дискретного логарифмирования в интервале зависит от

первоначального выбора «домашнего» и «дикого» множеств. В работе [28] для модификации алгоритма Годри-Шоста используется «дикое» множество уменьшенного размера, однако отсутствует анализ возможности дальнейшей оптимизации такого алгоритма. В настоящей работе автором сформулирована и доказана теорема, которая конструктивно показывает возможность улучшения известных асимптотических оценок средней трудоемкости решения задачи дискретного логарифмирования в интервале для группы с эффективным инвертированием.

Теорема 6. *[4] Пусть G — циклическая группа с эффективным инвертированием, пусть также $2|N$. Тогда для любого $\varepsilon > 0$ существует такой алгоритм решения задачи дискретного логарифмирования в интервале (см. определение 5) в группе G, что при случайном равновероятном выборе n, его средняя трудоемкость не превосходит $(1+\varepsilon)\sqrt{\frac{\pi N}{2}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций, где $N \to \infty$.*

Доказательство. Определим «домашнее» множество T и множество $\widetilde{T}$ представителей классов T

$$T = \{C(a) : -\frac{N}{2} \le a \le \frac{N}{2}\},$$

где $C(a)$ — множество (класс) пар, соответствующее классу эквивалентности точки вида aP, определенный в § 1.3,

$$\widetilde{T} = \{0, \ldots, \frac{N}{2}\}$$

(в работах [28, 43] такое множество называется фундаментальной областью «домашнего» множества). Обозначим T_0 объединение классов из множества T. Для регулирования размера «дикого» множества W введем параметр $k \in (0, 2)$ и положим

$$W_k = \{C(n+a) : -\frac{kN}{4} \le a \le \frac{kN}{4}\},$$

$$\widetilde{W}_k = \{a : -\frac{kN}{4} + n \le a \le \frac{kN}{4} + n\},$$

тогда

$$|\widetilde{W}_k| = 2 \cdot \lfloor k \cdot \frac{N}{4} \rfloor + 1.$$

Как и в алгоритме Годри-Шоста, будем параллельно вычислять последовательности точек

$$x_iP, x_i \in \widetilde{T}, i = 1, 2, \ldots, \tag{3.7}$$

$$Q + z_jP, z_j \in \widetilde{W_k}, j = 1, 2, \ldots \tag{3.8}$$

до тех пор, пока в них не найдутся две точки из одного класса эквивалентности, после чего находим решение задачи, как было показано в § 1.3 (при этом предполагается, что значения x_i и z_j выбираются случайно равновероятно и независимо из соответствующих множеств).

Для определения средней трудоемкости алгоритма воспользуемся теоремой 1, как это делается в § 1.2. Тогда в обозначениях теоремы $C = 2$: шары цвета 1 — это элементы множества $\widetilde{T}$, а шары цвета 2 — элементы множества $\widetilde{W_k}$. Вычисление последовательностей (3.7) и (3.8) происходит параллельно, поэтому мы можем считать, что $r_{j,1} = r_{j,2} = \frac{1}{2}$ для всех $j = 1, 2, \ldots$, откуда $p_1 = p_2 = \frac{1}{2}$. Множество урн в нашем случае — это $T \cup W_k$, и шар a попадает в урну $C(a)$. Ясно, что $N' = O(N)$.

Очевидно, что интересующая нас средняя трудоемкость, выраженная в количестве групповых операций, не превосходит математического ожидания суммарного числа $Z_{N'}$ значений x_i и $n + z_j$, выбираемых до появления значений x_k и $n + z_l$ таких, что $C(x_k) = C(n_1 + z_l)$. Вычислим условное математическое ожидание $\mathbf{M}(Z_{N'}|n)$ случайной величины $Z_{N'}$ при фиксированном n. Имеем:

$$q_{1,i} = \begin{cases} \frac{2}{N+2}, & \text{если } i \in T \\ 0, & \text{в противном случае} \end{cases}.$$

С учетом последнего равенства и утверждения теоремы 1 нас интересуют значения $q_{2,i}$ только для $i \in T \cap W_k$. Поскольку каждый класс $C(a)$ содержит не более 2 элементов, то $T \cap W_k$ разбивается на 2 непересекающихся подмножества $U_j, j = 1, 2$ таких, что в каждый класс из U_j попадает ровно j элементов из $\widetilde{W_k}$, т. е.

$$q_{2,i} = \frac{j}{|\widetilde{W_k}|}, i \in U_j.$$

Из двух последних равенств получаем:

$$A_{N'} = 2 \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{2}{N+2} \cdot \frac{1}{|\widetilde{W}_k|} \cdot \sum_{j=1}^{2} j \cdot |U_j| = \frac{|U|}{(N+2)|\widetilde{W}_k|},$$

где $U = \widetilde{W}_k \cap T_0$, и по теореме 1

$$\mathbf{M}(Z_{N'}|n) = \sqrt{\frac{\pi(N+2)|\widetilde{W}_k|}{2|U|}} + O_k(N^{\frac{1}{4}}). \tag{3.9}$$

Следуя работам [28, 43], положим $n = \frac{xN}{2}, |x| \leq 1$. Оценим мощность множества U в зависимости от значения x.

1. $n \in B_1 = \{xN : |x| \leq 1 - \frac{k}{2}\}$ (см. рис. 3.3) Вероятность события $n \in B_1$ равна $\frac{(1-k/2)N+1}{N+1}$. В этом случае множество $\widetilde{W}_k$ полностью содержится в T_0, т. е.

$$\frac{|\widetilde{W}_k|}{|U|} = 1$$

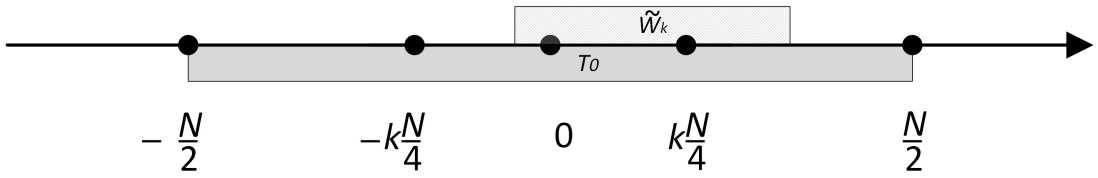

Рис. 3.3.

2. $n \in B_2 = \{xN : |x| > 1 - \frac{k}{2}\}$ (см. рис. 3.4) Вероятность события $n \in B_2$ равна $\frac{k \cdot N}{2(N+1)}$. В этом случае можно сделать оценку

$$\frac{|\widetilde{W}_k|}{|U|} \leq 2.$$

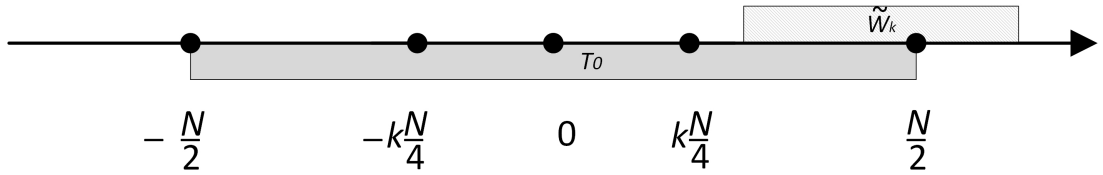

Рис. 3.4.

Теперь можем оценить математическое ожидание

$$\begin{aligned}\mathbf{M}(Z_{N'}) &= \frac{(1-\frac{k}{2})N+1}{N+1}\mathbf{M}(Z_{N'}|n\in B_1) + \frac{\frac{k}{2}\cdot N}{N+1}\cdot\mathbf{M}(Z_{N'}|n\in B_2)\\ &\le \frac{(1-\frac{k}{2})N+1}{N+1}\sqrt{\frac{\pi(N+2)}{2}} + \frac{\frac{k}{2}\cdot N}{N+1}\cdot\sqrt{\pi(N+2)} + O_k(N^{\frac{1}{4}})\\ &= \frac{(1+\frac{\sqrt{2}-1}{2}k)N+1}{N+1}\cdot\sqrt{\frac{\pi(N+2)}{2}} + O_k(N^{\frac{1}{4}})\end{aligned}$$

Т.е. при $N\to\infty$

$$\mathbf{M}(Z_{N'}) \le (1+\frac{(\sqrt{2}-1)k}{2})\sqrt{\frac{\pi N}{2}} + O_k(N^{\frac{1}{4}}),$$

откуда при $k\to 0$ получаем утверждение теоремы.

Теорема доказана. □

Из теоремы 6 получаем следующую модификацию алгоритма Годри-Шоста для решения задачи дискретного логарифмирования в интервале.

Алгоритм 2.

Вход. Группа G — подгруппа группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов; $P, Q \in G$, $N \in \mathbb{N}$, $Q = nP$ для некоторого (неизвестного) $n \in \{-\frac{N}{2}, \dots, \frac{N}{2}\}$, k — коэффициент сжатия «дикого» множества.
Выход: $n' \in \mathbb{Z}$ такое, что $Q = n'P$.

1. Инициализировать множества

$$\widetilde{T} = \{0, \dots, \frac{N}{2}\}$$

$$W_0 = \{a : -\frac{kN}{4} \leq a \leq \frac{kN}{4}\},$$

а также множества

$$S_{\widetilde{T}} = \varnothing,\ S_{\widetilde{W}} = \varnothing.$$

2. *Инициализировать счетчик шагов*

$$i = 1.$$

3. *Выполнить вычисление и сохранение очередного элемента «домашнего» множества.*

   (a) *выбрать элемент* $x_i \in_R \widetilde{T}$;

   (b) *вычислить* $P_{\widetilde{T}} = x_i P$;

   (c) *вычислить представитель* $P'_{\widetilde{T}}$ *класса эквивалентности* $\{P_{\widetilde{T}}, -P_{\widetilde{T}}\}$, *порожденного действием эффективного автоморфизма группы* G.

   (d) *добавить* $P'_{\widetilde{T}}$ *в множество* $S_{\widetilde{T}}$: $S_{\widetilde{T}} = S_{\widetilde{T}} \cup \{P'_{\widetilde{T}}\}$.

4. *Если* $S_{\widetilde{T}} \cap S_{\widetilde{W}} \neq \varnothing$, *перейти на шаг 8.*

5. *Выполнить вычисление и сохранение очередного элемента «дикого» множества.*

   (a) *выбрать элемент* $z_i \in_R W_0$;

   (b) *вычислить* $P_{\widetilde{W}} = Q + z_i P$;

   (c) *вычислить представитель* $P'_{\widetilde{W}}$ *класса эквивалентности* $\{P_{\widetilde{W}}, -P_{\widetilde{W}}\}$, *порожденного действием эффективного автоморфизма группы* G.

   (d) *добавить* $P'_{\widetilde{W}}$ *в множество* $S_{\widetilde{W}}$: $S_{\widetilde{W}} = S_{\widetilde{W}} \cup \{P'_{\widetilde{W}}\}$.

6. *Если* $S_{\widetilde{T}} \cap S_{\widetilde{W}} \neq \varnothing$, *перейти на шаг 8.*

7. *Увеличить значение счетчика* i, *перейти на шаг 3.*

8. Используя $S_{\widetilde{W}} \cap S_{\widetilde{T}}$, вычислить n.

Аналогично тому, как это делается в § 3.1.1, вычислим константу при главном члене в оценке средней трудоемкости решения задачи дискретного логарифмирования в интервале для различных значений размера «дикого» множества.

Для фиксированного $n \in \{-\frac{N}{2}, \ldots, \frac{N}{2}\}$ может быть вычислена мощность множества $\widetilde{W}_k \cap T_0$ (в обозначениях теоремы 6) и получена оценка средней трудоемкости алгоритма.

На множестве $\{-\frac{N}{2}, \ldots, \frac{N}{2}\}$ введем равномерную сетку:

$$\Omega_m = \{n^i = -\frac{N}{2} + ih, i = 0, \ldots, m; h = \frac{N}{m}\}.$$

Для проведения расчетов был реализован скрипт на языке python, с помощью которого для различных значений параметра k по формулам (3.9) была вычислена оценка средней трудоемкости алгоритма в каждом узле сетки Ω_m, а также усредненное значение по всем узлам.

Результаты проведенных вычислений константы при главном члене в оценке средней трудоемкости решения задачи дискретного логарифмирования в интервале с $m = 1000$ приведены в таблице 3.5 и согласуются с полученными ранее оценками средней трудоемкости алгоритма.

3.3 Выводы

К выводам главы 3 относятся следующие.

1. Автором выполнены расчеты константы при главном члене в оценке средней трудоемкости решения двумерной задачи дискретного логарифмирования (в группе с эффективным автоморфизмом) алгоритмом Годри-Шоста для различных размеров «дикого» множества.

2. Автором разработаны модификации алгоритма Годри-Шоста решения двумерной задачи дискретного логарифмирования и получены оценки средней трудоемкости:

Таблица 3.5: оценка средней трудоемкости решения задачи дискретного логарифмирования в интервале

Коэффициент сжатия «дикого» множества, k	Константа при главном члене в оценке средней трудоемкости
0.1	1.26406969161
0.2	1.27481951792
0.3	1.28557061692
0.4	1.29632203416
0.5	1.30707357871
0.6	1.31782518691
0.7	1.32857683148
0.8	1.33932849878
0.9	1.3500801812
1.0	1.36083187431 [1]
1.1	1.3715835751
1.2	1.38233528167

[1] результат получен в работе [28]

- для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов при $N_1 = N_2$ с оценкой средней трудоемкости $(1+\varepsilon)\sqrt{\frac{\pi N}{2}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций;
- для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax$ над конечным простым полем из $p \equiv 1 \bmod 4$ элементов при $P_2 = \varphi(P_1)$ и $N_1 = N_2$, где φ — эффективный автоморфизм порядка 4, с оценкой средней трудоемкости $(1+\varepsilon)\sqrt{\frac{\pi N}{4}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций;
- для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов при $P_2 = \varphi(P_1)$ и $N_1 = N_2$, где φ — эффективный автоморфизм порядка 6, с оценкой средней трудоемкости $(1+\varepsilon)\sqrt{\frac{\pi N}{4}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций.

Таким образом, получены наиболее эффективные в настоящее время алгоритмы решения указанных задач.

3. Автором предложена модификация алгоритма Годри-Шоста для решения задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием, и получена оценка средней трудоемкости, составляющая $(1+\varepsilon)\sqrt{\frac{\pi N}{2}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций в G. Разработанный алгоритм в настоящее время является наиболее эффективным известным методом решения указанной задачи.

В следующей главе будут представлены результаты численных экспериментов решения двумерной задачи дискретного логарифмирования и задачи дискретного логарифмирования в интервале с использованием разработанных модификаций алгоритма Годри-Шоста (алгоритмы 1, 2).

Глава 4

Численный эксперимент

В настоящей главе приводятся описание и результаты численных экспериментов с использованием изложенных в главе 3 вариантов алгоритма Годри-Шоста решения двумерной задачи дискретного логарифмирования в конечных циклических группах с эффективным автоморфизмом (алгоритм 1), а именно:

1) в случае подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов (эффективный автоморфизм порядка 2);

2) в случае подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax$ над конечным простым полем из $p \equiv 1 \bmod 4$ элементов (эффективный автоморфизм порядка 4);

3) в случае подгруппы группы точек эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов (эффективный автоморфизм порядка 6);

а также решения задачи дискретного логарифмирования в интервале для группы с эффективным инвертированием, а именно подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов (алгоритм 2).

4.1 Общая методика проведения численных экспериментов

Для проведения экспериментов для каждого из описанных вариантов двумерной задачи дискретного логарифмирования, а также задачи дискретного логарифмирования в интервале была выполнена программная реализация соответствующих вариантов алгоритма Годри-Шоста на языке python (листинг приведен в приложении В).

Для каждого из описанных вариантов двумерной задачи дискретного логарифмирования были выбраны по 3 набора параметров $\{p, A, B, P_1, q\}$, определяющих эллиптическую кривую $y^2 = x^3 + Ax + B$ над полем $GF(p)$ и точку P_1 большого простого порядка q, а также вычислена точка P_2.

- В случае подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов был выбран элемент $u \in_R [1,\ |\langle P_1 \rangle|)$, и вычислена $P_2 = uP_1$.

- В случае подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax$ над конечным простым полем из $p \equiv 1 \bmod 4$ элементов выбран элемент α порядка 4 по модулю p, и вычислены координаты точки P_2:

$$x_{P_2} = -x_{P_1},\ y_{P_2} = \alpha y_{P_1}.$$

- В случае подгруппы группы точек эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов выбран элемент β порядка 3 по модулю p, и вычислены координаты точки P_2:

$$x_{P_2} = \beta x_{P_1},\ y_{P_2} = -y_{P_1}.$$

Для каждой эллиптической кривой и для каждого значения коэффициента сжатия «дикого» множества $k = 0.1, 0.2, .., 1.0$ был проведен

ряд экспериментов с различными значениями параметра $N = 4N_1^2$: 6000 экспериментов с $N = 4000000$, 6000 экспериментов с $N = 36000000$.

Суть проводимых экспериментов состояла в следующем.

Описание эксперимента 1.

1. *Выбираются* $n_1, n_2 \in_R \{-N_1, \ldots, N_1\}$.
2. *Вычисляется* $Q = n_1 P_1 + n_2 P_2$.
3. *Для решения двумерной задачи дискретного логарифмирования (т. е. нахождения* $\{n_1', n_2' \in \{-N_1, \ldots, N_1\} : n_1' P_1 + n_2' P_2 = Q\}$*) применяется алгоритм 1, при этом выполняется подсчет количества произведенных групповых операций* c.
4. *Определяется коэффициент* $c_1 = \frac{c}{\sqrt{N}}$.

После этого для каждого N были вычислены средние значения c_1, аппроксимирующие константу при главном члене в оценке средней трудоемкости, и относительные погрешности от теоретических оценок, представленных в § 3.1.1.

Для случая задачи дискретного логарифмирования в интервале были выбраны 3 набора параметров $\{p, A, B, P, q\}$, определяющих эллиптическую кривую $y^2 = x^3 + Ax + B$ над полем $GF(p)$, а также точку P большого простого порядка q.

Для каждой эллиптической кривой и для каждого значения коэффициента сжатия «дикого» множества $k = 0.1, 0.2, .., 1.0$ был проведен ряд экспериментов с различными значениями параметра N: 6000 экспериментов с $N = 4000000$, 6000 экспериментов с $N = 32000000$.

Суть проводимых экспериментов состояла в следующем.

Описание эксперимента 2.

1. *Выбирается* $n_1 \in_R \{-\frac{N}{2}, \ldots, \frac{N}{2}\}$.
2. *Вычисляется* $Q = n_1 P$.

3. *Для решения задачи дискретного логарифмирования в интервале (т. е. нахождения* $\{n_1' \in \{-\frac{N}{2}, \ldots, \frac{N}{2}\} : n_1' P = Q\}$*) применяется алгоритм 2, при этом выполняется подсчет количества произведенных групповых операций* c*.*

4. *Определяется коэффициент* $c_1 = \frac{c}{\sqrt{N}}$*.*

После этого для каждого N были вычислены средние значения c_1, аппроксимирующие константу при главном члене в оценке средней трудоемкости, и относительные погрешности от теоретических оценок, представленных в § 3.2.

Следующие параграфы для каждого из описанных вариантов двумерной задачи дискретного логарифмирования, а также задачи дискретного логарифмирования в интервале содержат описание выбранных параметров эллиптических кривых, а также результаты проведенных экспериментов.

4.2 Двумерная задача в конечных циклических группах с эффективным автоморфизмом порядка 2

Настоящий параграф содержит детальное описание параметров и результатов экспериментов по решению двумерной задачи дискретного логарифмирования в группе с эффективным автоморфизмом порядка 2, а именно в подгруппе группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов.

Для проведения эксперимента были выбраны наборы параметров *secp256r1*, *secp192r1* и *secp112r1* (входят в число стандартизированных консорциумом SECG [13]), задающие соответствующие эллиптические кривые.

Набор 256-битных параметров *secp256r1* представлен множеством $\{p, A, B, P_1, q\}$ и задает эллиптическую кривую над полем $GF(p)$.

Конечное поле $GF(p)$ определено простым числом p:

$$p = 2^{224}(2^{32} - 1) + 2^{192} + 2^{96} - 1.$$

Эллиптическая кривая $y^2 = x^3 + Ax + B$ над полем $GF(p)$ определена параметрами

$$A = 115792089210356248762697446949407573530086143415290314195533631308867097853948,$$

$$B = 41058363725152142129326129780047268409114441015993725554835256314039467401291.$$

Образующий элемент P_1 подгруппы группы точек эллиптической кривой задан своими координатами

$$x_{P_1} = 48439561293906451759052585252797914202762949526041747995844080717082404635286,$$

$$y_{P_1} = 36134250956749795798585127919587881956611106672985015071877198253568414405109$$

и имеет порядок

$$q = 115792089210356248762697446949407573529996955224135760342422259061068512044369.$$

Результаты проведенных экспериментов по решению двумерной задачи дискретного логарифмирования для эллиптической кривой, заданной параметрами *secp256r1*, приведены в таблице 4.1. Видно, что они хорошо согласуются с теоретическими оценками, представленными в таблице 3.1: относительная погрешность при $N = 4000000$ менее 4.8%, а при $N = 36000000$ — менее 1.3%.

Набор 192-битных параметров *secp192r1* представлен множеством $\{p, A, B, P_1, q\}$ и задает эллиптическую кривую над полем $GF(p)$.
Конечное поле $GF(p)$ определено простым числом p:

$$p = 2^{192} - 2^{64} - 1.$$

Таблица 4.1: результаты численного эксперимента для набора параметров *secp256r1*

Коэффициент сжатия «дикого» множества, k	N=4000000, количество экспериментов=6000	Относительная погрешность, %	N=36000000, количество экспериментов=6000	Относительная погрешность, %
1.0	1.48097	0.23	1.49667	1.29
0.9	1.46629	0.82	1.45104	0.23
0.8	1.42841	0.20	1.43352	0.16
0.7	1.42225	0.98	1.41325	0.35
0.6	1.39652	0.78	1.37522	0.76
0.5	1.36455	0.10	1.36642	0.24
0.4	1.33187	0.67	1.33774	0.23
0.3	1.31821	0.04	1.31418	0.34
0.2	1.32447	2.13	1.29484	0.15
0.1	1.33528	4.72	1.27010	0.39

Эллиптическая кривая $y^2 = x^3 + Ax + B$ над полем $GF(p)$ определена параметрами

$$A = 62771017353866807638357894232076664160839087003903249612 76,$$

$$B = 24551555460089438177402939151974517847691080581611912380 65.$$

Образующий элемент P_1 подгруппы группы точек эллиптической кривой задан своими координатами

$$x_{P_1} = 60204628237568865675821348058752611191669897663688468 4818,$$

$$y_{P_1} = 17405033229362203140485755228021941036402348892738665 0641$$

и имеет порядок

$$q = 62771017353866807638357894231760590137671947731828422840 81.$$

Результаты проведенных экспериментов по решению двумерной задачи дискретного логарифмирования для эллиптической кривой, заданной

Таблица 4.2: Результаты численного эксперимента для параметров *secp192r1*

Коэффициент сжатия «дикого» множества, k	N=4000000, количество экспериментов=6000	Относительная погрешность, %	N=36000000, количество экспериментов=6000	Относительная погрешность, %
1.0	1.46314	0.98	1.49280	1.03
0.9	1.45742	0.21	1.43763	1.15
0.8	1.43789	0.46	1.43120	0.00
0.7	1.42681	1.31	1.39483	0.96
0.6	1.39112	0.39	1.40425	1.34
0.5	1.36712	0.29	1.36140	0.13
0.4	1.35207	0.84	1.34403	0.24
0.3	1.32674	0.61	1.33726	1.41
0.2	1.30562	0.68	1.29238	0.34
0.1	1.32533	3.94	1.27400	0.09

параметрами *secp192r1*, приведены в таблице 4.2. Видно, что они хорошо согласуются с теоретическими оценками, представленными в таблице 3.1: относительная погрешность при $N = 4000000$ менее 4.0%, а при $N = 36000000$ — менее 1.5%.

Набор 112-битных параметров *secp112r1* представлен множеством $\{p, A, B, P_1, q\}$ и задает эллиптическую кривую над полем $GF(p)$.
Конечное поле $GF(p)$ определено простым числом p:

$$p = (2^{128} - 3)/76439.$$

Эллиптическая кривая $y^2 = x^3 + Ax + B$ над полем $GF(p)$ определена параметрами

$$A = 4451685225093714772084598273548424,$$

$$B = 2061118396808653202902996166388514.$$

Образующий элемент P_1 подгруппы группы точек эллиптической кривой

Таблица 4.3: Результаты численного эксперимента для параметров *secp112r1*

Коэффициент сжатия «дикого» множества, k	N=4000000, количество экспериментов=6000	Относительная погрешность, %	N=36000000, количество экспериментов=6000	Относительная погрешность, %
1.0	1.48460	0.47	1.49414	1.12
0.9	1.45880	0.31	1.44049	0.95
0.8	1.42484	0.45	1.42804	0.23
0.7	1.40251	0.42	1.40992	0.11
0.6	1.41222	1.91	1.37251	0.95
0.5	1.35732	0.43	1.38477	1.58
0.4	1.34598	0.38	1.32881	0.90
0.3	1.32408	0.41	1.33296	1.08
0.2	1.29580	0.08	1.29861	0.14
0.1	1.31688	3.28	1.28596	0.85

задан своими координатами

$$x_{P_1} = 1882814650579725348922237787137 52,$$

$$y_{P_1} = 3419875491033170827167861896082688$$

и имеет порядок

$$q = 4451685225093714776491891542548933.$$

Результаты проведенных экспериментов по решению двумерной задачи дискретного логарифмирования для эллиптической кривой, заданной параметрами *secp112r1*, приведены в таблице 4.3. Видно, что они хорошо согласуются с теоретическими оценками, представленными в таблице 3.1: относительная погрешность при $N = 4000000$ менее 3.3%, а при $N = 36000000$ — менее 1.6%.

Следующий параграф содержит описание аналогичных экспериментов для групп с эффективным автоморфизмом порядка 4.

4.3 Двумерная задача в конечных циклических группах с эффективным автоморфизмом порядка 4

Настоящий параграф содержит детальное описание параметров и результатов экспериментов по решению двумерной задачи дискретного логарифмирования в группе с эффективным автоморфизмом порядка 4, а именно в подгруппе группы точек эллиптической кривой $y^2 = x^3 + Ax$ над конечным простым полем из $p \equiv 1 \bmod 4$ элементов.

Для проведения эксперимента с использованием математического пакета *Sage*[58] и алгоритма SEA [23, 20, 16, 47, 55] были выработаны наборы параметров E_1, E_2, E_3 и соответствующие им эллиптические кривые.

Набор 256-битных параметров E_1 представлен множеством $\{p, A, B, P_1, q\}$ и задает эллиптическую кривую над полем $GF(p)$.
Конечное поле $GF(p)$ определено простым числом p:

$$p = 101697139093680649955721589642330135261085947328513614498992339341860481594681.$$

Эллиптическая кривая $y^2 = x^3 + Ax + B$ над полем $GF(p)$ определена параметрами

$$A = 290935661046100636546724796820786591778 3,\ B = 0.$$

Образующий элемент P_1 подгруппы группы точек эллиптической кривой задан своими координатами

$$x_{P_1} = 760326245438067336891998545440518260657190462297804638401343924547740590454 84,$$

$$y_{P_1} = 231321330778271593484512920018593434332867080992116069596673374101621970475 57$$

и имеет порядок

$$q = 21274538578498275657876184688224704246907033833756057 97.$$

Для кривой, заданной параметрами E_1, был вычислен элемент порядка 4 по модулю p:

$$\alpha = 90453885126975965566034904908947760848536432355930775594036079789012667762769.$$

В таком случае $P_2 = \varphi(P_1)$ задана координатами

$$x_{P_2} = 25664514549873916266521735098278309195366901098733150658857946887086422549197;$$

$$x_{P_2} = 72651207633467805363748967934330799927253287542129869768448941187725421254 61;$$

Результаты проведенных экспериментов по решению двумерной задачи дискретного логарифмирования для эллиптической кривой, заданной параметрами E_1, приведены в таблице 4.4. Видно, что они хорошо согласуются с теоретическими оценками, представленными в таблице 3.2: относительная погрешность при $N = 4000000$ менее 2%, а при $N = 36000000$ — менее 1.5%.

Набор 192-битных параметров E_2 представлен множеством $\{p, A, B, P_1, q\}$ и задает эллиптическую кривую над полем $GF(p)$.
Конечное поле $GF(p)$ определено простым числом p:

$$p = 34159595325388058507604257415299814957311777569846337389 73.$$

Эллиптическая кривая $y^2 = x^3 + Ax + B$ над полем $GF(p)$ определена параметрами

$$A = 33178100315863813550203963 63,\ B = 0.$$

Образующий элемент P_1 подгруппы группы точек эллиптической кривой задан своими координатами

$$x_{P_1} = 70437783749540372983936925692072820432247256723278963 1467,$$

Таблица 4.4: Результаты численного эксперимента для набора параметров E_1

Коэффициент сжатия «дикого» множества, k	N=4000000, количество экспериментов=6000	Относительная погрешность, %	N=36000000, количество экспериментов=6000	Относительная погрешность, %
1.0	1.05108	0.60	1.05401	0.88
0.9	1.03335	0.48	1.02235	0.59
0.8	1.01716	0.50	1.01291	0.08
0.7	0.99064	0.53	0.98847	0.74
0.6	0.97730	0.26	0.97973	0.01
0.5	0.97536	1.19	0.97489	1.14
0.4	0.95735	0.97	0.94682	0.14
0.3	0.93317	0.07	0.91913	1.43
0.2	0.93022	1.45	0.92357	0.72
0.1	0.91885	1.91	0.90378	0.24

$$y_{P_1} = 2010798210574770737641892516468201281307023158544210389943$$

и имеет порядок

$$q = 7035985656443462210920975052 81.$$

Для кривой, заданной параметрами E_2, был вычислен элемент порядка 4 по модулю p:

$$\alpha = 260283030179885484762613633115236474270688763927449846238.$$

В таком случае $P_2 = \varphi(P_1)$ задана координатами

$$x_{P_2} = 271158169504340212092105648460925329140870518975184410750 6;$$

$$y_{P_2} = 126404010250148324295683333361226908917158392287613669904 9.$$

Результаты проведенных экспериментов по решению двумерной задачи дискретного логарифмирования для эллиптической кривой, задан-

Таблица 4.5: Результаты численного эксперимента для набора параметров E_2

Коэффициент сжатия «дикого» множества, k	N=4000000, количество экспериментов=6000	Относительная погрешность, %	N=36000000, количество экспериментов=6000	Относительная погрешность, %
1.0	1.04114	0.35	1.03735	0.71
0.9	1.02826	0.01	1.02413	0.41
0.8	1.02587	1.36	1.01532	0.32
0.7	1.00171	0.58	1.00085	0.50
0.6	0.99826	1.88	0.98551	0.58
0.5	0.96437	0.05	0.97123	0.76
0.4	0.95592	0.82	0.94067	0.79
0.3	0.93403	0.17	0.93106	0.15
0.2	0.92720	1.12	0.91791	0.10
0.1	0.92437	2.52	0.91883	1.91

ной параметрами E_2, приведены в таблице 4.5. Видно, что они хорошо согласуются с теоретическими оценками, представленными в таблице 3.2: относительная погрешность при $N = 4000000$ менее 2.6%, а при $N = 36000000$ — менее 2%.

Набор 112-битных параметров E_3 представлен множеством $\{p, A, B, P_1, q\}$ и задает эллиптическую кривую над полем $GF(p)$.
Конечное поле $GF(p)$ определено простым числом p:

$$p = 4841238326157243383903720159171921.$$

Эллиптическая кривая $y^2 = x^3 + Ax + B$ над полем $GF(p)$ определена параметрами

$$A = 22941412381246327,\ B = 0.$$

Образующий элемент P_1 подгруппы группы точек эллиптической кривой задан своими координатами:

$$x_{P_1} = 2651106297925279844851686784471241,$$

$$y_{P_1} = 933146249502556412223509092230002$$

и имеет порядок

$$q = 73135091417719572557297.$$

Для кривой, заданной параметрами E_3, был вычислен элемент порядка 4 по модулю p:

$$\alpha = 239518580906517470181602736988889.$$

В таком случае $P_2 = \varphi(P_1)$ задана координатами

$$x_{P_2} = 219013202823196353905203337470068 0;$$

$$y_{P_2} = 219743326241374214018738833270036 6.$$

Результаты проведенных экспериментов по решению двумерной задачи дискретного логарифмирования для эллиптической кривой, заданной параметрами E_3, приведены в таблице 4.6. Видно, что они хорошо согласуются с теоретическими оценками, представленными в таблице 3.2: относительная погрешность при $N = 4000000$ менее 2.8%, а при $N = 36000000$ — менее 2.2%.

Следующий параграф содержит описание аналогичных экспериментов для групп с эффективным автоморфизмом порядка 6.

4.4 Двумерная задача в конечных циклических группах с эффективным автоморфизмом порядка 6

Настоящий параграф содержит детальное описание параметров и результатов экспериментов по решению двумерной задачи дискретного логарифмирования в группе с эффективным автоморфизмом порядка 6, а именно в подгруппе группы точек эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов (такие эллиптические кривые получили широкое распространение и входят в число стандартизированных консорциумом SECG).

Таблица 4.6: Результаты численного эксперимента для набора параметров E_3

Коэффициент сжатия «дикого» множества, k	N=4000000, количество экспериментов=6000	Относительная погрешность, %	N=36000000, количество экспериментов=6000	Относительная погрешность, %
1.0	1.04789	0.29	1.05038	0.53
0.9	1.03200	0.35	1.03979	1.11
0.8	1.01168	0.04	1.03346	2.11
0.7	0.99287	0.30	0.99940	0.35
0.6	0.97784	0.20	0.99173	1.21
0.5	0.96639	0.26	0.96800	0.42
0.4	0.95373	0.59	0.94566	0.26
0.3	0.92956	0.31	0.93986	0.79
0.2	0.91186	0.56	0.91091	0.66
0.1	0.92659	2.77	0.90801	0.71

Для проведения эксперимента были выбраны наборы параметров *secp256k1*, *secp192k1* и *secp160k1*, которым соответствуют эллиптические кривые, предложенные Н. Коблицем в работе [40]. Указанные эллиптические кривые используются в ряде прикладных программ, так, например, кривая, заданная параметрами *secp256k1*, используется в схеме цифровой подписи в виртуальной валюте Bitcoin [48, 7].

Набор 256-битных параметров *secp256k1* представлен множеством $\{p, A, B, P_1, q\}$ и задает эллиптическую кривую над полем $GF(p)$.
Конечное поле $GF(p)$ определено простым числом p:

$$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1.$$

Эллиптическая кривая $y^2 = x^3 + Ax + B$ над полем $GF(p)$ определена параметрами

$$A = 0,\ B = 7.$$

Образующий элемент P_1 подгруппы группы точек эллиптической кривой

задан своими координатами:

$$x_{P_1} = 55066263022277343669578718895168534326250603453777594175500187360389116729240,$$

$$y_{P_1} = 32670510020758816978083085130507043184471273380659243275938904335757337482424$$

и имеет порядок

$$q = 11579208923731619542357098500868790785283756427907490438260516314151816149433 7.$$

Для кривой, заданной параметрами *secp256k1*, был вычислен элемент порядка 3 по модулю p:

$$\beta = 55594575648329892869085402983802832744385952214688224221778511981742606582254.$$

В таком случае $P_2 = \varphi(P_1)$ задана координатами

$$x_{P_2} = 85340279321737800624759429340272274763154997815782306132637707972559913914315;$$

$$y_{P_2} = 83121579216557378445487899878180864668798711284981320763518679672151497189239.$$

Результаты проведенных экспериментов по решению двумерной задачи дискретного логарифмирования для эллиптической кривой, заданной параметрами *secp256k1*, приведены в таблице 4.7. Видно, что они хорошо согласуются с теоретическими оценками, представленными в таблице 3.3: относительная погрешность при $N = 4000000$ менее 4.8%, а при $N = 36000000$ — менее 0.8%.

Набор 192-битных параметров *secp192k1* представлен множеством $\{p, A, B, P_1, q\}$ и задает эллиптическую кривую над полем $GF(p)$.
Конечное поле $GF(p)$ определено простым числом p:

$$p = 2^{192} - 2^{32} - 2^{12} - 2^8 - 2^7 - 2^6 - 2^3 - 1.$$

Таблица 4.7: Результаты численного эксперимента для набора параметров *secp256k1*

Коэффициент сжатия «дикого» множества, k	N=4000000, количество экспериментов=6000	Относительная погрешность, %	N=36000000, количество экспериментов=6000	Относительная погрешность, %
1.0	0.97859	0.05	0.98207	0.40
0.9	0.96262	0.50	0.96189	0.58
0.8	0.95170	0.57	0.95143	0.60
0.7	0.93875	0.89	0.95187	0.49
0.6	0.93615	0.15	0.94429	0.72
0.5	0.93810	1.07	0.92568	0.27
0.4	0.92900	1.07	0.91543	0.41
0.3	0.91476	0.47	0.91139	0.10
0.2	0.91038	0.92	0.90755	0.60
0.1	0.93653	4.75	0.89537	0.15

Эллиптическая кривая $y^2 = x^3 + Ax + B$ над полем $GF(p)$ определена параметрами

$$A = 0,\ B = 3.$$

Образующий элемент P_1 подгруппы группы точек эллиптической кривой задан своими координатами:

$$x_{P_1} = 5377521262291226325198505011805525673063229037935769709693,$$

$$y_{P_1} = 3805108391982600717572440947423858335415441070543209377693$$

и имеет порядок

$$q = 6277101735386680763835789423061264271957123915200845512077.$$

Для кривой, заданной параметрами *secp192k1*, был вычислен элемент порядка 3 по модулю p:

$$\beta = 1679096885901416186754303577286424073753807680599501814388.$$

Таблица 4.8: Результаты численного эксперимента для набора параметров *secp192k1*

Коэффициент сжатия «дикого» множества, k	N=4000000, количество экспериментов=6000	Относительная погрешность, %	N=36000000, количество экспериментов=6000	Относительная погрешность, %
1.0	0.96152	1.70	0.97797	0.02
0.9	0.97250	0.52	0.97240	0.51
0.8	0.95697	0.02	0.96838	1.17
0.7	0.95821	1.16	0.94700	0.02
0.6	0.92695	1.13	0.94493	0.79
0.5	0.93077	0.28	0.91414	1.52
0.4	0.92117	0.22	0.92546	0.68
0.3	0.92055	1.10	0.90985	0.07
0.2	0.91556	1.49	0.91008	0.88
0.1	0.91316	2.14	0.90858	1.62

В таком случае $P_2 = \varphi(P_1)$ задана координатами

$$x_{P_2} = 164110467967893616465613147583474543580537468012625450084 2;$$

$$y_{P_2} = 247199334340408004626334847578380808068691437391653016335 4.$$

Результаты проведенных экспериментов по решению двумерной задачи дискретного логарифмирования для эллиптической кривой, заданной параметрами *secp192k1*, приведены в таблице 4.8. Видно, что они хорошо согласуются с теоретическими оценками, представленными в таблице 3.3: относительная погрешность при $N = 4000000$ менее 2.2%, а при $N = 36000000$ — менее 1.7%.

Набор 160-битных параметров *secp160k1* [12] представлен множеством $\{p, A, B, P_1, q\}$ и задает эллиптическую кривую над полем $GF(p)$. Конечное поле $GF(p)$ определено простым числом p:

$$p = 2^{160} - 2^{32} - 2^{14} - 2^{12} - 2^9 - 2^8 - 2^7 - 2^3 - 2^2 - 1.$$

Эллиптическая кривая $y^2 = x^3 + Ax + B$ над полем $GF(p)$ определена параметрами

$$A = 0,\ B = 7.$$

Образующий элемент P_1 подгруппы группы точек эллиптической кривой задан своими координатами:

$$x_{P_1} = 338530205676502674729549372677647997389429898939,$$

$$y_{P_1} = 842365456698940303598009444920994870805149798382$$

и имеет порядок

$$q = 1461501637330902918203686915170869725397159163571.$$

Для кривой, заданной параметрами *secp160k1*, был вычислен элемент порядка 3 по модулю p:

$$\beta = 57293848650217072588620685307280219362697915479 2.$$

В таком случае $P_2 = \varphi(P_1)$ задана координатами

$$x_{P_2} = 269020659200579711614992709933274387611448004311;$$

$$y_{P_2} = 619136180631962614605675387795288148846487755909.$$

Результаты проведенных экспериментов по решению двумерной задачи дискретного логарифмирования для эллиптической кривой, заданной параметрами *secp160k1*, приведены в таблице 4.9. Видно, что они хорошо согласуются с теоретическими оценками, представленными в таблице 3.3: относительная погрешность при $N = 4000000$ менее 2.6%, а при $N = 36000000$ — менее 1.5%.

Следующий параграф содержит описание аналогичных экспериментов для задачи дискретного логарифмирования в интервале.

Таблица 4.9: Результаты численного эксперимента для набора параметров *secp160k1*

Коэффициент сжатия «дикого» множества, k	N=4000000, количество экспериментов=6000	Относительная погрешность, %	N=36000000, количество экспериментов=6000	Относительная погрешность, %
1.0	0.97355	0.47	0.97522	0.30
0.9	0.95592	1.19	0.97296	0.57
0.8	0.95662	0.06	0.95171	0.57
0.7	0.95168	0.47	0.93607	1.17
0.6	0.93643	0.12	0.93999	0.26
0.5	0.93009	0.20	0.93350	0.57
0.4	0.91925	0.01	0.91593	0.36
0.3	0.90773	0.30	0.91651	0.66
0.2	0.90662	0.50	0.90033	0.20
0.1	0.91649	2.51	0.90722	1.47

4.5 Задача дискретного логарифмирования в интервале

Настоящий параграф содержит детальное описание параметров и результатов экспериментов по решению задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием.

Задача дискретного логарифмирования в интервале рассматривается для циклической группы с эффективным автоморфизмом порядка 2, а именно подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов. Для проведения эксперимента были выбраны наборы параметров *nist-p-256*, *nist-p-192* (стандартизованы NIST [38]) и *brainpoolP160r1* (входит в стандарт рабочей группы Brainpool [61]), задающие соответствующие эллиптические кривые.

Набор 256-битных параметров *nist-p-256* представлен множеством

$\{p, A, B, P, q\}$ и задает эллиптическую кривую над полем $GF(p)$.
Конечное поле $GF(p)$ определено простым числом p:

$$p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1.$$

Эллиптическая кривая $y^2 = x^3 + Ax + B$ над полем $GF(p)$ определена параметрами

$$A = -3,$$

$$B = 41058363725152142129326129780047268409114441015993725554835256314039467401291.$$

Образующий элемент P подгруппы группы точек эллиптической кривой задан своими координатами:

$$x_P = 48439561293906451759052585252797914202762949526041747995844080717082404635286,$$

$$y_P = 36134250956749795798585127919587881956611106672985015071877198253568414405109$$

и имеет порядок

$$q = 11579208921035624876269744694940757352999695522413576034242225906106851204436 9;$$

Результаты проведенных экспериментов по решению задачи дискретного логарифмирования в интервале для эллиптической кривой, заданной параметрами *nist-p-256*, приведены в таблице 4.10. Видно, что они хорошо согласуются с теоретическими оценками, представленными в таблице 3.5: относительная погрешность для заданной эллиптической кривой менее 1.4%.

Набор 192-битных параметров *nist-p-192* представлен множеством $\{p, A, B, P, q\}$ и задает эллиптическую кривую над полем $GF(p)$.
Конечное поле $GF(p)$ определено простым числом p:

$$p = 2^{192} - 2^{64} - 1.$$

Таблица 4.10: Результаты численного эксперимента для набора параметров *nist-p-256*

Коэффициент сжатия «дикого» множества, k	N=4000000, количество экспериментов=6000	Относительная погрешность, %	N=32000000, количество экспериментов=6000	Относительная погрешность, %
1.0	1.37745	1.22	1.36364	0.21
0.9	1.36322	0.97	1.34035	0.72
0.8	1.33335	0.45	1.33187	0.56
0.7	1.33090	0.17	1.34656	1.35
0.6	1.30860	0.70	1.31822	0.03
0.5	1.30393	0.24	1.32332	1.24
0.4	1.30371	0.57	1.29131	0.39
0.3	1.28433	0.10	1.27457	0.86
0.2	1.28625	0.90	1.27214	0.21
0.1	1.26288	0.09	1.27117	0.56

Эллиптическая кривая $y^2 = x^3 + Ax + B$ над полем $GF(p)$ определена параметрами

$$A = -3,$$

$$B = 24551555460089438177402939151974517847691080581611912380 65.$$

Образующий элемент P подгруппы группы точек эллиптической кривой задан своими координатами:

$$x_P = 60204628237568865675821348058752611191669897663688468 4818,$$

$$y_P = 17405033229362203140485755228021941036402348892738665 0641$$

и имеет порядок

$$q = 62771017353866807638357894231760590137671947731828422840 81.$$

Результаты проведенных экспериментов по решению задачи дискретного логарифмирования в интервале для эллиптической кривой, заданной параметрами *nist-p-192*, приведены в таблице 4.11. Видно, что они

Таблица 4.11: Результаты численного эксперимента для набора параметров *nist-p-192*

Коэффициент сжатия «дикого» множества, k	N=4000000, количество экспериментов=6000	Относительная погрешность, %	N=32000000, количество экспериментов=6000	Относительная погрешность, %
1.0	1.36876	0.58	1.35610	0.35
0.9	1.35586	0.43	1.36461	1.08
0.8	1.35897	1.47	1.33372	0.42
0.7	1.33117	0.20	1.34757	1.43
0.6	1.30189	1.21	1.30605	0.89
0.5	1.31259	0.42	1.30266	0.34
0.4	1.29319	0.24	1.29627	0.00
0.3	1.28453	0.08	1.29303	0.58
0.2	1.27619	0.11	1.28682	0.94
0.1	1.26096	0.25	1.26353	0.04

хорошо согласуются с теоретическими оценками, представленными в таблице 3.5: относительная погрешность для заданной эллиптической кривой менее 1.5%.

Набор 160-битных параметров *brainpoolP160r1* представлен множеством $\{p, A, B, P, q\}$ и задает эллиптическую кривую над полем $GF(p)$. Конечное поле $GF(p)$ определено простым числом p:

$$p = 1332297598440044874827085558802491743757193798159.$$

Эллиптическая кривая $y^2 = x^3 + Ax + B$ над полем $GF(p)$ определена параметрами

$$A = 297190522446607939568481567949428902921613329152,$$

$$B = 173245649450172891208247283053495198538671808088.$$

Образующий элемент P подгруппы группы точек эллиптической кривой задан своими координатами:

$$x_P = 108947355763143528457796253973853251592056608249 9,$$

$$y_P = 127912481829969033206777085249718746721365418785.$$

и имеет порядок

$$q = 133229759844004487482708503883018136421294256845 7.$$

Результаты проведенных экспериментов по решению задачи дискретного логарифмирования в интервале для эллиптической кривой, заданной параметрами *brainpoolP160r1*, приведены в таблице 4.12. Видно, что они хорошо согласуются с теоретическими оценками, представленными в таблице 3.5: относительная погрешность для заданной эллиптической кривой менее 1.3%.

Таблица 4.12: Результаты численного эксперимента для набора параметров *brainpoolP160r1*

Коэффициент сжатия «дикого» множества, k	N=4000000, количество экспериментов=6000	Относительная погрешность, %	N=32000000, количество экспериментов=6000	Относительная погрешность, %
1.0	1.35226	0.63	1.34530	1.14
0.9	1.34347	0.49	1.35421	0.31
0.8	1.34010	0.06	1.33612	0.24
0.7	1.32993	0.10	1.32296	0.42
0.6	1.32898	0.85	1.31837	0.04
0.5	1.30292	0.32	1.31614	0.69
0.4	1.29507	0.10	1.28969	0.51
0.3	1.28566	0.01	1.28019	0.42
0.2	1.28110	0.49	1.28453	0.76
0.1	1.27739	1.05	1.28028	1.28

4.6 Выводы

К выводам главы 4 относятся следующие.

1. Для двумерной задачи дискретного логарифмирования автором разработана программная реализация модификации алгоритма

Годри-Шоста (алгоритм 1) и продемонстрирована согласованность теоретических оценок средней трудоемкости (таблицы 3.1, 3.2, 3.3) с экспериментальными.

2. Для задачи дискретного логарифмирования в интервале автором разработана программная реализация модификации алгоритма Годри-Шоста (алгоритм 2) и продемонстрирована согласованность теоретических оценок средней трудоемкости (таблица 3.5) с экспериментальными.

Заключение

В ходе работы получены следующие результаты.

- Разработана модификация алгоритма Годри-Шоста решения двумерной задачи дискретного логарифмирования в случае подгруппы группы точек эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов при $P_2 = \varphi(P_1)$ и $N_1 = N_2$, где φ — эффективный автоморфизм порядка 6. Оценка средней трудоемкости разработанного алгоритма составляет $(0.978 + o(1))\sqrt{N}$ групповых операций, где $N = 4N_1N_2$.

- Разработаны наиболее эффективные в настоящее время алгоритмы решения двумерной задачи дискретного логарифмирования, которые являются модификациями алгоритма Годри-Шоста:

  1) для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов при $N_1 = N_2$ с оценкой средней трудоемкости $(1 + \varepsilon)\sqrt{\frac{\pi N}{2}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций, где $N = 4N_1N_2$;
  2) для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + Ax$ над конечным простым полем из $p \equiv 1 \bmod 4$ элементов при $P_2 = \varphi(P_1)$ и $N_1 = N_2$, где φ — эффективный автоморфизм порядка 4, с оценкой средней трудоемкости $(1 + \varepsilon)\sqrt{\frac{\pi N}{4}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций, где $N = 4N_1N_2$;
  3) для случая подгруппы группы точек эллиптической кривой $y^2 = x^3 + B$ над конечным простым полем из $p \equiv 1 \bmod 3$ элементов при $P_2 = \varphi(P_1)$ и $N_1 = N_2$, где φ — эффектив-

ный автоморфизм порядка 6, с оценкой средней трудоемкости $(1+\varepsilon)\sqrt{\frac{\pi N}{4}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций, где $N = 4N_1N_2$.

- Разработана модификация алгоритма Годри-Шоста решения задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием, и получена оценка среденй трудоемкости, составляющая $(1+\varepsilon)\sqrt{\frac{\pi N}{2}} + O_\varepsilon(N^{\frac{1}{4}})$ групповых операций в G. Разработанный алгоритм в настоящее время является наиболее эффективным известным методом решения указанной задачи.

Варианты дальнейших исследований по теме.

1) Уточнение асимптотических оценок средней трудоемкости решения двумерной задачи дискретного логарифмирования и задачи дискретного логарифмирования в интервале алгоритмом Годри-Шоста. В текущих асимптотических оценках для указанных задач определены только константы при старшем члене.

2) Уточнение оценок средней трудоемкости решения двумерной задачи дискретного логарифмирования и задачи дискретного логарифмирования в интервале для практической реализации алгоритма Годри-Шоста. Необходимо проанализировать модификации алгоритма Годри-Шоста для решения указанных задач с учетом ограниченного объема памяти.

3) Анализ возможности разработки модификаций алгоритма Годри-Шоста для решения двумерной задачи дискретного логарифмирования и задачи дискретного логарифмирования в интервале для других групп с эффективными автоморфизмами.

4) Анализ возможности применения алгоритма Годри-Шоста и его модификаций для решения других обобщений классической задачи дискретного логарифмирования.

Список сокращений и обозначений

$A \times B$	декартово произведение множеств
GLV	метод Галланта-Ламберта-Ванстоуна разложения кратной точки эллиптической кривой в сумму кратных точек
$O_\varepsilon(...)$	константа, скрывающаяся под символом O, зависит от ε
$\mathbb{Z}$	множество целых чисел
$\mathbb{N}$	множество натуральных чисел
$\mid S \mid$	мощность множества S
$a \equiv b \bmod p$	$a - b$ делится на p
$GF(p)$	поле из p элементов
$\langle P \rangle$	циклическая группа с образующим элементом P
$a \in_R S$	элемент a выбирается случайным равновероятным образом из множества S

Приложение А

Оценка средней трудоемкости для некоторых значений параметров алгоритма Годри-Шоста

```
1  from shapely.geometry import Polygon
2  from shapely.affinity import translate
3  from shapely.affinity import scale
4  from math import sqrt
5  from math import pi
6  from random import random
7
8  f = open("p_log.txt", "w")
9
10 #размер сетки
11 step = 200
12
```

```
13 #количество итераций изменения размера дикого множества
14 step2 = 12
15
16 #количество итераций изменения размера домашнего
       множества
17 step3 = 1
18
19 for q in range (step2):
20   for w in range (step3):
21     #определяем коэффициенты изменения множеств
22     p2_scale_x = 0.1 + q*0.1
23     p2_scale_y = 0.1 + q*0.1
24     p1_scale_x = 1.0
25     p1_scale_y = 1.0
26
27     ans = 0
28
29     #определяем домашнее (p1) и дикое (p2) множества
30
31     #случай кривой y^2=x^3+Ax+B над конечным полем из p
         >3 элементов
32     #p1 = Polygon([(1, 1), (-1, 1), (-1, -1), (1, -1),
         (1, 1)])
33
34     #случай кривой y^2=x^3+Ax, при p = 1 (mod 4)
35     #p1 = Polygon([(1, 1), (-1, 1), (-1, -1), (1, -1),
         (1, 1)])
36
37     #случай кривой y^2=x^3+B при p = 1 (mod 3)
38     p1 = Polygon([(1, 1), (0, 1), (-1, 2), (-1, 1),
         (-2, 1), (-1, 0), (-1, -1), (0, -1), (1, -2),
         (1, -1), (2, -1), (1, 0), (1, 1)])
```

```
39
40
41      coef1 = p1.area
42      p1 = scale(p1, p1_scale_x, p1_scale_y)
43      coef1 = p1.area/coef1
44      p2 = Polygon([(0.5, 0.5), (-0.5, 0.5), (-0.5, -0.5)
            , (0.5, -0.5), (0.5, 0.5)])
45      coef2 = p2.area
46      p2 = scale(p2, p2_scale_x, p2_scale_y)
47      coef2 = p2.area/coef2
48
49      #получаем приближенное значение главного члена в
            оценке средней трудоемкости в определенной точке
             сетки
50      for i in range (step):
51        for j in range (step):
52          n1 = -1 + 2.0/step*i
53          n2 = -1 + 2.0/step*j
54          p_trans = translate(p2, n1, n2)
55          p_inter = p1.intersection(p_trans)
56          ans = ans + sqrt(1.0/p_inter.area)
57
58      #среднее значение по всей сетке
59      ans = (ans / (step*step)) * 0.5 * sqrt(pi) * sqrt(
            coef1) * sqrt(coef2)
60
61      #случай кривой y^2=x^3+Ax+B над конечным полем из p
            >3 элементов
62      # ans = ans * sqrt(2.0)
63
64      f.write("ans = ")
65      f.write(str(p2_scale_x))
```

```
66          f.write("␣")
67          f.write(str(p1_scale_x))
68          f.write(":␣")
69          f.write(str(ans))
70          f.write("\n")
71
72  f.close()
```

Приложение В

Программная реализация алгоритма Годри-Шоста

```
1  ECPoint = collections.namedtuple("ECPoint", ["x", "y"])
2
3  class EC:
4      # Реализация операций в группе точек эллиптической
           кривой
5
6      def __init__(self, a, b, p):
7          # Инициализация эллиптической кривой E_p(a,b) =
               y^2 = x^3 + a*x + b mod p
8          self.a = a
9          self.b = b
10         self.p = p
11         self.n_s = ecc_groups
12         self.zero = ECPoint(0, 0)
13
14     def neg(self, P):
15       # вычисление обратного элемента
16       return ECPoint(P.x, (-P.y) % self.p)
17
```

```
18      def auto4(self, P):
19        # вычисление автоморфизма порядка 4 для элемента
              P
20        return ECPoint((-P.x) % self.p, (self.alpha * P.y
              ) % self.p)
21
22      def auto6(self, P):
23        # вычисление автоморфизма порядка 6 для элемента
              P
24        return ECPoint((self.beta * P.x) % self.p, (-P.y)
               % self.p)
25
26      def sum(self, P1, P2):
27          # вычисление суммы точек P1 и P2
28          if P1 == self.zero:
29            return P2
30          elif P2 == self.zero:
31            return P1
32        elif P1.x == P2.x and (P1.y + P2.y) % self.p ==
              0:
33            return self.zero
34          if P1.x == P2.x and (P1.y != P2.y or P1.y == 0)
                :
35              return self.zero
36          if P1.x == P2.x and P1.y == P2.y:
37            lambda1 = (3 * P1.x**2 + self.a) * inv(2 * P1
                  .y, self.p) % self.p
38          else:
39            lambda1 = (P2.y - P1.y) * inv(P2.x - P1.x,
                  self.p) % self.p
40          x = (lambda1 * lambda1 - P1.x - P2.x) % self.p
41          y = (lambda1 * (P1.x - x) - P1.y) % self.p
```

```
42          return ECPoint(x, y)
43
44      def mul(self, P, n):
45          # Вычисление кратной точки
46          if n < 0:
47            n += self.r
48          Nc = P
49          Q = self.zero
50          while 0 < n:
51              if n & 1 == 1:
52                Q = self.sum(Q, Nc)
53              Nc = self.sum(Nc, Nc)
54              n = n >> 1
55          return Q
56
57 ###
58 ### Реализация алгоритма Годри–Шоста для одномерной
       задачи
59 ###
60
61 def putRepresent(P, x, Seq, Dic):
62   Q = ec.neg(P)
63   # выбор и сохранение представителя класса
       эквивалентности
64   if str(P.x)+str(P.y) < str(Q.x)+str(Q.y):
65     Seq.add(P)
66     Dic[str(P.x)+str(P.y)] = [x, 0]
67   else:
68     Seq.add(Q)
69     Dic[str(Q.x)+str(Q.y)] = [-x, 1]
70
71 def checkResult(Seq1, Seq2, Dic1, Dic2):
```

```
72    S = Seq1.intersection(Seq2)
73    # Пересечение элементов последовательностей Дикого и
          Домашнего множеств
74    if len(S) > 0:
75      ans = S.pop()
76      val1 = Dic1[str(ans.x)+str(ans.y)][0]
77      deg1 = Dic1[str(ans.x)+str(ans.y)][1]
78      val2 = Dic2[str(ans.x)+str(ans.y)][0]
79      deg2 = Dic2[str(ans.x)+str(ans.y)][1]
80      if deg2 == 0:
81        return val1-val2, True
82      else:
83        return val2-val1, True
84    return 0, False
85
86  def GaudrySchost_1D(ec, Q, coef):
87    # Инициализация последовательностей
88    Tseq = Set([])
89    Wseq = Set([])
90    # Вспомогательные структуры данных
91    Tdic = {}
92    Wdic = {}
93    # Количество операций выбора группового элемента
94    steps = 0
95    while True:
96      steps = steps + 1
97      # Вырабатываем элемент Домашнего множества
98      x = random.randint(0, N1)
99      P = ec.mul(ec.P1, x)
100     # Записываем элемент в базу
101     putRepresent(P, x, Tseq, Tdic)
```

```
102       # Проверяем Дикую и Домашнюю последовательности на
              пересечение
103       ans, fin = checkResult(Tseq, Wseq, Tdic, Wdic)
104       # В случае пересечения - выводим ответ
105       if fin:
106         return ans, steps
107       steps = steps + 1
108       # Вырабатываем элемент Дикого множества
109       z = random.randint(-N1*coef/2, N1*coef/2)
110       P = ec.sum(Q, ec.mul(ec.P1, z))
111       # Записываем элемент в базу
112       putRepresent(P, z, Wseq, Wdic)
113       # Проверяем Дикую и Домашнюю последовательности на
              пересечение
114       ans, fin = checkResult(Tseq, Wseq, Tdic, Wdic)
115       # В случае пересечения - выводим ответ
116       if fin:
117         return ans, steps
118
119 ###
120 ### Реализация алгоритма Годри-Шоста для двумерной
        задачи
121 ###
122
123 def phi_ord2(P, a, b, deg):
124     # вычисление автоморфизма порядка 2 для кривой y^2=x
          ^3+ax+b
125     deg = deg % 2
126     for i in range(1, deg+1):
127       P, a, b = ec.neg(P), b, a
128     return P, a, b
129
```

```
130 def phi_ord2_any(P, a, b, deg):
131   # вычисление автоморфизма порядка 2 для кривой y^2=x
        ^3+ax+b
132   deg = deg % 2
133   for i in range(1, deg+1):
134     P, a, b = ec.neg(P), -a, -b
135   return P, a, b
136
137 def phi_ord4(P, a, b, deg):
138   # вычисление автоморфизма порядка 4 для кривой y^2=x
        ^3+ax
139   deg = deg % 4
140   for i in range(1, deg+1):
141     P, a, b = ec.auto4(P), -b, a
142   return P, a, b
143
144 def phi_ord6(P, a, b, deg):
145   # вычисление автоморфизма порядка 6 для кривой y^2=x
        ^3+b
146   deg = deg % 6
147   for i in range(1, deg+1):
148     P, a, b = ec.auto6(P), -b, a+b
149   return P, a, b
150
151 def putRepresent2D(ec, P, x1, x2, Seq, Dic):
152   Q, a1, a2, deg = P, x1, x2, 0
153   # выбор и сохранение представителя класса
        эквивалентности
154   for i in range (1, ec.ord):
155     P, x1, x2 = ec.phi(P, x1, x2, 1)
156     if str(P.x)+str(P.y) < str(Q.x)+str(Q.y):
157       Q, a1, a2, deg = P, x1, x2, i
```

```
158     Seq.add(Q)
159     Dic[str(Q.x)+str(Q.y)] = [a1, a2, deg]
160
161 def checkResult2D(ec, Seq1, Seq2, Dic1, Dic2):
162     # Пересечение элементов последовательностей Дикого и
          Домашнего множеств
163     S = Seq1.intersection(Seq2)
164     if len(S) > 0:
165         ans = S.pop()
166         x1, y1 = Dic1[str(ans.x)+str(ans.y)][0], Dic1[str(
              ans.x)+str(ans.y)][1]
167         d1 = Dic1[str(ans.x)+str(ans.y)][2]
168         x2, y2 = Dic2[str(ans.x)+str(ans.y)][0], Dic2[str(
              ans.x)+str(ans.y)][1]
169         d2 = Dic2[str(ans.x)+str(ans.y)][2]
170         Q1, t1, y1 = ec.phi(ans, x1, y1, ec.ord-d2)
171         Q2, t2, y2 = ec.phi(ans, x2, y2, ec.ord-d2)
172         return t1-t2, y1-y2, True
173     return 0, 0, False
174
175 def GaudrySchost_2D(ec, Q, coef):
176     # Инициализация последовательностей
177     Tseq = Set([])
178     Wseq = Set([])
179     # Вспомогательные структуры данных
180     Tdic = {}
181     Wdic = {}
182     # Количество операций выбора группового элемента
183     steps = 0
184     while True:
185         steps = steps + 1
186         # Вырабатываем элемент Домашнего множества
```

```
187     if ec.ord == 6:
188       x1 = random.randint(0, N1)
189       x2 = random.randint(0, N1)
190     else:
191       x1 = random.randint(-N1, N1)
192       x2 = random.randint(-N1, N1)
193     P = ec.sum(ec.mul(ec.P1, x1), ec.mul(ec.P2, x2))
194     # Записываем элемент в базу
195     putRepresent2D(ec, P, x1, x2, Tseq, Tdic)
196     # Проверяем Дикую и Домашнюю последовательности на
          пересечение
197     ans1, ans2, fin = checkResult2D(ec, Tseq, Wseq,
          Tdic, Wdic)
198     # В случае пересечения - выводим ответ
199     if fin:
200       return ans1, ans2, steps
201     steps = steps + 1
202     # Вырабатываем элемент Дикого множества
203     z1 = random.randint(-N1*coef/2, N1*coef/2)
204     z2 = random.randint(-N1*coef/2, N1*coef/2)
205     P = ec.sum(Q, ec.sum(ec.mul(ec.P1, z1), ec.mul(ec.
          P2, z2)))
206     # Записываем элемент в базу
207     putRepresent2D(ec, P, z1, z2, Wseq, Wdic)
208     # Проверяем Дикую и Домашнюю последовательности на
          пересечение
209     ans1, ans2, fin = checkResult2D(ec, Tseq, Wseq,
          Tdic, Wdic)
210     # В случае пересечения - выводим ответ
211     if fin:
212       return ans1, ans2, steps
```

Список литературы

[1] Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. — Москва : МЦНМО, 2003.

[2] Кнут Д.Э. Искусство программирования. Том 3. Сортировка и поиск. — 2-е изд. — Москва : Вильямс, 2007. — Т. 3.

[3] Коблиц Н. Курс теории чисел и криптографии. — Москва : Научное издательство ТВП, 2001.

[4] Николаев М.В. О сложности задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием // Прикладная дискретная математика. — 2015. — № 2. — С. 97–102.

[5] Николаев М.В., Матюхин Д.В. О сложности двумерной задачи дискретного логарифмирования в конечной циклической группе с эффективным автоморфизмом порядка 6 // Дискретная математика. — 2013. — Т. 25, № 4. — С. 54–65.

[6] Adleman L.M., DeMarrais J. A subexponential algorithm for discrete logarithms over all finite fields // Mathematics of Computation. — 1993. — no. 61. — P. 1–15.

[7] BitcoinWiki. Secp256k1. — [Online]. Режим доступа: `https://en.bitcoin.it/wiki/Secp256k1`.

[8] Blackburn S. R., Scott S. The discrete logarithm problem for exponents of bounded height // LMS Journal of Computation and Mathematics. — 2014. — no. 17. — P. 148–156.

[9] Blake I. F., Seroussi G., Smart N. P. Elliptic Curves in Cryptography. — New York, NY, USA : Cambridge University Press, 1999.

[10] Boneh D., Goh E. J., Nissim K. Evaluating 2-DNF formulas on ciphertexts // Lecture Notes in Computer Science. — 2005. — Vol. 3378. — P. 325–341.

[11] Bos J.W., Costello C., Miele A. Elliptic and Hyperelliptic Curves: A Practical Security Analysis // Public-Key Cryptography – PKC 2014: 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, March 26-28, 2014. Proceedings / Ed. by Hugo Krawczyk. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2014. — P. 203–220.

[12] Certicom Research. Sec 2: Recommended elliptic curve domain parameters ver. 1.0. — 2000. — Режим доступа: http://www.secg.org/SEC2-Ver-1.0.pdf.

[13] Certicom Research. Sec 2: Recommended elliptic curve domain parameters ver. 2.0. — 2010. — Режим доступа: http://www.secg.org/sec2-v2.pdf.

[14] Cheon J. H. Security analysis of the strong Diffie-Hellman problem // Lecture Notes in Computer Science. — 2006. — Vol. 4004. — P. 1–11.

[15] Costello C., Hisil H., Smith B. Faster Compact Diffie–Hellman: Endomorphisms on the x-line // Advances in Cryptology – EUROCRYPT 2014: 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings / Ed. by P. Q. Nguyen, E. Oswald. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2014. — P. 183–200.

[16] Csirik A. An exposition of the SEA algorithm. — 2000. — Режим доступа: http://www.csirik.net/sch-survey.pdf.

[17] Diffie W., Hellman M. New directions in cryptography // Transactions on Information Theory. — 1976. — Vol. 22, no. 6. — P. 644–654.

[18] Doche C., Icart T., Kohel D.R. Efficient scalar multiplication by isogeny decompositions // International Workshop on Public Key Cryptography. — 2005. — P. 191–206.

[19] Duursma I. M., Gaudry P., Morain F. Speeding up the discrete log computation on curves with automorphisms // Lecture Notes in Computer Science. — 1999. — Vol. 1716. — P. 103–121.

[20] Efficient implementation of Schoof's algorithm / T. Izu, J. Kogure, M. Noro, K. Yokoyama // Lecture Notes in Computer Science. — 1998. — Vol. 1514. — P. 66–79.

[21] An Elementary Introduction to Hyperelliptic Curves / A. Menezes, University of Waterloo. Dept. of Combinatorics, Optimization и др. Research report (University of Waterloo. Faculty of Mathematics). — Faculty of Mathematics, University of Waterloo, 1996. — Режим доступа: http://cacr.uwaterloo.ca/~ajmeneze/publications/hyperelliptic.pdf.

[22] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms // Transactions on Information Theory. — 1985. — Vol. 31, no. 4.

[23] Elkies N. D. Elliptic and modular curves over finite fields and related computational issues // Computational Perspectives in Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin. — 1998. — P. 21–76.

[24] EMVCo. EMV ECC Key Establishment Protocols. — 2012. — Draft 1st Edition. Режим доступа: http://www.emvco.com/download_agreement.aspx?id=760.

[25] Galbraith S. D., Holmes M. A non-uniform birthday problem with applications to discrete logarithms // Discrete Applied Mathematics. — 2012. — Vol. 160, no. 10-11. — P. 1547–1560.

[26] Galbraith S. D., Lin X., Scott M. Endomorphisms for faster elliptic curve cryptography on a large class of curves // Journal of Cryptology. — 2011. — Vol. 24, no. 3. — P. 446–469.

[27] Galbraith S. D., Ruprai R. S. An improvement to the Gaudry-Schost algorithm for multidimensional discrete logarithm problems // Lecture Notes in Computer Science. — 2009. — Vol. 5921, no. 10-11. — P. 368–382.

[28] Galbraith S. D., Ruprai R. S. Using equivalence classes to accelerate solving the discrete logarithm problem in a short interval // Lecture Notes in Computer Science. — 2010. — Vol. 6056. — P. 368–383.

[29] Gallant R., Lambert R., Vanstone S. Faster point multiplication on elliptic curves with efficient endomorphisms // Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology. — CRYPTO '01. — London, UK : Springer-Verlag, 2001. — P. 190–200.

[30] Gaudry P., Schost E. A low-memory parallel version of Matsuo, Chao and Tsujii's algorithm // Lecture Notes in Computer Science. — 2004. — Vol. 3076. — P. 208–222.

[31] Gennaro R. An improved pseudo-random generator based on discrete log // Lecture Notes in Computer Science. — 2000. — Vol. 1880. — P. 469–481.

[32] Gillies S.C. Shapely. — Режим доступа: `https://pypi.python.org/pypi/Shapely`.

[33] GLV/GLS Decomposition, Power Analysis, and Attacks on ECDSA Signatures with Single-Bit Nonce Bias / D. F. Aranha, P. Fouque,

B. Gérard et al. // Advances in Cryptology – ASIACRYPT 2014: 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I / Ed. by P. Sarkar, T. Iwata. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2014. — P. 262–281.

[34] Gopalakrishnan K., Theriault N., Yao C. Z. Solving discrete logarithms from partial knowledge of the key // Lecture Notes in Computer Science. — 2007. — Vol. 4859. — P. 224–263.

[35] Hankerson D., Menezes A. J., Vanstone S. Guide to Elliptic Curve Cryptography. — Secaucus, NJ, USA : Springer-Verlag New York, Inc., 2003.

[36] High-Performance Scalar Multiplication Using 8-Dimensional GLV/GLS Decomposition / J. W. Bos, C. Costello, H. Hisil, K. Lauter // Cryptographic Hardware and Embedded Systems - CHES 2013: 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings / Ed. by G. Bertoni, J.-S. Coron. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2013. — P. 331–348.

[37] Jao D., Yoshida K. Boneh-Boyen signatures and the strong Diffie-Hellman problem // Lecture Notes in Computer Science. — 2009. — Vol. 5671. — P. 1–16.

[38] Kerry C. F., Gallagher P. D. FIPS PUB 186-4 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION Digital Signature Standard (DSS). — 2013. — Режим доступа: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

[39] Koblitz N. Hyperelliptic cryptosystems // Journal of Cryptology. — 1989. — Vol. 1, no. 3. — P. 139–150.

[40] Koblitz N. CM curves with good cryptographic properties // CRYPTO 1991: Advances in Cryptology - CRYPTO '91. — 1992. — P. 279–287.

[41] Lenstra Jr H. W., Pila J., Pomerance C. A hyperelliptic smoothness test, II // Proceedings of the London Mathematical Society. — 2002. — Vol. 84, no. 1. — P. 105–146.

[42] Lim C. H., Lee P. J. A key recovery attack on discrete log-based schemes using a prime order subgroup // Lecture Notes in Computer Science. — 1997. — Vol. 1294. — P. 249–263.

[43] Liu W. Improved algorithms for the 2-dimensional discrete logarithm problem with equivalence classes : Msc thesis / W. Liu ; University of Auckland. — 2010. — Режим доступа: http://www.math.auckland.ac.nz/~sgal018/Wei-Liu-MSc.pdf.

[44] Matsuo K., Chao J., Tsujii S. An improved Baby Step Giant Step algorithm for point counting of hyperelliptic curves over finite fields // Proceedings of the 5th International Symposium on Algorithmic Number Theory. — ANTS-V. — London, UK, UK : Springer-Verlag, 2002. — P. 461–474.

[45] Milne J. S. Jacobian Varieties // Arithmetic Geometry / Ed. by G. Cornell, J. H. Silverman. — New York, NY : Springer New York, 1986. — P. 167–212.

[46] Montgomery P. L. Speeding the Pollard and elliptic curve methods of factorization // Mathematics of Computation. — 1987. — Vol. 48, no. 177. — P. 243–264.

[47] Morain F. Calcul du nombre de points sur une courbe elliptique dans un cops fini: aspects algorithmiques // Journal de theorie des nombres de Bordeaux. — 1995. — Vol. 7, no. 1. — P. 255–282.

[48] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. — 2008. — Режим доступа: http://bitcoin.org/bitcoin.pdf.

[49] Nikolaev M. V. On the complexity of two-dimensional discrete logarithm problem in a finite cyclic group with efficient automorphism // Математические вопросы криптографии. — 2015. — Т. 6, № 2. — С. 45–57.

[50] Oorschot P. C. van, Wiener M. J. On Diffie-Hellman key agreement with short exponents // Lecture Notes in Computer Science. — 1996. — Vol. 1070. — P. 332–343.

[51] Oorschot P. C. van, Wiener M. J. Parallel collision search with cryptanalytic applications // Journal of Cryptology. — 1999. — Vol. 12, no. 1. — P. 1–28.

[52] Patel S., Sundaram G. S. An efficient discrete log pseudo random generator // Advances in Cryptology — CRYPTO '98: 18th Annual International Cryptology Conference Santa Barbara, California, USA August 23–27, 1998 Proceedings / Ed. by H. Krawczyk. — Berlin, Heidelberg : Springer Berlin Heidelberg, 1998. — P. 304–317.

[53] Pollard J. M. Monte Carlo methods for index computation (mod p) // Mathematics of Computation. — 1978. — Vol. 32, no. 143. — P. 918–924.

[54] Pollard J. M. Kangaroos, monopoly and discrete logarithms // Journal of Cryptology. — 2000. — no. 13. — P. 437–447.

[55] Schoof R. Elliptic curves over finite fields and the computation of square roots mod p // Mathematics of Computation. — 1985. — Vol. 44. — P. 483–494.

[56] Shanks D. The infrastructure of a real quadratic field and its applications // Proceedings of the Number Theory Conference. — 1972. — P. 217–224.

[57] Software Implementation of the NIST Elliptic Curves Over Prime Fields / M. Brown, D. Hankerson, J. López, A. Menezes // Topics in Cryptology — CT-RSA 2001: The Cryptographers' Track at RSA Conference 2001 San Francisco, CA, USA, April 8–12, 2001 Proceedings / Ed. by David Naccache. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2001. — P. 250–265.

[58] Stein W. Sagemath. — Режим доступа: `http://www.sagemath.org/`.

[59] Stichtenoth H. Algebraic Function Fields and Codes. — 2nd edition. — Springer Publishing Company, Incorporated, 2008.

[60] Teske E. Speeding up Pollard's rho method for computing discrete logarithms // Technical Report No. TI01/98, Technische Hochschule Darmstadt. — 1998.

[61] The ECC Brainpool. Standard curves and curve generation v. 1.0. — 2005. — Режим доступа: http://www.ecc-brainpool.org/download/Domain-parameters.pdf.

[62] Trading inversions for multiplications in elliptic curve cryptography / M. Ciet, M. Joye, K. Lauter, P. L. Montgomery // Des. Codes Cryptography. — 2006. — Vol. 39, no. 2. — P. 189–206.

[63] Two is the fastest prime: lambda coordinates for binary elliptic curves / T. Oliveira, J. López, D. F. Aranha, F. Rodríguez-Henríquez // Journal of Cryptographic Engineering. — 2013. — Vol. 4. — P. 3–17.

[64] Wiener M. J., Zuccherato R. J. Faster attacks on elliptic curve cryptosystems // Lecture Notes in Computer Science. — 1999. — Vol. 1556. — P. 190–200.