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

Криптографические приложения эллиптических кривых

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Кузнецова Егора Дмитриевича

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

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

Саратов 2026

ВВЕДЕНИЕ

Криптография на основе эллиптических кривых (ECC) на протяжении последних тридцати лет эволюционировала из сферы теоретических изысканий в один из ключевых и широко используемых средств обеспечения безопасности информации. Она стала основой для современных протоколов защищенной связи, таких как TLS и SSH, а также для цифровых подписей и алгоритмов обмена ключами. Эта технология активно применяется в таких областях, как блокчейн, интернет вещей (IoT) и электронные удостоверения.

Одним из основных преимуществ ECC является возможность достижения уровня безопасности, сравнимого с классическими алгоритмами, такими как RSA и DSA, при значительно меньшей длине ключей. В условиях растущей популярности мобильных устройств с ограниченными ресурсами и с учетом развития квантовых вычислений, поиск эффективных и надежных криптографических решений становится особенно актуальным.

Целью данной работы является изучение криптографических приложений эллиптических кривых, программная реализация алгоритма цифровой подписи на эллиптических кривых (ECDSA) и сравнительный анализ криптографических схем цифровой подписи и обмена ключами с помощью эллиптических кривых.

Основными решаемыми задачами данной работы являются:

1) изучение эллиптических кривых в форме Вейерштрасса;
2) изучение эллиптических кривых в форме Эдвардса;
3) изучение принципа работы криптографических схем подписи ECDSA, EdDSA и их программная реализация;
4) изучение принципа работы криптографических схем обмена ключами ECDH, X25519 и их программная реализация;
5) проведение сравнительного анализа рассмотренных криптосистем.

В результате работы выполнен сравнительный анализ криптографических свойств современных схем цифровой подписи и схем обмена ключами, которые

широко используются в интернет-протоколах. В рамках исследования рассматриваются криптографическая схема цифровой подписи на эллиптических кривых (ECDSA) и протокол обмена ключами Диффи-Хеллмана на эллиптических кривых (ECDH), схема цифровой подписи на кривых Эдвардса (EdDSA) и схема обмена ключами на основе кривой Curve25519 (X25519), а также классическая схема цифровой подписи (DSA) и протокол обмена ключами Диффи-Хеллмана (DH).

Дипломная работа состоит из введения, 5 разделов, заключения, списка использованных источников и 5 приложений. Общий объем работы – 89 страниц, из них 50 страниц – основное содержание, включая 24 рисунка и 5 таблиц, список использованных источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе «Общие сведения о криптографии на эллиптических кривых» представлены основные теоретические сведения об эллиптических кривых и групповом законе на эллиптических кривых.

В подразделе 1.1 «Определение эллиптической кривой. Уравнение Вейерштрасса» вводится понятие эллиптической кривой, уравнения Вейерштрасса эллиптической кривой, изоморфных форм эллиптической кривой Вейерштрасса, дискриминанта и j-инварианта кривой.

В подразделе 1.2 «Групповой закон на эллиптической кривой» описываются геометрическая и алгебраическая интерпретация группового закона сложения точек эллиптической кривой.

Во втором разделе «Формы представления эллиптических кривых» представлены различные формы представления эллиптических кривых с групповыми законами для этих форм.

В подразделе 2.1 «Форма Гессе» описывается кривая в форме Гессе и приводятся формулы группового закона со стоимостью операций.

В подразделе 2.2 «Форма Эдвардса» описывается кривая в форме Эдвардса, приводятся формулы группового закона и изоморфная форма кривой.

В подразделе 2.3 «Скрученные кривые Эдвардса» описываются скрученные кривые Эдвардса как обобщение кривых Эдвардса и приводятся формулы группового закона со стоимостью операций.

В подразделе 2.4 «Форма Монтгомери» описывается кривая в форме Монтгомери и приводятся формулы группового закона со стоимостью операций.

В подразделе 2.5 «Форма Якоби» описывается кривая в форме Якоби и приводятся формулы группового закона со стоимостью операций.

В третьем разделе «Эллиптические кривые в форме Эдвардса» более подробно рассматриваются кривые в форме Эдвардса вместе с описанием эффективности вычислений на кривых Эдвардса.

В подразделе 3.1 «Определение и уравнение кривой Эдвардса. Групповой закон» описывается кривая в форме Эдвардса с модификацией от Даниэля Бернштейна и Тани Ланге, которая позволяет описать универсальный закон сложения точек на эллиптических кривых в форме Эдвардса.

В подразделе 3.2 «Эффективность вычислений на кривых Эдвардса» описывается групповой закон сложения на эллиптических кривых Эдвардса в проективных координатах и инвертированных проективных координатах с оценкой стоимости вычислений.

В четвёртом разделе «Криптографические протоколы на основе эллиптических кривых» приводятся описания алгоритмов генерации доменных параметров для кривых Эдвардса, алгоритмов на эллиптических кривых Вейерштрасса, а также адаптированных алгоритмов для использования с формой Эдвардса.

В подразделе 4.1 «Построение доменных параметров для кривых Эдвардса» описывается алгоритм построения доменных параметров для кривых Эдвардса, использующий переход от кривой в форме Вейерштрасса к кривой в форме Монтгомери, а затем к кривой в форме Эдвардса.

В подразделе 4.2 «Протокол обмена ключами ECDH» описывается алгоритм Elliptic-Curve Diffie-Hellman (ECDH), который представляет собой схему установления общего секрета между двумя сторонами, основанную на операциях в группе точек эллиптической кривой над конечным полем.

В подразделе 4.3 «Алгоритм цифровой подписи ECDSA» описывается схема цифровой подписи ECDSA (Elliptic Curve Digital Signature Algorithm) на группе точек эллиптической кривой над конечным полем.

В подразделе 4.4 «Адаптация протоколов для использования с формой Эдвардса» рассматриваются схемы цифровой подписи и обмена ключами на эллиптических кривых Эдвардса.

В подразделе 4.4.1 «X25519 и X448» описываются конкретные реализации схемы Диффи-Хеллмана на эллиптических кривых Монтгомери Curve25519 и Curve448.

В подразделе 4.4.2 «EdDSA» описывается алгоритм цифровой подписи на эллиптических кривых Эдвардса.

В пятом разделе работы «Сравнительный анализ» приводится программная реализация алгоритмов цифровой подписи и обмена ключами. В данном разделе демонстрируется интерфейс программы и её функционал. Кроме того, здесь проведен анализ производительности схем цифровой подписи и обмена ключами.

В подразделе 5.1 «Описание программного комплекса» описывается структура проекта, а также использованные технологии.

В подразделе 5.2 «Описание работы программного комплекса» рассматривается интерфейс программы. Он приведен на рисунке ниже.

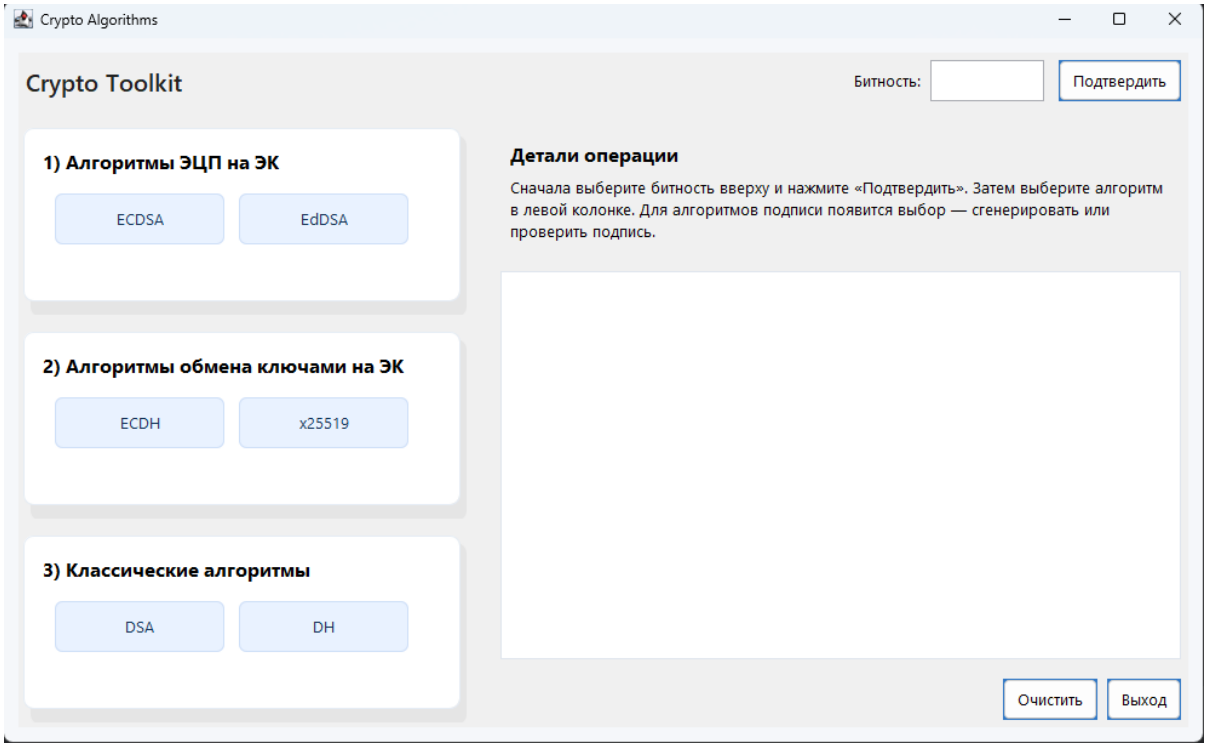

Рисунок 16 – Главное меню программы

Кроме того, здесь приведен функционал программы для различных алгоримтов, который представлен на рисунках ниже.

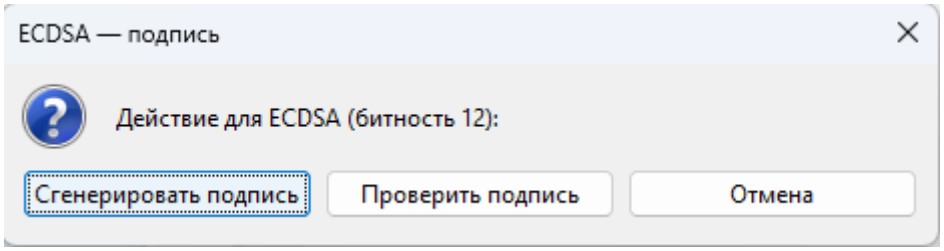

Рисунок 17 – Функционал для алгоритмов подписи

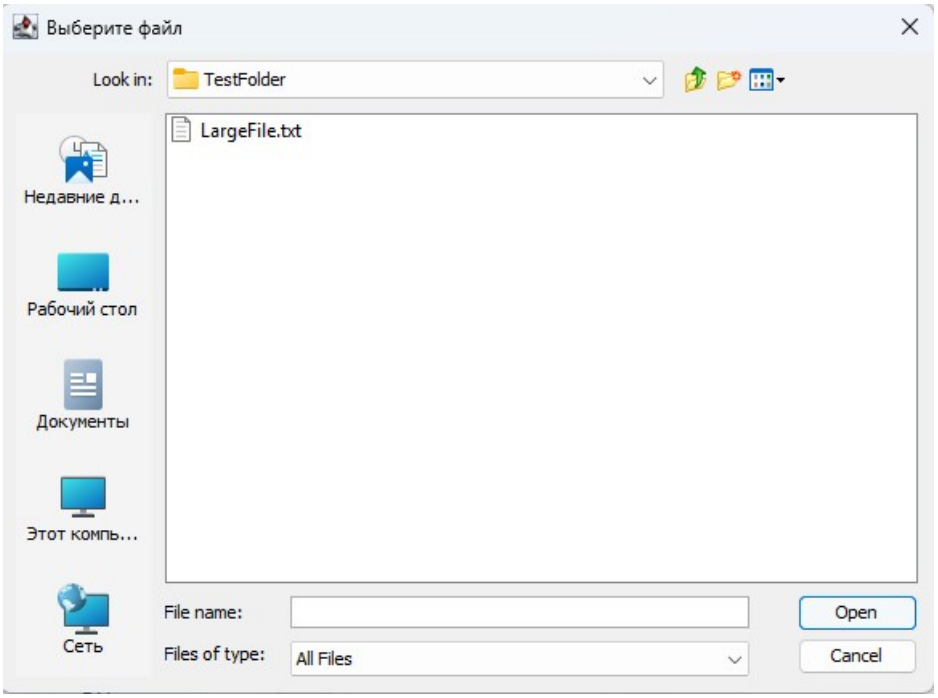

Рисунок 18 – Окно выбора файла для подписи

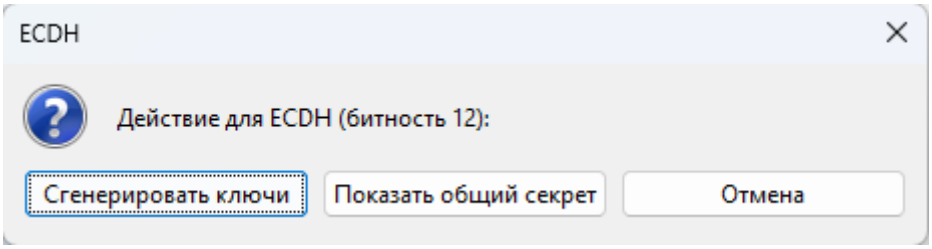

Рисунок 19 – Функционал для алгоритмов обмена ключами

```
[22:27:38] Битность установлена: 12 бит
[22:27:46] Генерация подписи: ECDSA, 12 бит
[22:27:59] Файл успешно подписан. Подпись сохранена в LargeFile.txt.sig
[22:28:03] Проверка подписи: ECDSA, 12 бит
[22:28:13] Подпись валидна
```

Рисунок 20 – Информирование пользователя об успешности операций

В подразделе 5.3 «Сравнительный анализ криптосистем» рассматривается информация о быстродействии алгоритмов на различных формах эллиптических кривых.

Результаты тестирования схем цифровой подписи на эллиптических кривых Вейерштрасса, Эдвардса и классической схемы цифровой подписи представлены в таблицах ниже.

Таблица 1 – Результаты анализа схемы ECDSA

Число бит	Время выполнения (миллисекунды)
10	506,71
11	1838,04
12	1910,53
13	6652,32
14	27188,35
15	174210,20

Таблица 2 – Результаты анализа схемы EdDSA

Число бит	Время выполнения (миллисекунды)
10	69,79
11	217,78
12	284,04
13	307,08
14	381,73
15	535,21

Таблица 4 – Результаты анализа схемы DSA

Число бит	Время выполнения (миллисекунды)
10	119,768045
11	204,463335
12	185,33934
13	168,341135
14	264,17443
15	267,914595

На рисунке 23 представлен график роста времени выполнения в зависимости от количества бит. Алгоритм ECDSA на кривых Вейерштрасса работает медленнее классического алгоритма DSA и алгоритма на кривых

Эдвардса EdDSA из-за сложности генерации доменных параметров. В свою очередь EdDSA показал сопоставимую с DSA скорость выполнения, но безопасность EdDSA при равном значении битов выше, чем при использовании DSA.

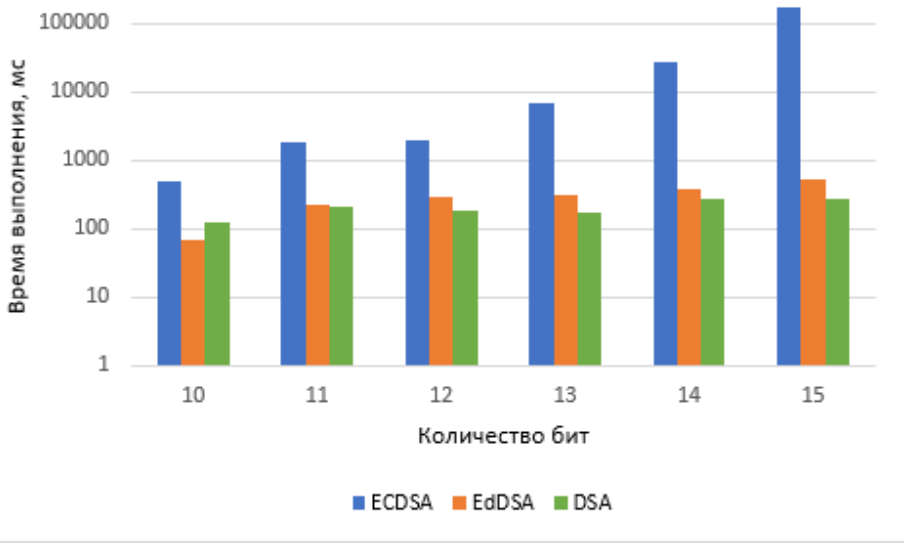

Рисунок 23 – Анализ алгоритмов ECDSA, EdDSA, DSA по времени

Результаты тестирования схем обмены ключами на эллиптических кривых Вейерштрасса, Эдвардса и классической схемы Диффи-Хэллмана представлены в таблицах ниже.

Таблица 3 – Результаты анализа схемы ECDH

Число бит	Время выполнения (миллисекунды)
10	760,840245
11	1366,532579
12	5601,6162
13	7089,46717
14	19181,95704
15	104381,0687

Для схемы обмена ключами X25519 среднее время выполнения программы составило 2,88 миллисекунд. Такая скорость достигается за счёт отсутствия в алгоритме процесса генерации доменных параметров кривой.

Таблица 5 – Результаты анализа схемы DH

Число бит	Время выполнения (миллисекунды)
10	2,982315
11	3,35659
12	2.974955
13	2,92719
14	3,225795
15	3,182455

Рисунок 24 демонстрирует колоссальное преимущество классического алгоритма DH во времени выполнения перед алгоритмом ECDH, но также как и в случае со схемами подписи, безопаность DH ниже алгоритма ECDH на эллиптических кривых при равных значениях бит.

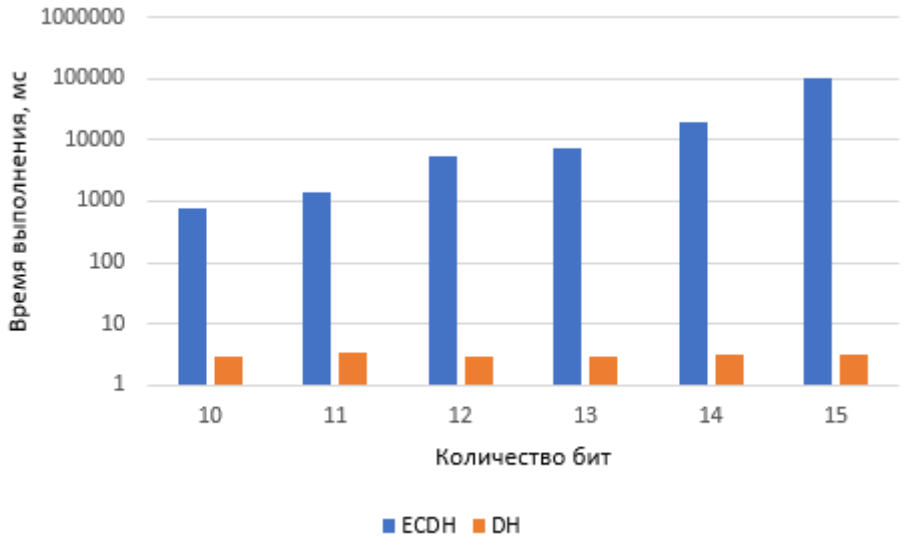

Рисунок 24 – Анализ алгоритмов ECDH, DH по времени

ЗАКЛЮЧЕНИЕ

В данной работе изучены криптографические приложения эллиптических кривых и программно реализован алгоритм ECDSA, а также проведён сравнительный анализ схем подписи и обмена ключами, реализованных на эллиптических кривых Вейерштрасса, Эдвардса, а также классические схем.

Для схем подписи выполнен сравнительный анализ по скорости генерации ключей и подписи файла, для схем обмена ключами сравнительный анализ проведён по скорости генерации публичного и приватного ключей.

Результаты исследования показали, что на этапе генерации параметров кривой алгоритмы на эллиптических кривых требуют выполнения сложных математических операций, что обычно приводит к меньшей скорости по сравнению с классическими методами, которые могут использовать заранее выбранные большие простые числа. При использовании заранее сгенерированных и стандартизированных параметров кривой, таких как secp256r1 или Curve25519, алгоритмы на эллиптических кривых показывают высокую скорость работы, не уступая, а порой и значительно превосходя классические алгоритмы, особенно в операциях верификации и установления сеанса при аналогичном уровне безопасности.

Кроме того, важным результатом исследования является тот факт, что алгоритм EdDSA, реализованный на эллиптических кривых Эдвардса, работает в среднем в 7 раз быстрее алгоритма ECDSA, который основан на эллиптических кривых Вейерштрасса. Это преимущество достигается благодаря формулам группового закона, оптимизированным для использования с кривыми Эдвардса.