МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Сравнительный анализ алгоритмов вычисления дискретных логарифмов

АВТОРЕФЕРАТ
дипломной работы

студентки 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Кайдышевой Дарьи Сергеевны

Научный руководитель
д. ф.-м. н., профессор _____ В. А. Молчанов
19.01.2026 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
19.01.2026 г.

Саратов 2026

ВВЕДЕНИЕ

Как известно, существуют два типа шифрования на основе ключа: симметричное (один ключ для шифрования и дешифрования) и ассиметричное (два ключа – открытый и закрытый). Открытый ключ находится в свободном доступе и служит для шифрования данных. Расшифровать сообщение может только обладатель закрытого ключа. Но стоит заметить, что ключи в случае ассиметричного шифрования обязательно связаны математически. Предположение о существовании односторонних функций лежит в основе этой связи [1].

Если для любого x справедливо соотношение $f(g(x)) = x$, то функция $g(x)$ называется обратной функции $f(x)$ и обозначается как $f^{-1}(x)$. Сложность алгоритма вычисления функции $f(x)$ по значению x назовем сложностью функции $f(x)$. Функция $f(x)$ называется односторонней, если ее сложность существенно меньше сложности обратной ей функции $g(x) = f^{-1}(x)$ [1].

Но в настоящее время не существует функций, односторонность которых доказана.

К числу потенциальных односторонних функций относят дискретное экспоненцирование. Хотя труднообратимость этой функции формально не доказана, многочисленные исследования в данной сфере до сих пор не выявили эффективного алгоритма, способного выполнить обратное преобразование. Попытка обратить операцию дискретного возведения в степень приводит к задаче вычисления дискретного логарифма (Discrete Logarithm Problem – DLP).

Большая часть современных криптографических систем строится на вычислительной сложности математических задач – в частности, на задаче дискретного логарифмирования. К примерам таких криптосистем с открытым ключом относятся: RSA, DSA (Digital Signature Algorithm – алгоритм цифровой подписи), протокол Диффи-Хэллмана, схема Эль-Гамаля, схема Шнорра, ГОСТ Р 34.10-2012, протокол Мэсси-Омуры и ECDSA (DSA на эллиптических кривых).

Чтобы взломать большинство таких систем или подделать цифровую подпись, необходимо решить задачу вычисления дискретного логарифма. Поэтому исследование методов решения этой задачи, оценка их эффективности и практическая реализация имеют важное значение для обеспечения безопасности информационных систем, защиты их от атак.

Целью данной работы является исследование и сравнительный анализ алгоритмов вычисления дискретных логарифмов путем решения следующих задач:

1) изучение математических основ задачи дискретного логарифмирования;

2) изучение и программная реализация алгоритмов DLP: Гельфонда-Шенкса, ρ-метода Полларда, λ-метода Полларда, Сильвера-Полига-Хеллмана и индекс-метода;

3) изучение и программная реализация алгоритмов ECDLP (Elliptic Curve Discrete Logarithm Problem): Гельфонда-Шенкса, ρ-метода Полларда, полного перебора;

4) разработка веб-приложения на базе Python/Flask;

5) подготовка наборов входных данных, удовлетворяющих требованиям алгоритмов и проведение тестирования;

6) проведение экспериментального исследования временной и пространственной сложностей разных методов;

7) выполнение сравнительного анализа полученных результатов;

8) формулирование выводов по проделанной работе.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 15 приложений. Общий объем работы – 98 страниц, из них 55 страниц – основное содержание, включая 24 рисунка и 5 таблиц, список использованных источников из 23 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе «Теоретические основы задачи дискретного логарифмирования» приводятся необходимые теоретические сведения, связанные с арифметикой в конечных полях, циклическими группами, а также основами эллиптической криптографии. Эти знания используются при описании алгоритмов дискретного логарифмирования, представленных в последующих главах, и при реализации программного комплекса – веб-приложения.

В подразделе 1.1 «Конечные циклические группы» вводится понятие дискретного логарифма, описывается сложность задачи DLP и приводятся типы циклических групп, выделяемых в прикладной криптографии.

В подразделе 1.2 «Эллиптические кривые» вводятся теоретические основы эллиптических кривых, определяется задача дискретного логарифмирования на эллиптической кривой и подчеркивается ключевое отличие алгоритмов ECDLP от DLP.

Во второй главе «Алгоритмы дискретного логарифмирования» приведен разбор упомянутых ранее алгоритмов DLP и ECDLP. Описанные методы составляют основу последующей программной реализации и сравнительного анализа.

В подразделе 2.1 «Алгоритмы DLP» представлено описание пяти методов для работы в произвольной конечной циклической группе и конечном простом поле. Каждый из пунктов содержит шаги алгоритма; теоретическое обоснование корректности работы алгоритма; временную и пространственную оценки сложностей:

- пункт 2.1.1 «Метод Гельфонда-Шенкса»,
- пункт 2.1.2 «ρ-метод Полларда»,
- пункт 2.1.3 «λ-метод Полларда»,
- пункт 2.1.4 «Метод Сильвера-Полига-Хэллмана»,
- пункт 2.1.5 «Индекс-метод».

В подразделе 2.2 «Алгоритмы ECDLP» описываются алгоритмы общего назначения для решения задачи дискретного логарифмирования в группе точек эллиптической кривой:

- пункт 2.2.1 «Метод Гельфонда-Шенкса»,
- пункт 2.2.2 «ρ-метод Полларда»,
- пункт 2.2.3 «Полный перебор».

В третьей главе «Реализация программного комплекса» рассматривается практическая реализация программного комплекса, предназначенного для исследования и сравнения алгоритмов решения задачи дискретного логарифмирования. Основное внимание уделяется архитектуре системы, выбору технологического стека, непосредственной реализации вычислительных методов и организации их взаимодействия в единой программной среде.

Подраздел 3.1 «Стек технологий и архитектура» описывает выбор инструментов разработки (язык и библиотеки) и общую структурную организацию проекта. Также в подразделе рассматривается интерфейс разработанного веб-приложения, основная страница которого показана на рисунке 3.

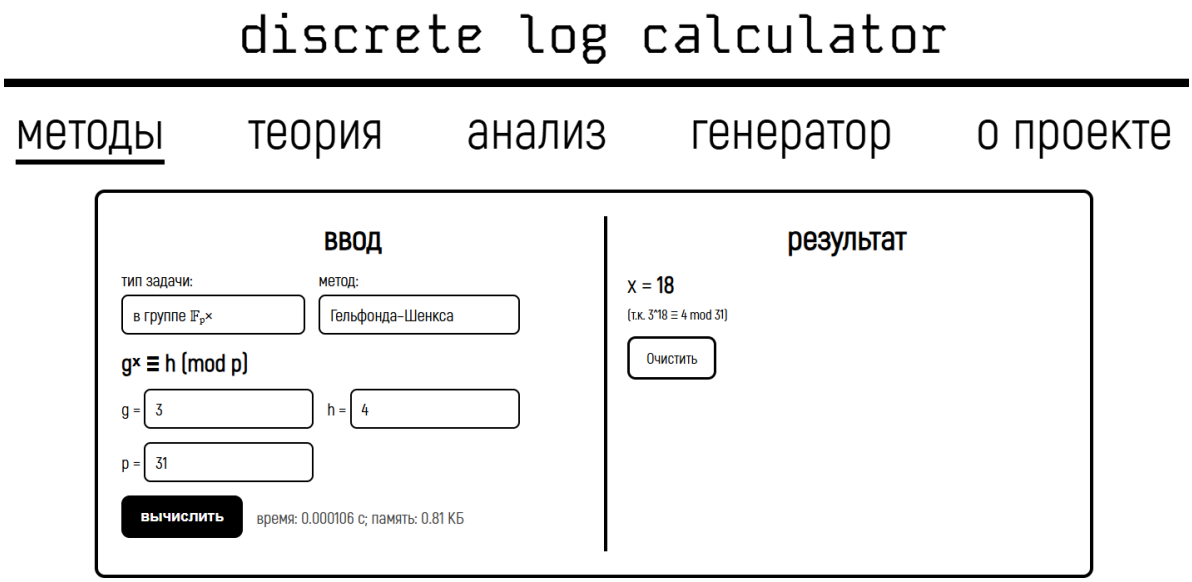

Рисунок 3 – Основная страница сайта, калькулятор DLP/ECDLP

В подразделе 3.2 «Реализация алгоритмов DLP» рассматриваются ключевые аспекты, связанные с разработкой всех пяти алгоритмов,

рассмотренных в разделе 2.1: используемые встроенные функции, оптимизации и улучшения.

В подразделе 3.3 «Реализация алгоритмов ECDLP» аналогичным образом описываются детали их программной реализации. Для этого сначала реализуется базовый набор функций, осуществляющих базовые операции над точками эллиптических кривых.

В разделе 4 «Сравнительный анализ алгоритмов вычисления дискретных логарифмов» демонстрируется пример работы комплекса, а также сравнительный анализ полученных результатов на подготовленных данных.

В подразделе 4.1 «Пример работы комплекса» описываются возможности всех разделов реализованного веб-приложения. Генерация примитивного корня показана на рисунке 9.

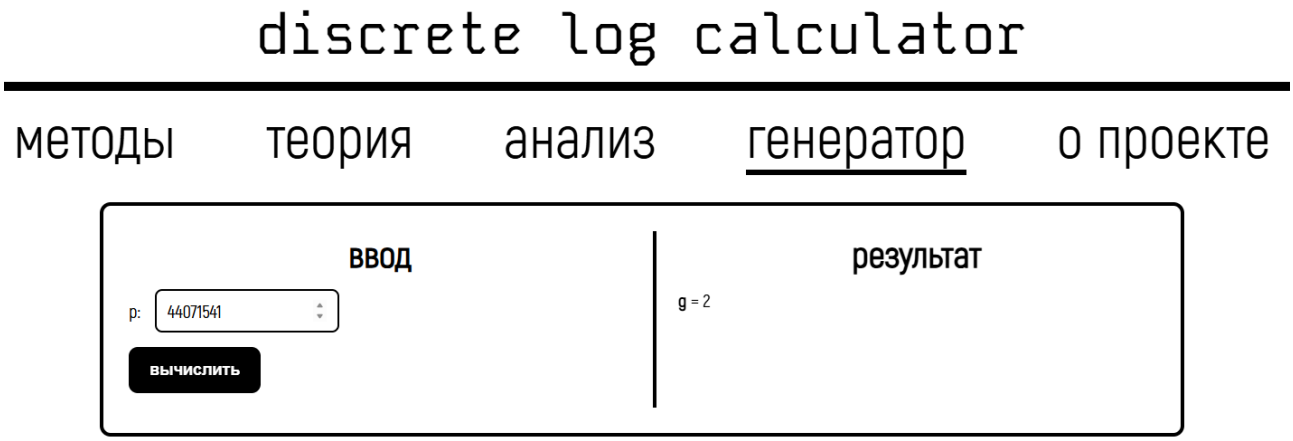

Рисунок 9 – Генерация примитивного корня

Пример работы λ-метода Полларда (раздел «Методы») демонстрируется на рисунке 10. Фиксируются время работы и затрачиваемая память. Эти характеристики необходимы для последующего сравнительного анализа.

Сокращения, используемые в интерфейсе веб-приложения и графиках при сопоставлении результатов, показаны в таблице 1.

Раздел анализ – основной инструмент для сопоставления различных алгоритмов, показан на рисунке 12 (тип задачи – в мультипликативной группе конечного простого поля).

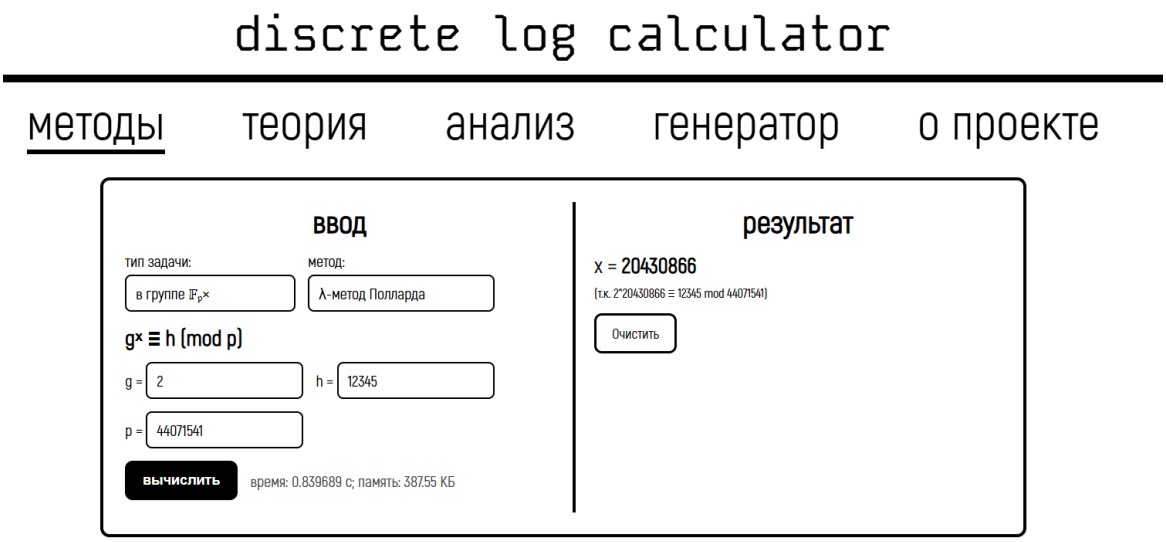

Рисунок 10 – Пример работы λ-метода Полларда

Таблица 1 – Сокращения названий алгоритмов для графиков

DLP	ECDLP
BSGS – метод Гельфонда-Шенкса	BSGS – метод Гельфонда-Шенкса
ρ, rho – ρ-метод Полларда	ρ, rho – ρ-метод Полларда
λ, lambda – λ-метод Полларда	BF, Brute – полный перебор
SPH – метод Сильвера-Полига-Хеллмана	
index/Index – Индекс-метод	

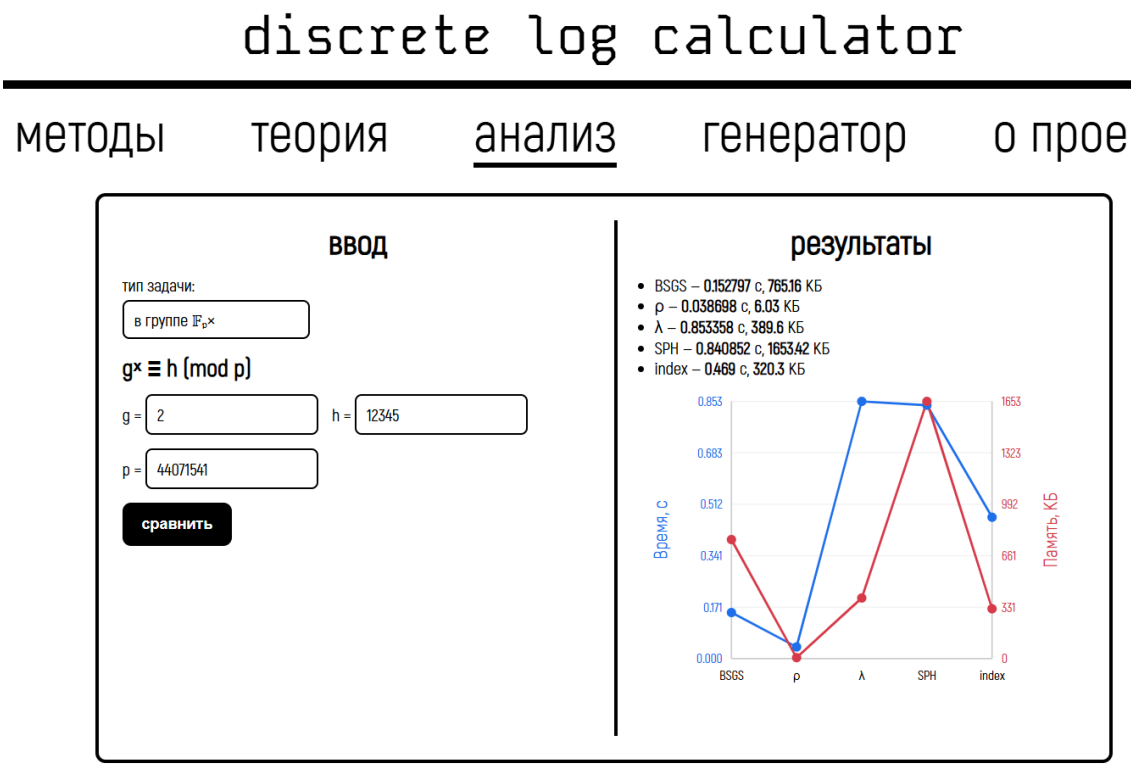

Рисунок 12 – Построение графиков для алгоритмов в группе $\mathbb{F}_p^\times$

Работа раздела «Методы» показана на рисунке 14 на примере алгоритма больших и малых шагов в группе точек эллиптической кривой:

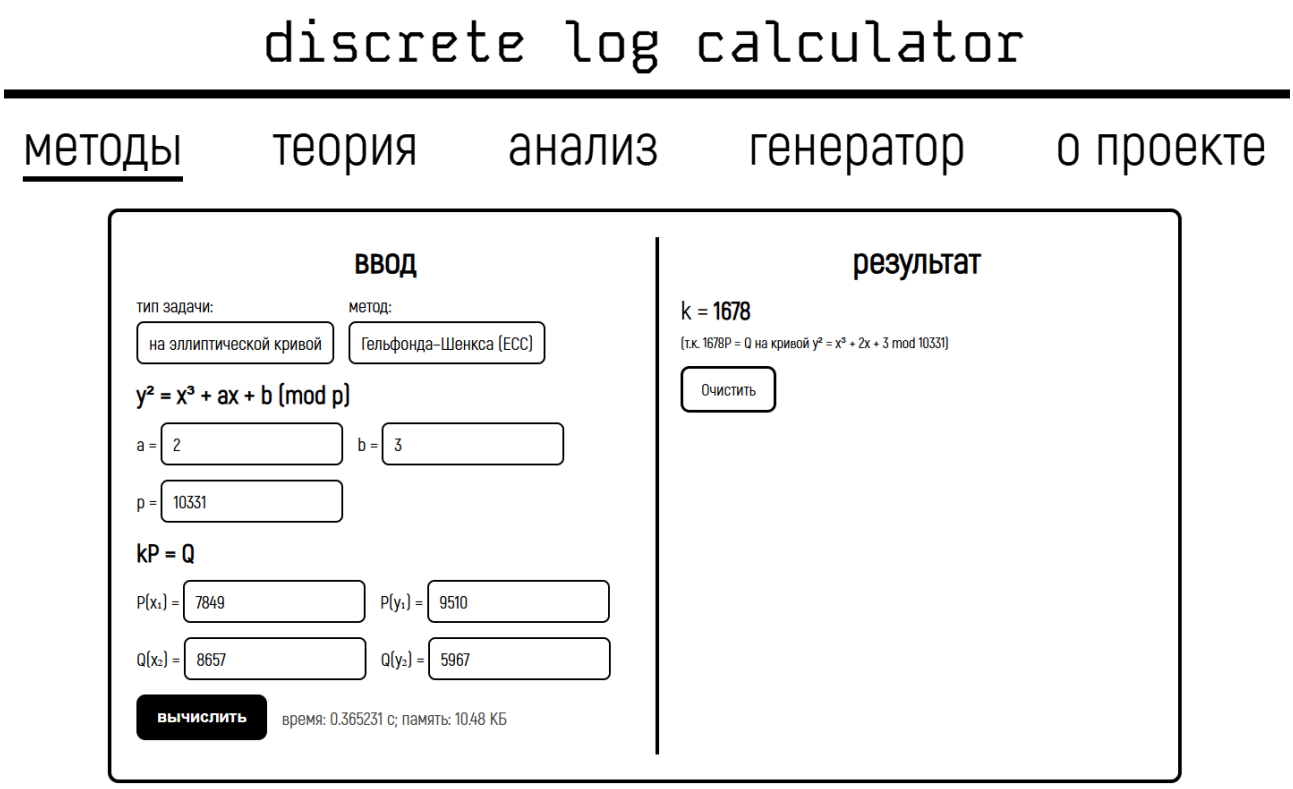

Рисунок 14 – Пример работы алгоритма Гельфонда-Шенкса в группе точек эллиптической кривой

Анализ алгоритмов ECDLP при общих входных параметрах показан на рисунке 16.

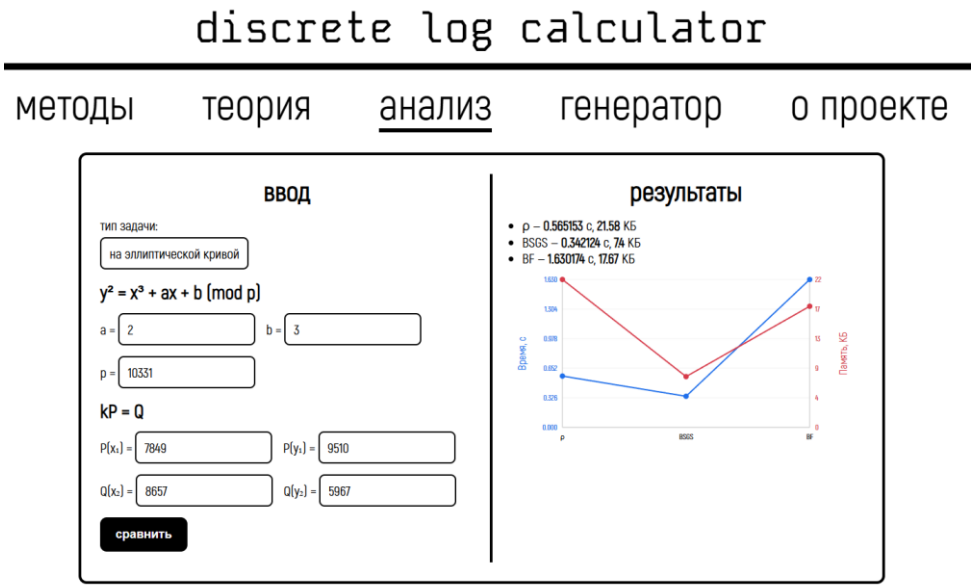

Рисунок 16 – Построение графиков для алгоритмов на эллиптической кривой

В подразделе 4.2 «Сравнительный анализ алгоритмов» представлен подробный сравнительный анализ реализованных алгоритмов вычисления дискретного логарифма как в мультипликативных группах конечных простых полей, так и в группах точек эллиптических кривых.

В таблице 2 демонстрируются результаты сравнения алгоритмов вычисления дискретного логарифма в группе $\mathbb{F}_p^\times$ по параметру потребления памяти.

Таблица 2 – Потребление памяти алгоритмами DLP в группе $\mathbb{F}_p^\times$

k	$p \sim 2^k$	g	h	Методы (память в килобайтах)				
				BSGS	ρ	λ	***SPH***	***Index***
10	127	3	85	0.9	5.2	0.9	0.9	8.6
15	31873	11	30735	18.7	19.6	12.5	5.3	38.2
20	1031549	2	371915	91.5	5.6	52.5	19.4	97.6
25	26019533	2	13540427	454.8	6.6	387.6	379.2	299.2
30	710636357	2	620074028	3213.2	5.6	1547.8	89.2	956.8
35	32666571601	7	4378508791	26311.5	27.5	13352.1	212788.5	3412.6
40	416845646249	3	232147377643	61241.8	8.2	31652.2	1740526.7	4634.9
45	29678785401971	2	27664452845457	509640.5	8.9	433189.0	1539.6	35777.4
50	1352965139617621	2	1276366349815327	3645548.4	5.1	1899566.1	1777.82	71529.5

По данным из таблицы 2 были построены логарифмические графики:

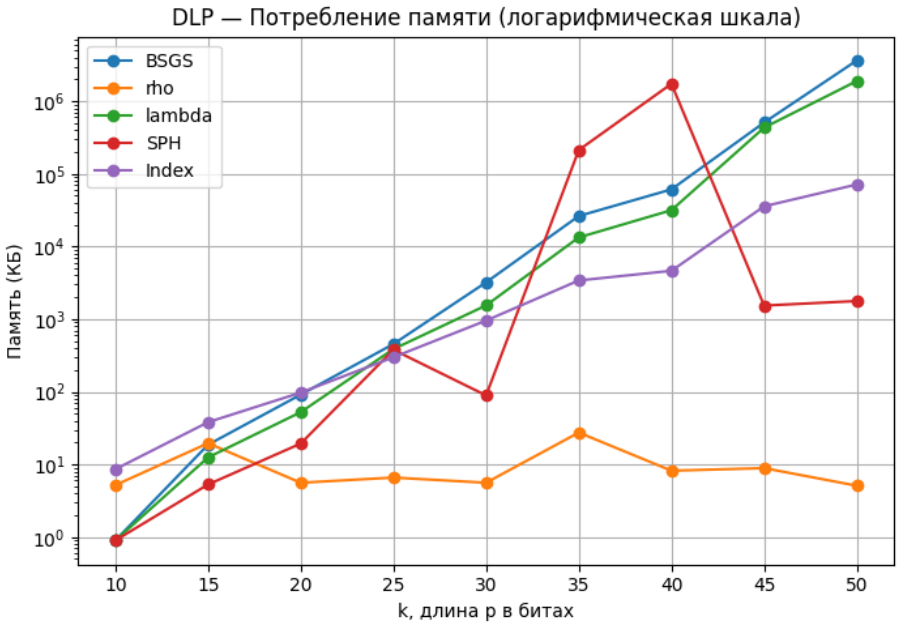

Рисунок 18 – Графики потребления памяти (логарифмическая шкала) для алгоритмов DLP

Аналогично по данным из таблицы 3 были построены графики для сравнения алгоритмов вычисления дискретного логарифма в группе $\mathbb{F}_p^\times$ по времени выполнения (рисунок 20).

Таблица 3 – Время выполнения алгоритмов DLP в группе $\mathbb{F}_p^\times$

k	$p \sim 2^k$	g	h	Методы (время в секундах)				
				$BSGS$	ρ	λ	SPH	$Index$
10	127	3	85	0.000	0.001	0.000	0.000	0.002
15	31873	11	30735	0.002	0.006	0.016	0.003	0.035
20	1031549	2	371915	0.014	0.0422	0.157	0.013	0.071
25	26019533	2	13540427	0.091	0.097	0.682	0.153	0.36
30	710636357	2	620074028	0.581	0.303	0.373	0.050	1.197
35	32666571601	7	4378508791	10.26	2.34	15.65	216.05	13.09
40	416845646249	3	232147377643	37.48	7.13	19.08	1877.60	12.58
45	29678785401971	2	27664452845457	343.99	184.74	372.04	1.92	131.22
50	1352965139617621	2	1276366349815327	2507.18	1713.86	786.57	3.89	271.65

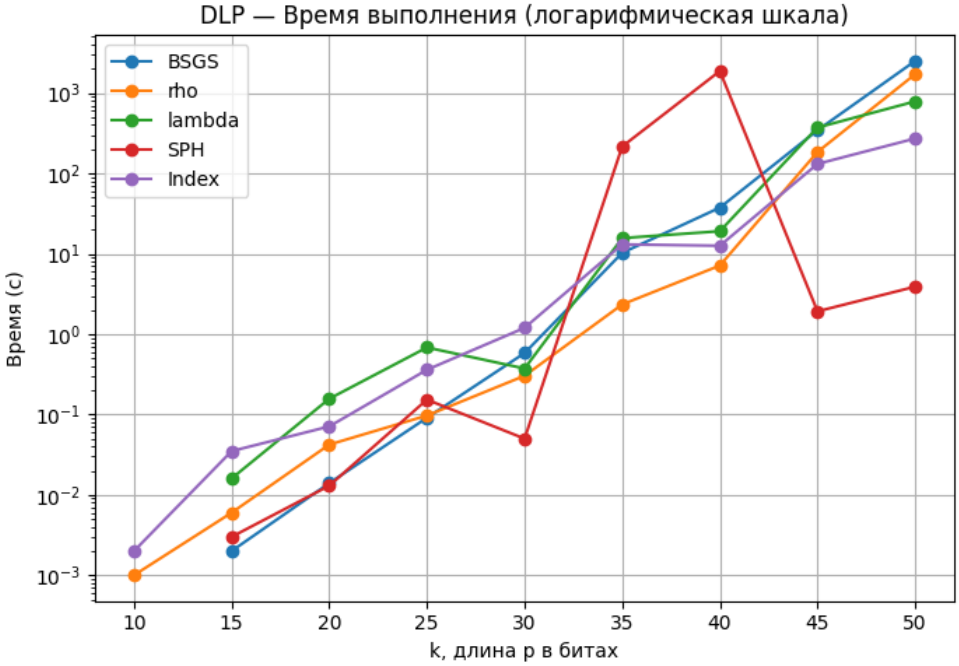

Рисунок 20 – Графики времени выполнения (логарифмическая шкала) для алгоритмов DLP

В таблице 4 представлены результаты сравнения алгоритмов ECDLP по параметру потребления памяти. По данным этой таблицы были построены графики в логарифмическом масштабе (рисунок 22).

Таблица 4 – Потребление памяти алгоритмами ECDLP на эллиптической кривой

k	$p \sim 2^k$	a	b	P	Q	Методы (память в килобайтах)		
						$BSGS$	ρ	$Brute\ Force$
5	11	7	8	(1,7)	(7,9)	0.25	12.43	0.09
10	757	12	87	(223,754)	(415,399)	2.5	28.2	0.4
13	4111	2987	3999	(2808, 4106)	(3243,1053)	10.6	30.1	10.2
15	11069	156	3676	(102,171)	(7044, 7603)	17.7	4.78	18.5
17	55763	23441	14683	(2946,3874)	(38459,25604)	30.27	10010.8	0.0
20	233141	199413	183956	(16186,59421)	(106043,165242)	14.0	42.0	19.0

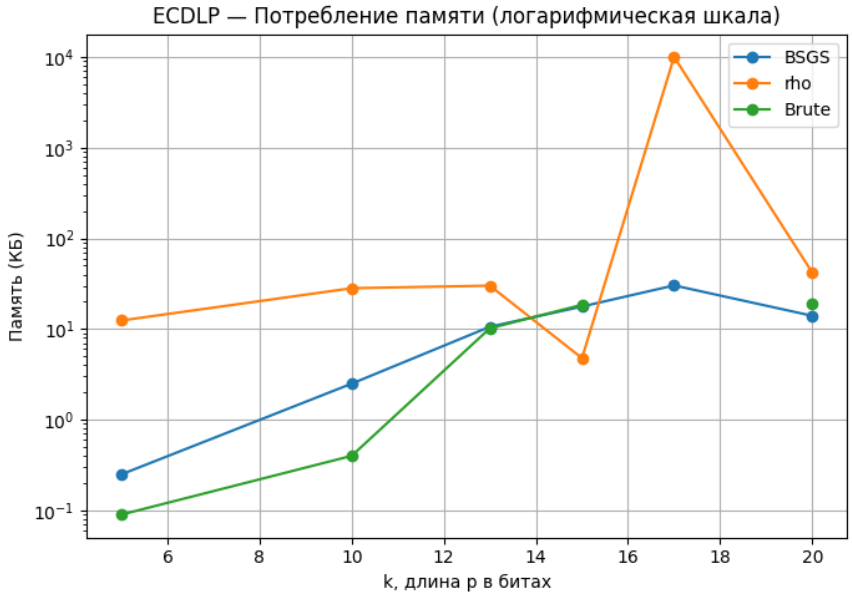

Рисунок 22 – Графики потребления памяти (логарифмическая шкала) для алгоритмов ECDLP

Также по данным из таблицы 5 были построены графики, иллюстрирующие время выполнения алгоритмов ECDLP (рисунок 24).

Таблица 5 – Время выполнения алгоритмов ECDLP на эллиптической кривой

k	$p \sim 2^k$	a	b	P	Q	Методы (время в секундах)		
						BSGS	***ρ***	***Brute Force***
5	11	7	8	(1,7)	(7,9)	0.0001	0.016	0.0003
10	757	12	87	(223,754)	(415,399)	0.03	0.21	0.37
13	4111	2987	3999	(2808, 4106)	(3243,1053)	0.2	0.632	3.32
15	11069	156	3676	(102,171)	(7044, 7603)	0.647	0.634	6.37
17	55763	23441	14683	(2946,3874)	(38459,25604)	7.5	12.1	106.86
20	233141	199413	183956	(16186,59421)	(106043,165242)	1.10	2.35	8.35

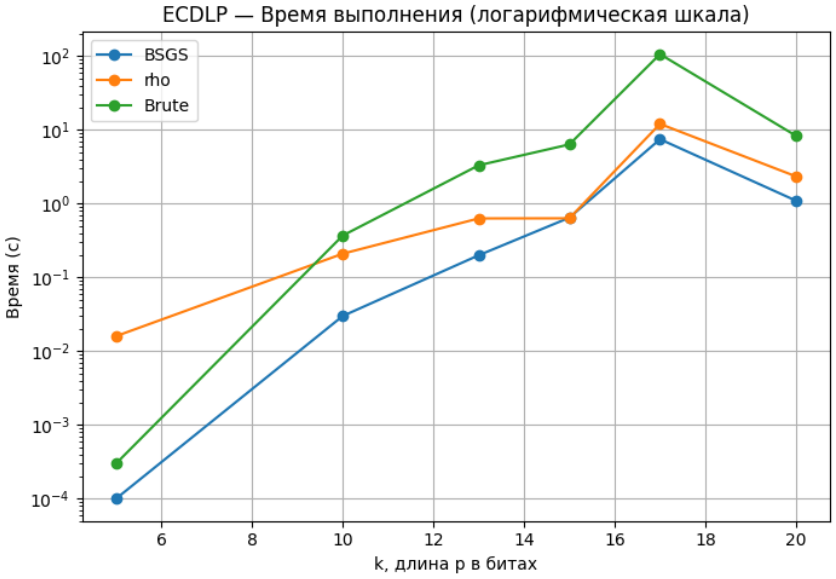

Рисунок 24 – Графики времени выполнения (логарифмическая шкала) для алгоритмов

ЗАКЛЮЧЕНИЕ

В работе выполнен теоретический и практический анализ задачи дискретного логарифмирования в мультипликативных группах конечных простых полей и в группах точек эллиптических кривых. Изучены математические основы, необходимые для понимания структуры рассматриваемых групп и особенностей алгоритмов, что позволило корректно интерпретировать результаты последующих экспериментов.

В рамках работы реализован программный комплекс (веб-приложение на *flask*), включающий набор алгоритмов вычисления дискретного логарифма:

- DLP – Гельфонда–Шенкса, ρ-метод Полларда, λ-метод Полларда, Сильвера-Полига-Хэллмана и индекс-метод;
- ECDLP – Гельфонда–Шенкса, ρ-метод Полларда и метод полного перебора.

Экспериментальное исследование подтвердило теоретические оценки сложности. Из алгоритмов DLP наилучшую практическую эффективность показал ρ-метод Полларда благодаря минимальному использованию памяти и стабильному времени работы. Алгоритм Гельфонда-Шенкса продемонстрировал ожидаемое увеличение объёма памяти. Метод Сильвера-Полига-Хэллмана оказался эффективными только при «гладких» порядках группы, а индекс-метод показывал стабильную работу при больших p в среднем.

Для эллиптических кривых единственным практически применимым методом из рассмотренных стал ρ-метод Полларда.

Поставленные задачи выполнены полностью. Веб-приложение готово и может использоваться в качестве учебного инструмента как основа для дальнейших исследований, включающих расширение набора методов и изучение алгоритмов постквантовой криптографии.