На правах рукописи

Сабри Наурас Хуссейн Сабри

# МЕТОДЫ СНИЖЕНИЯ ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ ЦИФРОВОЙ ПОДПИСИ ДЛЯ УСТРОЙСТВ С ОГРАНИЧЕННЫМИ РЕСУРСАМИ

2.3.6. Методы и системы защиты информации, информационная безопасность

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2026

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)» на кафедре информационной безопасности факультета компьютерных технологий и информатики.

| | |
|---|---|
| Научный руководитель: | кандидат физико-математических наук, доцент<br>**Левина Алла Борисовна** |
| Официальные оппоненты: | **Саенко Игорь Борисович**,<br>доктор технических наук, профессор,<br>Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), лаборатория проблем компьютерной безопасности, главный научный сотрудник<br><br>**Широков Игорь Викторович**,<br>доктор физико-математических наук, профессор,<br>федеральное государственное бюджетное образовательное учреждение высшего образования<br>«Омский государственный технический университет»,<br>кафедра комплексной защиты информации, профессор |
| Ведущая организация: | Федеральное государственное автономное образовательное учреждение «Национальный исследовательский университет ИТМО», г. Санкт-Петербург |

Защита состоится 15 апреля 2026 года в 16.00 на заседании объединенного диссертационного совета 99.2.038.03, созданного на базе Федерального государственного бюджетного образовательного учреждения высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова», Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения», Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» по адресу: Санкт-Петербург, пр. Большевиков, д. 22, корп. 1, ауд. 554/1.

С диссертацией можно ознакомиться в библиотеке СПбГУТ по адресу Санкт-Петербург, пр. Большевиков, д. 22, корп. 1 и на сайте www.sut.ru.

Автореферат разослан 10 февраля 2026 года.

Ученый секретарь
диссертационного совета 99.2.038.03,
к.т.н., доц. А.Г. Владыко

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы исследования.** Встраиваемые системы являются основой современных цифровых устройств, обеспечивая выполнение задач в критически важных областях, таких как медицина и оборона. Их ядро (микроконтроллер), объединяет вычислительные модули, память, интерфейсы ввода-вывода, модули связи и таймеры.

Особенно активно встраиваемые системы развиваются в области беспилотных транспортных систем (UVS), применяемых для мониторинга, оборонных операций и других задач. Эти системы функционируют в условиях ограниченной памяти и энергопотребления, при этом решают задачи, напрямую влияющие на безопасность, но современные микроконтроллерные платформы UVS не обладают достаточными ресурсами для применения традиционных криптографических алгоритмов (RSA, DSA).

Практика эксплуатации UVS показала рост атак (GPS Spoofing, UAV Hijacking), что подтверждается инцидентами 2020–2025 гг., когда злоумышленники перехватывали управление или дезориентировали дроны с помощью SDR и средств радиоэлектронной борьбы (РЭБ). Эти случаи демонстрируют, что системы навигации и связи без надёжной криптографической защиты остаются уязвимыми. Одним из ключевых методов защиты является электронная цифровая подпись (ЭЦП), которая обеспечивает аутентичность и целостность данных.

Научное сообщество разрабатывает лёгкие криптографические методы для таких устройств. Перспективными являются алгоритмы на основе эллиптических кривых (ECDSA, EdDSA), обеспечивающие уровень безопасности RSA при меньших вычислительных затратах. Тем не менее, даже эти решения имеют высокую вычислительную сложность (например, операции ECPM и другие ресурсоёмкие задачи), что делает их использование серьёзным вызовом и требует оптимизации для снижения ресурсопотребления.

Существующие меры защиты (например, OSNMA в системе Galileo) основаны на ЭЦП для проверки подлинности навигационных данных. Однако перенос подобных решений на малые беспилотники сталкивается с ограничениями по производительности и энергопотреблению из-за ограниченных ресурсов микроконтроллеров. В этой связи существует острая потребность в разработке криптографических протоколов с минимальными требованиями к ресурсам и методов реализации ЭЦП, оптимизированных для микроконтроллеров, а также эффективных способов защиты от атак Replay и MITM (Man In the Middle Attack (Атака посредника)).

Современное развитие систем UVS и встроенных решений выявило фундаментальное противоречие: необходимость обеспечения высокого уровня криптографической безопасности (аутентичность, целостность, отказоустойчивость) при одновременном выполнении криптографических операций с использованием меньших ресурсов по сравнению с традиционными подходами, таких как вычислительная мощность, объём памяти и энергопотребление. Это противоречие усугубляется требованием функционирования в режиме реального времени, которое накладывает жёсткие ограничения на допустимые задержки при выполнении криптографических операций.

Таким образом, актуальность исследования определяется ростом применения UVS в критически важных задачах и подтверждёнными угрозами безопасности. Существующие криптографические алгоритмы недостаточно эффективны для устройств с ограниченными ресурсами, что требует разработки новых методов ЭЦП, обеспечивающих необходимую

криптостойкость при минимальных вычислительных затратах.

**Степень разработанности темы исследования.** Вопрос кибербезопасности и устойчивости систем электронной цифровой подписи (ЭЦП) на основе криптографии на эллиптических кривых (ECC) активно изучается. Значительный вклад внесли учёные В. И.Коржик, В. А. Яковлев, Клаус Петер Шнорр, Тахер Эль Гамаль, Нил Коблиц, Виктор Миллер, Дэниел Бернштейн, Таня Ланге, Дэвид Пойнтшеваль, Элетт Бойле, Н. А. Молдовян, А. А. Молдовян, Александрова Е. Б. и другие, чьи работы посвящены надёжности и безопасности информационных систем с использованием эллиптической криптографии.

Монография «*Основы криптографии*» (В. И. Коржик, В. А. Яковлев), подробно раскрывающая математические основы ЭЦП на ECC, заложила фундамент для глубокого понимания этого направления и открыла путь для его дальнейшего развития.

В работах Н. А. Молдовяна представлены значимые теоретические и практические подходы к оптимизации алгоритмов электронной подписи. В монографии «*Теоретический минимум и алгоритмы цифровой подписи*» обоснованы математические методы построения эффективных схем ЭЦП, в том числе на эллиптических кривых, а в работе «*Множественная подпись: новые решения на основе понятия коллективного открытого ключа*» предложены усовершенствованные протоколы коллективной и композиционной ЭЦП, снижающие вычислительную сложность и повышающие гибкость систем безопасности. Эти исследования создают научную базу для разработки новых решений в условиях ограниченных вычислительных ресурсов.

Настоящая диссертация является логическим продолжением исследований, направленных на разработку решений для устройств с ограниченными ресурсами, включая микроконтроллеры.

**Объект исследования:** Электронная цифровая подпись на основе криптографии на эллиптических кривых, реализованная во встраиваемых системах с ограниченными ресурсами (например, микроконтроллерах), используемых в беспилотных транспортных системах (UVS).

**Предмет исследования:** Вычислительная сложность электронной цифровой подписи на основе криптографии на эллиптических кривых.

**Цель исследования:** Снижение вычислительной сложности электронной цифровой подписи на основе криптографии на эллиптических кривых без снижения криптостойкости, для повышения эффективности и расширения применимости данных подписей в устройствах с ограниченными ресурсами.

**Гипотеза исследования** заключается в том, что достижение поставленной цели возможно за счёт снижения количества операций сложения и удвоения точек, необходимых для выполнения операции умножения точки на скаляр на эллиптической кривой (которая является ключевой и наиболее ресурсоёмкой в ECC и ЭЦП на её основе), путём интеграции свойств циклических групп и аддитивных обратных элементов из теории групп с проверенными методами умножения точек на скаляр на эллиптических кривых, а также за счёт дальнейшей оптимизации самой схемы ЭЦП основанный на оптимизированном умножении точек на скаляр на эллиптических кривых (на базе ранее предложенного метода), использующий детерминированной алгоритм генерации однократно используемого числа, исключении его открытого значения при вычислении вызова (challenge) и подтверждении владения закрытым ключом с применением агрегированного открытого ключа вместо

традиционных доказательств с нулевым разглашением (NIZK).

Для достижения цели исследования сформулирована **научная задача**, которая заключается в разработке математических методов оптимизации операции умножения точки на эллиптической кривой и схем электронной цифровой подписи на основе криптографии на эллиптических кривых, направленных на снижение вычислительной сложности.

В предлагаемой формулировке цель исследования и научная задача определены впервые. Цель и научная задача **соответствуют специальности 2.3.6** Методы и системы защиты информации, информационная безопасность по следующим пунктам паспорта специальности:

- Пункт 12. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.
- Пункт 15. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

В процессе исследования **научная задача была декомпозирована на следующую совокупность взаимоувязанных частных научных и прикладных задач:**

1. Разработка нового математического метода умножения точек на скаляр на эллиптических кривых, основанного на использовании свойств циклической группы и противоположных элементов из теории групп.

Задача включает:

- Исследование математических основ криптографии на эллиптических кривых (в особенности операции умножения точки на скаляр) и проблем её реализации в условиях ограниченных ресурсов. Задача включает глубокий анализ принципов криптографии на эллиптических кривых и выявление специфических проблем её реализации на устройствах с ограниченными ресурсами, с учётом особенностей встроенных систем и базовых операций.
- Создание математически обоснованного метода, позволяющего сократить количество операций сложения и удвоения точек на эллиптической кривой, что приводит к снижению вычислительной сложности ЭЦП на основе ECC для встроенных систем с ограниченными ресурсами.

2. Разработка нового математического метода построения схемы электронной цифровой подписи на основе криптографии на эллиптических кривых, обеспечивающего снижение вычислительной сложности, времени обработки, количества процессорных тактов, использования памяти и требуемой пропускной способности каналов связи без снижения криптостойкости.

Задача включает:

- Исследование математических основ существующих схем электронной цифровой подписи и проблем их реализации в условиях ограниченных ресурсов. Задача включает глубокий анализ принципов электронной цифровой подписи и выявление специфических проблем её реализации на устройствах с ограниченными ресурсами, с учётом особенностей встроенных систем и базовых операций.
- Разработка метода, основанного на использовании ранее предложенного оптимизированного метода умножения точек на скаляр на эллиптических кривых, как ключевого компонента схемы, и применении детерминированной генерации однократно используемого числа, отказе от использования его публичного значения при вычислении вызова (challenge) и подтверждении владения приватным ключом на основе агрегированного открытого ключа вместо традиционных доказательств с нулевым разглашением без

взаимодействия (NIZK), обеспечивающих снижение вычислительной сложности без снижения криптостойкости.

3. Программная Реализация двух предложенных методов в рамках единой схемы электронной цифровой подписи на основе криптографии на эллиптических кривых в условиях ограниченных ресурсов (микроконтроллера ATmega2560 Arduino) и демонстрация эффективности и практической применимости предложенных методов в реальных условиях.

Задача включает:

- Демонстрация практической применимости и эффективности предложенных теоретических решений в реальных условиях функционирования.
- Проведение оценки эффективности предложенных методов для подтверждения их практической ценности.
- Выполнение сравнительного анализа предложенных методов с существующими решениями с целью демонстрации их преимуществ и выявления возможностей для дальнейшего совершенствования.

**Положения, выносимые на защиту,** соответствуют результатам решения вышеуказанных частных научных и прикладных задач:

- Метод умножения точек на скаляр на эллиптических кривых, основанный на использовании свойств циклической группы и свойств противоположного числа из теории групп, снижающий количество операций сложения и удвоения точек в процессе умножения точки на скаляр, обеспечивающий снижение общей вычислительной сложности без снижения криптостойкости (пункт 15 паспорта специальности).
- Метод построения схемы ЭЦП на основе ECC, основанный на оптимизированном умножении точек на скаляр на эллиптических кривых (на базе ранее предложенного метода), использующий детерминированной алгоритм генерации однократно используемого числа, исключении его открытого значения при вычислении вызова (challenge) и подтверждении владения закрытым ключом с применением агрегированного открытого ключа вместо традиционных доказательств с нулевым разглашением (NIZK). приводящий к снижению общей вычислительной сложности без снижения криптостойкости (пункт 12 паспорта специальности).
- Программное обеспечение реализующие оптимизированное умножения точек на скаляр на эллиптических кривых (первый метод) и схемы ЭЦП (второй метод) на микроконтроллере ATmega2560, демонстрирующее повышение производительности систем с ограниченным ресурсами по сравнению с существующими решениями.

**Научная новизна.** Полученные в работе новые научные и прикладные результаты обладают следующими признаками новизны.

1. За счёт интеграции свойства циклической группы точек эллиптической кривой и свойства аддитивного обратного элемента из теории групп, в первом положении, выносимом на защиту, предложена математическая конструкция, позволяющая сократить количество операций сложения и удвоения точек, необходимых для реализации операции умножения точки на скаляр на эллиптической кривой, обеспечивающая снижение вычислительной сложности реализации электронной цифровой подписи на основе криптографии на эллиптических кривых на устройствах с ограниченными ресурсами. Так же новым подходом является то, что при его реализации интегрируется метод, основанный на лестнице Монтгомери, при котором операции сложения с использованием единичного элемента (точки на бесконечности) вставляются при появлении нулевых бит в двоичном представлении скаляра. Такой подход устраняет несогласованности в реализации, которые могли бы быть использованы в атаках по сторонним каналам для извлечения секретного ключа, сохраняя при

этом уровень криптостойкости, сопоставимый с существующими решениями, не снижая надёжность системы.

2. За счёт следующих ключевых нововведений впервые разработан новый метод к генерации ЭЦП упрощающий существующие схемы, представленный во втором положении, выносимом на защиту:

a. Детерминированная генерация однократно используемого числа, исключающая зависимость от генераторов случайных чисел, предотвращающая повторное использование однократно используемого числа и защищающая от утечек закрытого ключа, связанных с недостаточной случайностью.

b. Исключение публичного однократно используемого числа ($R$) из вычисления вызова (challenge) упрощает вычисления и снижает потребление памяти.

c. Отказ от применения NIZK с заменой на проверку на основе агрегированного открытого ключа. Это снижает нагрузку на канал связи и повышает эффективность генерации подписи на устройствах с ограниченными ресурсами.

3. Впервые показана эффективность реализации обоих предложенных методов на устройствах с ограниченными ресурсами, таких как микроконтроллер ATmega2560. Реализация обоих методов привела к снижению вычислительной сложности, что, в свою очередь, сократило потребление памяти, количество тактов процессора и пропускную способность, необходимую для передачи и приёма подписи. При этом криптостойкость схемы не снижена: она сохраняет устойчивость к основным типам атак, включая Nonce Reuse Attack, Key Cancellation Attack, Rogue Key Attack, Virtual Machine Rewinding Attack и Replay Attack.

Предложенные методы демонстрируют высокую стойкость к различным типам атак, включая атаки повторного использования однократно используемого числа (Nonce Reuse Attack), отмены ключа (Key Cancellation Attack), атаки с использованием поддельного ключа (Rogue Key Attack), атаки перемотки виртуальной машины и атаки повторного воспроизведения (Replay Attack).

Таким образом, в диссертации представлены новые научные и практические результаты, позволяющие решить научную задачу, имеющую существенное значение для развития научно-методического аппарата повышения эффективности и надежности алгоритмов ЭЦП на основе ECC в условиях информационно-вычислительных систем с ограниченными ресурсами. Предложенные решения направлены на снижение вычислительной сложности и обеспечение эффективной генерации подписей в условиях возрастания киберугроз. Указанные результаты соответствуют требованиям пункта 9 «Положения о присуждении учёных степеней», данная диссертация является научно-квалификационной работой, содержащей результаты, которые можно квалифицировать как научное достижение, новое научно обоснованное решение, имеющее значительный вклад в развитие страны.

**Теоретическая значимость работы** заключается в развитии научно-методического аппарата построения базовых криптографических операций на эллиптических кривых (ECPM) и схем ЭЦП для встроенных систем. Предложены математически обоснованные методы, позволяющие снизить вычислительную сложность без снижения криптостойкости за счёт интеграции свойств циклических групп и отказа от использования открытого однократно используемого числа и NIZK. Работа формирует новые методы к построению эффективных и безопасных криптографических протоколов для систем с ограниченными ресурсами.

**Практическая значимость работы** состоит в возможности применения разработанных методов оптимизации ECPM и схем ЭЦП на основе ECC для встраиваемых микроконтроллерных систем, используемых в UVS и других устройствах с ограниченными

ресурсами. Реализация методов на платформе ATmega2560 показала снижение вычислительной нагрузки, потребления памяти, времени выполнения и энергозатрат, что подтверждает их эффективность для практического использования.

**Достоверность научных результатов** подтверждается:

- Использованием принципов системного анализа при формулировании научной задачи и разработке методов снижения вычислительной сложности криптографических операций на основе эллиптических кривых;
- Строгим аналитическим выводом математических зависимостей, лежащих в основе предложенных методов оптимизации операции ECPM и методов построения ЭЦП;
- Согласованностью экспериментальных результатов, полученных при реализации методов на платформе микроконтроллера ATmega2560, с теоретическими расчётами, что подтверждает корректность математических решений и их практическую применимость;
- Соответствием полученных результатов опубликованным научным работам и фундаментальным исследованиям в области криптографии на эллиптических кривых и оптимизации криптографических вычислений;
- Апробацией результатов исследования путём публикации в рецензируемых научных изданиях, а также их представлением и обсуждением на международных научно-практических конференциях.

**Методы исследования** включают в себя методы математического моделирования и теории групп для оптимизации базовых криптографических операций; методы алгоритмической оптимизации и анализа вычислительной сложности; методы теории информации и криптографии для обеспечения безопасности цифровых подписей; а также экспериментальные методы для оценки производительности на микроконтроллерных платформах с ограниченными ресурсами. Кроме того, использовались методы сравнительного анализа, моделирования и статистической обработки для верификации эффективности предложенных решений.

**Публикации по теме диссертации.** По теме диссертации опубликовано 12 печатных работ, 2 [1, 2] из которых – в изданиях из перечня рецензируемых научных журналов ВАК при Минобрнауки России, соответствующих пункту 11 «Положения о присуждении учёных степеней» по защищаемой специальности 2.3.6, в том числе 4 [2, 9, 10, 12] из них без соавторства; 4 [5, 6, 7, 8] – в международных изданиях, индексируемых в базах данных Web of Science и Scopus, которые в соответствии с Рекомендацией ВАК № 3-пл/1 от 21.12.2023 г. приравниваются к публикациям в рецензируемых изданиях, рекомендованном ВАК, категории К1; 2 [3, 4] свидетельства о государственной регистрации программы для ЭВМ, в соответствии с п. 12.1 «Положения о присуждении ученых степеней», приравнивается к публикациям в рецензируемых изданиях, рекомендованных ВАК; 4 [9, 10, 11, 12] работ, опубликованных в других изданиях.

Все представленные публикации отражают основные научные результаты диссертационного исследования, включая разработку математического метода умножения точек на скаляр на эллиптических кривых, позволяющего снизить вычислительную сложность без снижения криптостойкости; математического метода построения схемы ЭЦП, направленного на снижение общей вычислительной сложности и сопутствующих затрат, включая количество процессорных тактов, объём используемой памяти и нагрузку на коммуникационные каналы; а также реализацию этих методов на микроконтроллере ATmega2560, демонстрирующую повышение эффективности использования ЭЦП в системах

с ограниченными ресурсами по сравнению с существующими решениями.

**Личный вклад соискателя**. Из 11 представленных публикаций работы [2, 9, 10] выполнены единолично.

Указанные публикации подтверждают самостоятельное выполнение исследований и достижение основных результатов, выносимых на защиту. При этом статья в журнале «Труды учебных заведений связи» опубликована в рецензируемом издании, входящем в перечень ВАК, рекомендованном для публикации результатов диссертационных исследований.

В публикациях в международных рецензируемых научных изданиях — Applied Sciences (MDPI), IEEE Access, Mathematics (MDPI) и Scientific Reports (Nature Publishing Group), а также в статье, опубликованной в российском рецензируемом журнале из перечня ВАК — Вестник компьютерных и информационных технологий, личный вклад автора определяется следующим образом:

- Автору принадлежит основная роль в уточнении формулировки целей и задач исследования, разработке методов, определении исходных допущений, проведении математического моделирования, разработке программного обеспечения, выполнении вычислительных экспериментов, анализе полученных результатов, формулировании выводов и подготовке первоначальных версий публикаций.
- Научный руководитель А.Б. Левина принимала ведущее участие в формировании общей концепции исследования, постановке научных задач, контроле выполнения работ, редактировании текстов публикаций и административной поддержке проекта.

Все теоретические и практические выводы, разработка методов снижения вычислительной сложности цифровой подписи на основе криптографии на эллиптических кривых, написание программных моделей и алгоритмов, анализ результатов измерений, содержащиеся в данной диссертационной работе, выполнены автором самостоятельно. Постановка целей и задач принадлежит научному руководителю.

**Апробация результатов исследования.** Результаты диссертационного исследования были апробированы и обсуждены на двух международных научных конференциях, проведённых в 2024 году:

– *13th Mediterranean Conference on Embedded Computing (MECO)* (Будва, Черногория, июнь 2024 г.);

– *16th International Conference “Intelligent Systems” (INTELS’24)* (Москва, Московский государственный университет имени М. В. Ломоносова, 2024 г.).

Подтверждением апробации результатов исследования на указанных конференциях является публикация тезисов и статей в официальных сборниках трудов конференций, индексируемых в международных научных базах данных, включая IEEE Xplore [11].

**Внедрение и реализация результатов исследования.**

Основные результаты диссертационного исследования были внедрены при:

- Сабри Н.Х. Акт о внедрении результатов диссертационной работы на тему «Методы снижения вычислительной сложности цифровой подписи для устройств с ограниченными ресурсами» // АНО «Институт инженерной физики». – Серпухов, 11.09.2025. – 1 с.

- Сабри Н.Х. Акт о внедрении результатов диссертационной работы на тему «Методы снижения вычислительной сложности цифровой подписи для устройств с ограниченными ресурсами» // ООО «ТР-СОФТ». – Санкт-Петербург, 2025. – 1 с.

**Структура и объем диссертации.** Диссертационная работа состоит из введения, четырёх глав, заключения, списков сокращений, а также списка литературы из 119 наименований. Общий объём работы составляет 201 страниц, включая 45 рисунков и 17 таблиц.

## СОДЕРЖАНИЕ РАБОТЫ

**Во введении** обоснована актуальность темы диссертационного исследования, поставлена цель и сформулирована основная научная задача. Научная задача декомпозирована на совокупность частных научных и прикладных задач. Представлены положения, выносимые на защиту, соответствующие результатам решения частных научных и прикладных задач, сведения об их научной новизне, теоретической и практической значимости, а также иные формальные положения диссертационного исследования. Представлены сведения об апробации и внедрении результатов диссертационного исследования. Приведено краткое содержание диссертационного исследования по главам.

**В первой главе** представлен обзор эволюции криптографии и математических основ, необходимых для построения протоколов электронной цифровой подписи (ЭЦП) на базе эллиптических кривых (ECC). Особое внимание уделено операции скалярного умножения точки (ECPM), лежащей в основе ECC, и проблемам её реализации в условиях ограниченных ресурсов. Глава охватывает основы ECC и схем ЭЦП, что важно для решения научной задачи диссертации.

Рассмотрены основы теории эллиптических кривых Коблица и Миллера, основанные на групповой структуре точек над конечными полями и сложности задачи дискретного логарифма (ECDLP). Эти свойства позволяют строить эффективные криптографические протоколы с меньшими длинами ключей.

Эллиптическая кривая задаётся кубическим уравнением (общая форма Вейерштрасса, стандартный общий вид эллиптических кривых):

$$E\colon\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

в криптографии применяют сокращённую форму над полем $F_p$ : $y^2 \equiv x^3 + ax + b(mod\ p), 4a^3 + 27b^2 \neq 0(mod\ p)$ гарантирующую гладкость кривой. Пример кривой показан на Рис. 1.

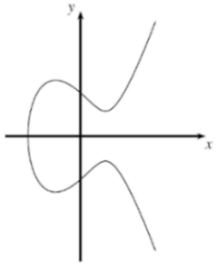


Рис. 1. Эллиптическая кривая $y^2 = x^3 - 3x + 3$ над полем $\mathbb{R}$.

Также в работе рассматриваются и другие формы уравнений (Эдвардса, Монтгомери), удобные для реализации.

Групповую операцию можно определить геометрически: прямая через две точки $P$ и $Q$ (или касательная в $P$ при удвоении) пересекает кривую в третьей точке, отражение которой относительно оси $x$ даёт результат сложения. Вводятся нейтральный элемент $O$, обратный элемент $-P = (x, -y)$ (над $F_p$: $-y \equiv p - y\,(mod\ p)$ и базовая (генерирующая) точка $G$, с помощью которой порождается циклическая подгруппа.

Для сложения точек $P = (x_1, y_1)$ и $Q = (x_2, y_2)$, $P \neq Q$ необходимо вычислить:

$s = \frac{y_2 - y_1}{x_2 - x_1}\ (mod\ p)$, $x_3 = s^2 - x_1 - x_2\ (mod\ p)$, $y_3 = s(x_1 - x_3) - y_1 (mod\ p)$

Для удвоения точки $P = (x_1, y_1)$ необходимо вычислить:

$s = \frac{3x_1^2 + a}{2y_1}\ (mod\ p)$, $x_3 = s^2 - 2x_1 (mod\ p)$, $y_3 = s(x_1 - x_3) - y_1 (mod p)$

Эти операции лежат в основе скалярного умножения $kP = P + ... + P$ ($k$ раз).

Операции сложения и удвоения точек могут выполняться в различных системах координат, таких как проективная система координат или расширенная проективная система координат, чтобы исключить вычислительно дорогие операции деления (или нахождения обратного числа).

Порядок $E$, это количество точек на кривой (включая $O$). Он играет ключевую роль при генерации ключей, оценке безопасности, согласовании параметров и корректном выполнении скалярного умножения. Задача дискретного логарифма на эллиптических кривых формулируется как вычисление $k$ из $P$ и $T = kP$, что крайне сложно. На сложности решения этой задачи основана безопасность ECC.

В первой главе рассмотрены математические основы и принципы работы основных схем ЭЦП, обеспечивающих аутентичность, целостность и невозможность отказа от авторства. Подчёркивается, что традиционные алгоритмы с открытым ключом, такие как RSA и DSA, требуют больших длин ключей (2048–4096 бит) и значительных вычислительных ресурсов, что делает их малоэффективными для встроенных систем. Криптография на эллиптических кривых (ECDSA, EdDSA, Шнорр) обеспечивает сопоставимую безопасность при длине ключей 256–521 бит, что повышает производительность и энергоэффективность.

Алгоритм **RSA** основывается на факторизации больших чисел, а его работа использует пару ключей $(e, n)$ и $(d, n)$, где $n = p\,q$, $\varphi(n) = (p-1)(q-1)$, $e$ выбирается взаимно простым с $\varphi(n)$, а $d \equiv e^{-1} (mod \varphi(n))$, секретный ключ. **Подпись** формируется как $s \equiv H(m)^d (mod\ n)$, а **проверка** осуществляется проверкой равенства $H(m) \equiv s^e (mod\ n)$. Корректность обеспечивается тем, что $s^e \equiv (H(m)^d)^e \equiv H(m)^{de} \equiv H(m) (mod\ n)$, так как $de \equiv 1 (mod \varphi(n))$.

Алгоритм **DSA** основан на сложности задачи дискретного логарифмирования в модульной арифметике. **Генерация ключей:** выбираются простые числа $p$ и $q$ (где $p - 1$ делится на $q$), параметр $g = h^{(p-1)/q} (mod\ p)$, секретный ключ $x \in (1, q)$, открытый ключ $y = g^x (mod\ p)$. **Генерация подписи:** для сообщения $m$ выбирается случайное $k \in (1, q)$, вычисляются $r = (g^k (mod\ p)) mod\ q$ и $s = k^{-1}(H(m) + x \cdot r)\ mod\ q$. Подпись представляет

собой пару (r, s). **Проверка подписи:** проверяются $0 < r, s < q$, затем вычисляются $\omega = s^{-1} \bmod q, u_1 = H(m)\omega \bmod q, u_2 = r\omega \bmod q$ , $v = (g^{u_1} y^{u_2} \bmod p) \bmod q$ . Подпись корректна, если $v = r$. **Доказательство корректности:** из формул генерации следует, что $v = r$, так как $(H(m) + xr)s^{-1} \equiv k \bmod q$, что приводит к $v = g^k \bmod p \bmod q = r$.

Алгоритм **ECDSA** является аналогом DSA, использующим криптографию на эллиптических кривых. **Генерация ключей:** выбирается эллиптическая кривая над полем $F_p$ или $F_{2^m}$, базовая точка $G$ порядка $n$, секретный ключ $x \in (1, n)$, открытый ключ $X = xG$. **Генерация подписи:** вычисляется хеш $H(m)$, выбирается случайное $k \in (1, n)$, точка $(x_1, y_1) = kG, r = x_1 \bmod n, \quad s = k^{-1}(H(m) + xr) \bmod n$. Подпись — пара $(r, s)$. **Проверка подписи:** вычисляется $\omega = s^{-1} \bmod n, u_1 = H(m')\omega \bmod n, u_2 = r\omega \bmod n, (x_1, y_1) = u_1 G + u_2 X$. Подпись корректна, если $x_1 \bmod n = r$. **Доказательство корректности:** из $s = k^{-1}(H(m) + xr)$ следует $\omega(H(m') + xr) \equiv k \bmod n$, значит $(x_1, y_1) = kG$, и $x_1 \bmod n = r$.

Алгоритм **EdDSA** основан на скрученных кривых Эдвардса и задаче дискретного логарифмирования на эллиптических кривых. Для генерации ключей выбирается скрученная кривая Эдвардса с параметрами $(p, d, q, G)$. Закрытый ключ $x$ формируется как случайная битовая строка, а открытый ключ вычисляется как $X = x \cdot G$. Процесс **подписи** сообщения $m$ включает вычисление $r = H(x|m) \bmod q$, затем точки $R = r \cdot G$ и значения $S = (r + H(R|X|m) \cdot x) \bmod q$ . Подпись представляет собой пару (R, S). Проверка подписи выполняется с помощью условия $S \cdot G = R + h \cdot X$, где $h = H(R|X|m') \bmod q$, и если это равенство выполняется, подпись считается корректной. Корректность схемы обеспечивается тем, что $S \cdot G = (r + h \cdot x) \cdot G = r \cdot G + h \cdot X = R + h \cdot X$, что гарантирует аутентичность и целостность данных.

Алгоритм **Шнорра** отличается простотой вычислений, эффективностью и устойчивостью к подделке благодаря использованию задачи дискретного логарифмирования. Линейная структура подписей Шнорра делает её удобной для агрегирования, что повышает эффективность современных криптографических протоколов. **Генерация ключей** выполняется путём выбора циклической группы $G$ простого порядка $p$ с генератором $g$. Закрытым ключом является число $x$, где $0 < x < p$, а открытый ключ вычисляется как $X = g^x$. Процесс **подписи** сообщения включает выбор случайного числа $r$ и вычисление $R = g^r$. Далее формируется значение вызова $c = H(X, R, m)$, и рассчитывается $s = (r + c \cdot x) \bmod p$. Подписью служит пара $(R, s)$. **Проверка** подписи осуществляется путем проверки равенства $g^s = R \cdot X^c$, что гарантирует её подлинность. Корректность схемы следует из того, что $s = r + c\,x$, и, следовательно, $g^s = g^{r+cx} = g^r \cdot g^{cx} = R \cdot X^c$, что подтверждает правильность проверки.

**Агрегация подписей**, это криптографический метод, позволяющий объединять несколько цифровых подписей в одну компактную подпись, что снижает требования к хранению данных и ускоряет процесс их проверки. Такая схема особенно полезна в системах, где важна высокая эффективность, например, в блокчейнах. **Генерация ключей:** Каждый участник генерирует секретный ключ $k$ и соответствующий открытый ключ $P = kG$. Для подписи выбирается случайное число $r$, из которого вычисляется $R = rG$. **Генерация и проверка подписи**: Хеш $c = H(R||P||m)$ используется для построения подписи $s = r + c\,k$. Проверка подписи осуществляется проверкой равенства $sG = R + Pc$ . В случае мультиподписей агрегированная подпись строится как $P_{\text{agg}} = P_a + P_b$ и $s_{\text{agg}} = s_a + s_b$ . **Доказательство корректности**: Так как $s = r + c\,k$, выполняется: $sG = (r + ck)G = rG + c(kG) = R + Pc$, что подтверждает корректность подписи.

Схема **мультиподписи Шнорра** позволяет нескольким подписантам совместно создавать единую компактную подпись для сообщения $m$. **Генерация ключей**: Каждый участник выбирает секретный ключ $x_i$ и вычисляет открытый ключ $X_i = g^{x_i}$. Агрегированный открытый ключ определяется как $\tilde{X} = \prod_{i=1}^{n} X_i$. **Генерация и проверка подписи**: Каждый подписант выбирает случайное число $r_i$, вычисляет $R_i = g^{r_i}$), после чего: $R = \prod_{i=1}^{n} R_i$ , $c = H(\tilde{X}, R, m)$, $s_i = r_i + cx_i$. Общая подпись вычисляется как: $s = \sum_{i=1}^{n} s_i \, mod \, p$, и пара $(R, s)$ отправляется для проверки. Подпись считается корректной, если выполняется: $g^s = R \cdot \tilde{X}$. **Доказательство корректности**: так как $s = \sum(r_i + cx_i)$, имеем: $g^s = \prod g^{r_i} \cdot \prod g^{x_i} = R \cdot \tilde{X}$, что подтверждает правильность схемы.

Сравнение (Таблица 1) показывает, что ECC-алгоритмы (ECDSA, EdDSA, Шнорр и их агрегированные варианты) при равной стойкости имеют меньшие длины ключей и вычислительные затраты по сравнению с RSA/DSA, что делает их предпочтительными для систем с ограниченными ресурсами.

| Алгоритм | Задачи, на которых основан алгоритм | Размер ключа |
|---|---|---|
| RSA | Факторизация | 2048–4096 бит |
| DSA | Проблема дискретного логарифмирования | 2048–3072 бит |
| ECDSA | Эллиптические кривые | 256–521 бит |
| EdDSA | Скрученные кривые Эдвардса | 256 бит |
| Шнорра | Дискретный логарифм, Эллиптические кривые | 256–512 бит |

Таблица 1: Сравнение алгоритмов электронной подписи

Несмотря на эффективность, современные схемы подписей сохраняют высокую вычислительную сложность, что требует дальнейшей оптимизации для устаревших и ресурсно-ограниченных платформ.

**Во второй главе** представлены результаты первого положения, выносимого на защиту, направленного на разработку математического метода умножения точек на скаляр на эллиптических кривых, основанного на использовании свойств циклической группы и свойств противоположного числа из теории групп, снижающих количество операций сложения и удвоения точек в процессе умножения точки на скаляр и обеспечивающих снижение общей вычислительной сложности без снижения криптостойкости.

Глава начинается с подробного описания операции умножения точки на скаляр на эллиптической кривой (ECPM) и демонстрации её ключевой роли в криптографии на основе эллиптических кривых. Проведён анализ вычислительной сложности данной операции в условиях ограниченных вычислительных ресурсов и обоснована необходимость её оптимизации для повышения эффективности схем цифровой подписи в таких системах.

Выполнен всесторонний обзор существующих методов оптимизации ECPM, включая метод лестница Монтгомери, и оконный метод, с акцентом на их вычислительные затраты, требования к памяти и устойчивость к атакам по сторонним каналам.

Отмечены противоречия – необходимость обеспечения высокой скорости работы и высокого уровня безопасности при минимизации потребления ресурсов, что подчёркивает необходимость сбалансированного подхода при реализации криптографии на эллиптических кривых в средах с ограниченными ресурсами, по сравнению с существующими решениями.

Подробно рассмотрены три основных метода:

- метод удвоения и сложения как простой и лёгкий по вычислениям, но уязвимый к

атакам по времени;

- оконный метод, обеспечивающий высокую скорость за счёт использования таблиц предвычисленных точек, но обладающий высокими требованиями к памяти и подвержен утечкам по времени;

- и метод лестница Монтгомери, обладающий защитой за счёт постоянного времени выполнения, но требующий большего числа вычислительных операций.

Проведено экспериментальное сравнение этих методов на кривой secp256k1 в аффинных и однородных системах координат. В аффинных координатах метод удвоения и сложения показал время от 0.0097 до 0.0241 секунды, метод лестница Монтгомери — от 0.0151 до 0.0300 секунды, а оконный метод — от 0.0030 до 0.0123 секунды. В однородных координатах результаты улучшились: удвоение и сложение — от 0.00046 до 0.0095 секунды, лестница Монтгомери — от 0.00088 до 0.0097 секунды, оконный метод — от 0.00028 до 0.0092 секунды, как показано на следующей диаграмме:

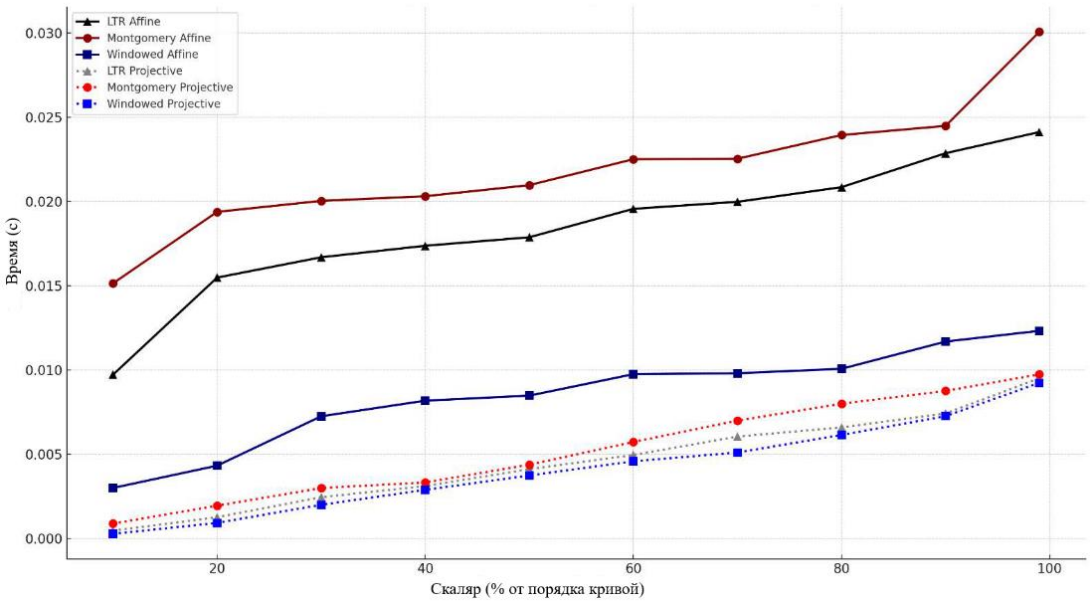


Рис.2: Требования к времени для умножения точек с использованием методов «удвоения и сложения», метода «лестница Монтгомери» и оконного метода.

Анализ подтверждает, что несмотря на высокую скорость оконного метода, его высокая потребность в памяти делает его непрактичным для устройств с ограниченными ресурсами. Метод лестница Монтгомери остаётся предпочтительным с точки зрения устойчивости к атакам по времени.

На основе выявленных ограничений предложен новый метод оптимизации ECPM, ориентированный на устройства с ограниченными ресурсами. Метод сочетает свойства циклических групп и аддитивных обратных элементов в методах удвоения и сложения, а также лестнице Монтгомери. Метод является применим к широкому спектру симметричных кривых, таких как Secp256k1, NIST P-256, Curve25519 и Edwards25519. Ниже представлен алгоритм, описывающий основу предлагаемого метода умножения точки на эллиптической кривой:

Псевдокод предлагаемого метода $(k, G, E, p)$:
если $k \leq \frac{\#E}{2}$ то
вернуть ЦГАО_метод $(k, G)$ // ЦГАО — Циклическая Группа и Аддитивный Обратный

иначе
$x = \#E - k$
$Q$ = ЦГАО_метод$(x, G)$ // Используется свойство циклической группы и аддитивного обратного
вернуть $(Q.x, p - Q.y)$ // Отразить точку, чтобы получить kG
ЦГАО_метод $(k, G)$:
Вход: $k$ — двоичное представление скаляра, $G$ — базовая точка
Выход: $Q = k \cdot G$
Q ← G
для $i$ от $m$ до 0:
если $k_i = 0$ то
$Q \leftarrow$ удвоение_точки$(Q)$
$Q \leftarrow$ сложение_точек$(Q, O)$ // $O$ — нейтральный элемент, операция для выравнивания времени
иначе
$Q \leftarrow$ удвоение_точки$(Q)$
$Q \leftarrow$ сложение_точек$(Q, G)$
вернуть $Q$

Проведён эксперимент в среде Python с реализацией предложенного метода на кривой secp256k1, используемой в среде Bitcoin. Результаты приведены на следующей диаграмме:

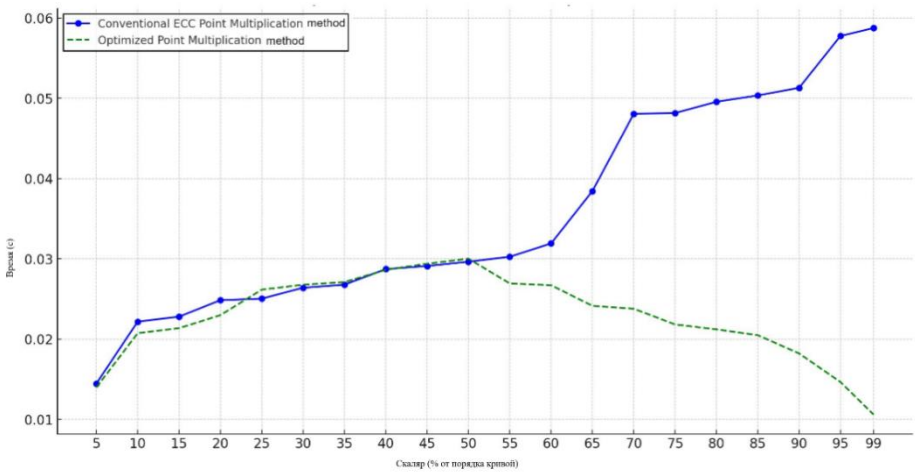


Рис. 3: Сравнительный анализ временных затрат на умножение точек на кривой Secp256k1

Предложенный метод улучшает производительность, сокращая время выполнения примерно на 74.6% – 81.9% по сравнению с традиционным методом, что существенно снижает вычислительную сложность в условиях ограниченных ресурсов.

Произведенный эксперимент демонстрирует, что предложенный метод обеспечивает значительное сокращение числа операций по сравнению с существующими традиционными методами умножения точек на эллиптической кривой, улучшая производительность без снижения криптостойкости. Сравнительный анализ показывает, что предложенный метод существенно превосходит существующие методы по времени выполнения.

Предлагаемый метод повторяет принцип Лестницы Монтгомери (удвоение и «симметричное» сложение для каждого бита), однако при бите 0 сложение выполняется с нейтральной точкой, что не требует реального сложения. Благодаря этому сохраняется постоянное время выполнения и структура, но снижаются вычислительные затраты и требования к ресурсам.

Также уровень безопасности ECC равен примерно половине длины порядка кривой, потому что задача дискретного логарифма решается быстрее с помощью алгоритма Полларда. Поэтому сокращение числа операций сложения и удвоения точек, необходимых для реализации умножения точки на эллиптической кривой, не снижает безопасность алгоритма.

Это подтверждает его высокую эффективность и практическую применимость для оптимизации операций криптографии на эллиптических кривых в условиях устройств с ограниченными ресурсами без снижения криптостойкости.

**В третьей главе** Представлены результаты второго положения, выносимого на защиту, направленного на разработку математического метода построения схемы ЭЦП на основе ECC, обеспечивающего снижение вычислительной сложности, уменьшение времени обработки, количества процессорных тактов, потребляемой памяти и нагрузки на пропускную способность канала связи для систем с ограниченными ресурсами.

Основное внимание уделено созданию математического метода, который повышает эффективность подписи без снижения криптостойкости.

Глава начинается с обзора современных исследований в области криптографии, посвящённых рискам, связанным с генерацией и использованием однократно используемого числа в алгоритмах электронной подписи, таких как Schnorr, MuSig, EdDSA и их модификациях.

Рассматриваются ключевые уязвимости, связанные с повторным использованием однократно используемого числа, недостатками случайных генераторов, а также сложностью реализации схем с доказательствами с нулевым разглашением (NIZK).

Анализируются современные подходы к устранению этих уязвимостей, включая протоколы MuSig-DN и MuSig2, которые применяют детерминированную генерацию однократно используемых чисел для повышения безопасности, однако требуют дополнительных вычислительных затрат, особенно связанных с использованием NIZK-доказательств.

Особое место в главе занимает сравнительный анализ трёх наиболее популярных алгоритмов электронной подписи (RSA, ECDSA и EdDSA) с позиций их применимости в ресурсно-ограниченных средах, результаты которого представлены на следующих диаграммах:

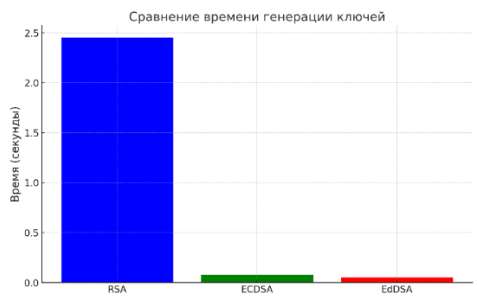


Рис. 4: Время, затраченное на генерацию ключей для RSA, ECDSA и EdDSA


Рис. 5: Потребление памяти при генерации ключей для RSA, ECDSA и EdDSA

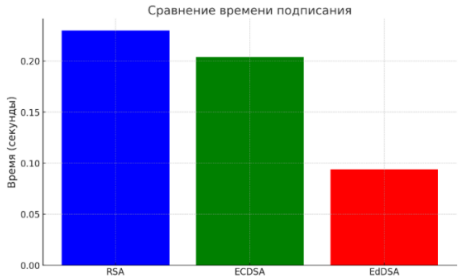


Рис. 6: Время, затраченное на процесс подписания для RSA, ECDSA и EdDSA


Рис. 7: Потребление памяти во время процесса подписания для RSA, ECDSA и EdDSA

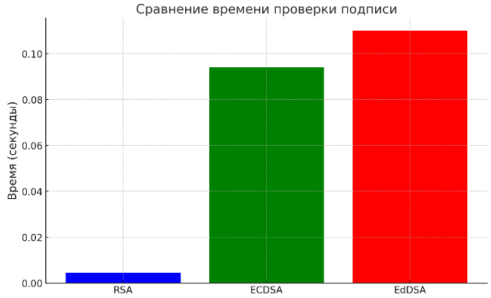


Рис. 8: Время, затраченное на проверку для RSA, ECDSA и EdDSA


Рис. 9: Потребление памяти во время проверки для RSA, ECDSA и EdDSA

Анализ показал, что RSA требует значительных объёмов оперативной памяти и имеет высокий уровень вычислительных затрат, особенно на этапах генерации ключей и подписания. Несмотря на быстрое время проверки, RSA не подходит для систем, где важна компактность и энергоэффективность.

Алгоритм ECDSA показал более сбалансированные результаты по скорости и потреблению ресурсов, однако остаётся уязвимым к атакам, связанным с повторным использованием однократно используемого числа (одной из самых опасных угроз для криптосистем данного класса). Ошибки в генерации случайных чисел могут привести к полному раскрытию закрытого ключа, как это уже происходило в известных инцидентах, включая взлом PlayStation 3 и проблемы с криптокошельками на Android.

Наиболее высокие результаты продемонстрировал алгоритм EdDSA, который обеспечивает надёжную защиту. Этот алгоритм показал наилучшее соотношение между скоростью, потреблением памяти и безопасностью, а операции подписания и проверки выполняются быстрее, чем у других алгоритмов.

На основе анализа существующих решений предложен оригинальный метод оптимизации схем электронной подписи на основе ECC. Метод базируется на детерминированной генерации приватного однократно используемого числа, исключении открытого однократно используемого числа из вычисления вызова (challenge) и внедрении проверки владения закрытым ключом через использование агрегированного открытого ключа вместо применения NIZK-доказательств. Такая конструкция позволяет полностью устранить необходимость в дополнительных раундах взаимодействия между участниками и снижает сложность протокола.

Ниже представлен алгоритм, описывающий основу предлагаемого метода ЭЦП на базе алгоритма Шнорра (одиночная и мультиподписная схемы):

I. Схема с одной подписью
Подписание сообщения $m$:

- Выбирается случайный секретный ключ $x$, где $0 < x < p$.
- Вычисляется открытый ключ $X = x \cdot g$
- Вычисляется $h = H(x)$.
- Вычисляется закрытое однократно используемое число $r = H(h \,||\, m)$.
- Вычисляется открытое однократно используемое число $R = r \cdot g$
- Вычисляется $c = H(X, m)$.
- Вычисляется $s = (r + c \cdot x) mod\ p$. Подпись: $(R, s)$. Отправить $(m, X, R, s)$.

Проверка подписи: подпись корректна только если $s \cdot g == R + c \cdot X$

II. Мультиподписная схема с детерминированным однократно используемым числом
Ключевая генерация (для каждого подписанта $i$):

- Выбрать секретный ключ $x_i$, где $0 < x_i < p$.
- Вычислить открытый ключ $X_i = x_i \cdot g$

Подписание сообщения $m$ (группа из $n$ подписантов):
Раунд 1:

1. Вычислить $L = H_{agg}(X_1 || X_2 || \ldots || X_n)$.
2. Для каждого $i \in \{1, \ldots, n\}$:

a. Вычислить $a_i = H_{\text{agg}}(L, X_i)$.

b. Вычислить агрегированный открытый ключ $\tilde{X} = \prod_{i=1}^{n} a_i \cdot X_i$. Если $\tilde{X} = a_i \cdot X_i$ (ошибка проверки), завершить процесс.

c. Вычислить $h_i = H_{\text{agg}}(x_i)$.

d. Вычислить закрытое число $r_i = H_{agg}(h_i || m)$.

e. Вычислить открытое число $R_i = r_i \cdot g$

f. Отправить $R_i$ другим подписантам и получить $R_j$ от остальных.

Раунд 2:

1. Вычислить $c = H_{\text{sig}}(\tilde{X}, m)$.
2. Для каждого $i$: $s_i = (r_i + c \cdot a_i \cdot x_i)\ mod\ p$.
3. После получения всех $s_i$ вычислить: $R = \prod_{i=1}^{n} R_i$ и $s = \sum_{i=1}^{n} s_i\ mod\ p$.
4. Подпись: $(R, s)$. Отправить $(m, R, s)$.

Проверка агрегированной подписи получателем:

1. Вычислить $L = H_{agg}(X_1 || X_2 || \ldots || X_n)$.
2. Для каждого $i \in \{1, \ldots, n\}$: $a_i = H_{\text{agg}}(L, X_i)$.
3. Вычислить $\tilde{X} = \prod_{i=1}^{n} a_i \cdot X_i$.
4. Вычислить $c = H_{\text{sig}}(\tilde{X}, m)$.
5. Проверить: $s \cdot g == R + \text{c} \cdot \tilde{X}$
6. Если равенство выполняется — подпись корректна.

В математическом обосновании метода показано, что использование хеш-функции от закрытого ключа и сообщения для генерации однократно используемого числа обеспечивает его уникальность и устойчивость к атакам, включая атаки с повторным использованием однократно используемого числа. Одновременно отказ от открытого однократно используемого числа в формировании вызова снижает вычислительную сложность процесса, что критически важно для устройств с ограниченными ресурсами.

В отличие от традиционных схем мультиподписи, требующих сложных NIZK-

доказательств для подтверждения владения закрытыми ключами, предложенный метод использует механизм проверки через агрегированный открытый ключ. Если агрегированный открытый ключ совпадает с любым из индивидуальных ключей подписантов, процесс подписания прерывается.

Для объяснения того, как предлагаемый метод защищает от основных атак, таких как атака на повторное использование однократно используемого числа (nonce reuse attack), рассмотрим данную известную уязвимость.

В ECDSA при двух различных сообщениях случайно используется одно и то же однократно используемое число $k$, злоумышленник может просто вычесть одну подпись из другой и найти значение $k$. После этого, зная $k$, параметры подписи и хэши сообщений, легко вычисляется закрытый ключ. Эта атака показывает, насколько важно каждый раз использовать уникальное однократно используемое число при создании подписи.

В предлагаемом методе однократно используемое число вычисляется детерминированно на основе приватного ключа и сообщения. Поэтому для разных сообщений всегда получаются разные значения, и злоумышленник не может использовать стандартную атаку, вычитая подписи. Даже если одно и то же сообщение подписывается дважды, подписи одинаковые и не раскрывают приватный ключ. Таким образом, проблема повторного использования однократно используемого числа полностью устранена.

Предлагаемый метод защищает не только от атаки повторного использования однократно используемого числа, но и от других угроз. Атака отмены ключа предотвращается путём проверки, что агрегированный открытый ключ не совпадает с любым из индивидуальных ключей. Атака с поддельным ключом исключена, потому что все открытые ключи проходят проверку через общий хэш. Кроме того, атаки отката виртуальной машины невозможны, так как однократно используемое число вычисляется заново из приватного ключа и сообщения и не хранится в состоянии системы, а предложенные механизмы в методе обеспечивают сохранение двухраундовой модели взаимодействия, в отличие от схем типа MuSig и MuSig-DN, которые требуют трёх и более раундов.

Проведённый сравнительный анализ и математическое моделирование подтвердили, что предложенный метод обеспечивает значительное снижение вычислительной сложности, уменьшение потребления памяти и нагрузки на пропускную способность канала связи по сравнению с традиционными схемами мультиподписи, основанными на использовании неинтерактивных доказательств с нулевым разглашением (NIZK) и открытых однократно используемых чисел. При этом предложенное решение сохраняет высокий уровень криптографической стойкости, устойчивость к атакам повторного использования однократно используемого числа, а также атакам с использованием поддельного ключа (Rogue Key Attack) и отмены ключа (Key Cancellation Attack), что делает метод особенно подходящим для применения в устройствах с ограниченными ресурсами, включая встраиваемые устройства, беспилотные платформы и IoT-системы.

Таким образом, предложенный в третьей главе метод решает ключевую проблему повышения эффективности цифровых подписей на основе ECC для устройств с ограниченными ресурсами без снижения криптостойкости и обладает высокой практической ценностью для применения в системах Интернета вещей (IoT), беспилотных транспортных системах, встраиваемых платформах и других приложениях, где критичны компактность, энергоэффективность и высокая степень защиты данных.

**В четвёртой главе** представлены результаты практической реализации и экспериментальной оценки разработанных методов оптимизации криптографии на основе эллиптических кривых (ECC) на микроконтроллере с ограниченными ресурсами Arduino ATmega2560 R3. Несмотря на жёсткие ограничения по объёму памяти и производительности (8-битная архитектура, 8 КБ SRAM, 256 КБ Flash, 16 МГц), предложенные математические и алгоритмические оптимизации позволили существенно повысить эффективность выполнения криптографических операций по сравнению с существующими методами.

Первый метод основан на использовании однородных координат и оконного метода, интегрируя свойства циклической группы точек и аддитивных обратных элементов. Основой является кривая Edwards25519, определяемая уравнением: $ax^2 + y^2 = 1 + dx^2y^2$

Метод включает следующие шаги:

1. Проверка, что количество операций умножения не превышает порядок кривой $0 \leq \tilde{s} < E$.

2. Оптимизация с использованием оконного метода и предварительного вычисления точек. Если $\tilde{s} \geq \frac{E}{2}$, товыполняетсязамена $\tilde{s}' = \tilde{s} - \frac{E}{2}$

3. Инициализация результата нейтральным элементом.

4. Для каждого окна: $Q = 2^{\omega}Q$ (выполнение $\omega$ операций удвоения), затем $Q = Q +$ Precomputed[размерокна], где Precomputed — предварительно вычисленная таблица точек, а размер окна: количество бит, обрабатываемых одновременно.

Для защиты от атак по сторонним каналам, зависящих от времени выполнения, реализован алгоритм с постоянным временем. Это достигается добавлением нейтральной точки $0G = (0:1:1)$ в таблицу предварительно вычисленных точек. Такая модификация гарантирует, что операция сложения выполняется всегда, даже если значение окна равно нулю, устраняя вариативность во времени выполнения. Дополнительно использование свойств циклической группы и аддитивных обратных элементов обеспечивает гибкость в выборе размера окна и поддерживает безопасность реализации.

Реализация предложенного метода, основанного на свойствах циклической группы, противоположного числа с учётом зависимости объёма работы, выполняемой алгоритмом, от размера входных данных, показала высокую эффективность. Проведённое исследование на микроконтроллере Atmega2560 подтвердило, что использование однородных координат в сочетании с оконным методом позволяет добиться сокращения количества тактов на 60%, снижения использования динамической памяти (SRAM) на 78.66%, а также уменьшения потребления Flash-памяти на 28.21% по сравнению с традиционными методами, при сохранении тех же входных параметров. Подробные данные показаны на диаграмме 9, которая наглядно демонстрирует улучшения ключевых метрик производительности.

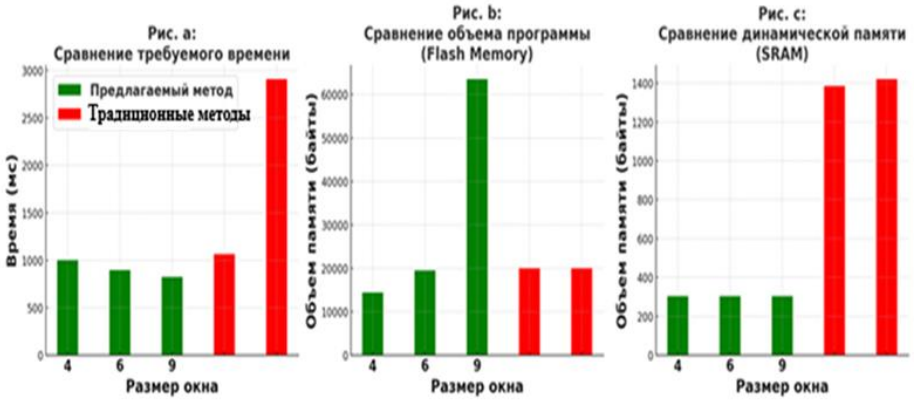


Рис. 9: Сравнение результатов (время выполнения, флеш-память и SRAM) с существующими методами

Второй метод реализован в рамках расширенной скрученной проективной системы координат, которая позволяет устранить параметр кривой $a$ в процессе удвоения. В традиционном подходе операция удвоения требует вычисления: $D = a \cdot A,$ где$a = -1(\mathrm{mod}P)$ что заменяется на более эффективную операцию: $D = P - A$, при которой вычитание в конечном поле требует меньше вычислительных ресурсов, чем умножение.

Для интеграции с оконным методом используется представление скаляра: $\tilde{s} = \sum_{i=0}^{n-1} s_i \cdot 2^{i\cdot\omega+4}$, где $s_i$ — значение окна, $\omega$ — размер окна, а смещение на 4 бита обеспечивает правильное позиционирование наиболее значимого окна.

Каждое обновление целевой точки $Q$ выполняется по формуле: $Q = (Q \cdot 2^{\omega}) + \mathrm{Precomputed}[s_i]$, обеспечивая эффективное удвоение и добавление.

Для защиты от атак по времени используется модификация массива предвычисленных точек путём добавления нейтральной точки в расширенной проективной системе координат $OG = (0:1:0:1)$, что гарантирует одинаковое выполнение операций независимо от значения окна. Это устраняет утечки по времени и обеспечивает постоянный шаблон выполнения операций.

Реализация предложенного метода на микроконтроллере Atmega2560 с использованием языка C и ассемблера в среде Arduino IDE позволила достичь сокращения времени выполнения и количества тактов на 71%, снижения использования динамической памяти (SRAM) на 80%, а также уменьшения потребления Flash-памяти на 15% по сравнению с предыдущими методами. При этом использовались те же параметры скалярного умножения и кривой, что и в традиционных решениях. Подробные данные показаны на диаграмме 10, которая наглядно демонстрирует улучшения ключевых метрик производительности.

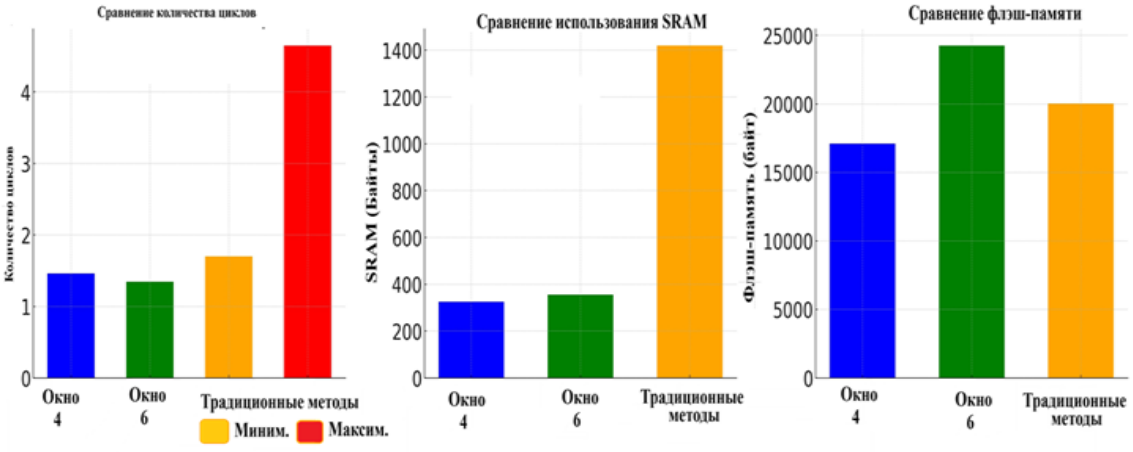


Рис. 10: Сравнение результатов (циклы, SRAM и флеш-память) с существующими методами

Интеграция указанных методов в схему электронной подписи на основе ECC с использованием расширенной проективной системы координат и оптимизированного оконного умножения с учётом зависимости объёма работы, выполняемой алгоритмом, от размера входных данных обеспечила комплексное повышение эффективности. Основные результаты реализации схемы электронной подписи на Edwards25519 на микроконтроллере Atmega2560 показали следующие улучшения: генерация ключей — сокращение количества тактов на 54% и использование SRAM на 73%; процесс создания подписи — снижение тактов на 40% и потребления SRAM более чем на 59%; проверка подписи — сокращение количества тактов на 29.59% и снижение использования SRAM на 12,01%. При использовании меньшего размера окна выигрыш по количеству тактов при проверке снизился на 6.5%. Подробные данные показаны на диаграммах 11, 12 и 13, которые наглядно демонстрируют улучшения ключевых метрик производительности. Следовательно, предложенный метод эффективно снижает вычислительную сложность скалярного умножения точки на эллиптической кривой, так как зависимость объёма работы от размера входных данных у предлагаемого метода меньше, чем у существующих алгоритмов, что делает его более эффективным при использовании одного и того же размера входных данных.

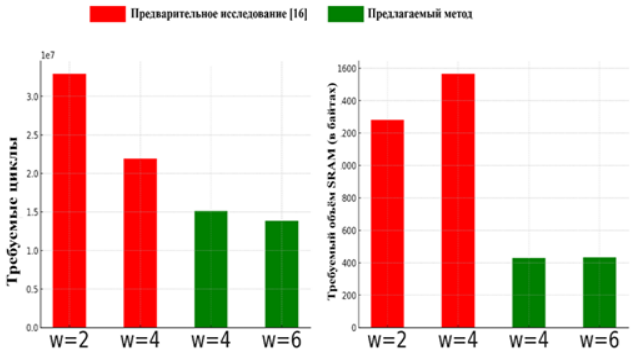


Рис 11: Генерация ключей, сравнение результатов (циклы и SRAM) с существующими методами

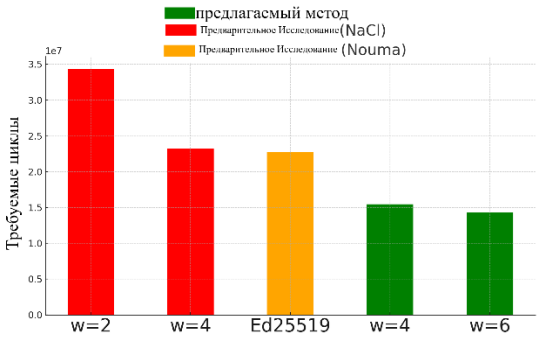


Рис 12: Создание подписи, сравнение результатов (циклы) с существующими методами

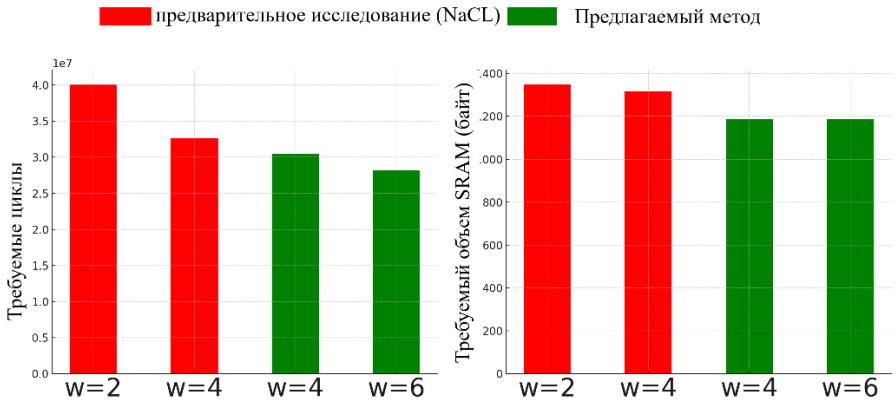


Рис 13: Проверка подписи, сравнение результатов (циклы и SRAM) с существующими методами

Полученные результаты подтверждают, что предложенные методы обеспечивают эффективную реализацию криптографии с открытым ключом на 8-битных микроконтроллерах и демонстрируют их применимость в условиях ограниченных ресурсов. Это обеспечивает значительное преимущество по сравнению с существующими методами и соответствует третьему положению, выносимому на защиту.

## ЗАКЛЮЧЕНИЕ

Поставленная в диссертационном исследовании цель по снижению вычислительной сложности электронной цифровой подписи на основе криптографии на эллиптических кривых без снижения криптостойкости, для повышения эффективности и расширения применимости данных подписей в устройствах с ограниченными ресурсами, выполнена.

Для её достижения были решены противоречия между требованиями высокой вычислительной эффективности в условиях ограниченных ресурсов и необходимостью криптографической стойкости, минимизацией объёма передаваемых данных и ограничениями энергопотребления при выполнении ресурсоёмких операций эллиптической криптографии. В рамках исследования разработаны два метода, направленные на снижение вычислительной сложности базовой операции умножения точки эллиптической кривой (ECPM) и всей схемы цифровой подписи.

Основные результаты исследования:

1. Разработан математический метод снижения количества операций сложения и удвоения точек при выполнении операции умножения точки на эллиптической кривой над симметричными эллиптическими кривыми (Secp256k1, Edwards25519) с использованием свойств циклической группы и аддитивной инверсии.

- Позволяет уменьшить зависимость объёма работы алгоритма ECPM от размера входных данных;
- Сократить число операций сложения и удвоения в ECPM, используя свойства циклической группы и аддитивной инверсии;
- Сохраняет криптографическую стойкость при снижении вычислительных затрат.

2. Разработан метод снижения вычислительной сложности самой схемы цифровой подписи, предусматривающий совмещение п. 1 с:

- детерминированной генерацией однократно используемого числа (nonce);

- исключением использования открытого значения однократно используемого числа при вычислении вызова (challenge);
- подтверждением владения приватным ключом через агрегированный публичный ключ без применения неинтерактивных доказательств с нулевым разглашением.

Метод снижает вычислительную нагрузку, уменьшает объём передаваемых данных и повышает устойчивость к атакам (Nonce Reuse Attack, Key Cancellation Attack, Rogue Key Attack, Replay Attack и др.), учитывая риски атак по сторонним каналам.

3. Выполнена программная реализация и экспериментальная верификация разработанных методов на платформе ATmega2560, характерной для устройств с ограниченными ресурсами (например, в контроллерах беспилотных систем UVS). Предложенные решения совмещают математические оптимизации ECPM и архитектурные приёмы для минимизации использования SRAM/Flash и процессорных циклов, необходимых для реализации цифровой подписи.

- Для Secp256k1 получен прирост производительности на 82% по сравнению с классическими методами;
- Для Edwards25519 (проективные координаты) сокращено количество тактов на 60%, время выполнения на 71.69%, использование SRAM до 80.6%, Flash на 28.21%;
- Для Edwards25519 (расширенные проективные координаты) сокращено количество тактов на 71%, Flash на 15%, SRAM на 80%.

Эффективность методов подтверждена при генерации ключей (сокращение тактов на 54%, SRAM на 73%), формировании подписи (такты −40%, SRAM − 59%) и проверке подписи (такты −29.59%, SRAM −12%).

Доказано, что предложенные методы обеспечивают снижение вычислительной сложности и ресурсных затрат при формировании и проверке цифровых подписей на базе ECC без потери криптостойкости, а также повышают устойчивость к ключевым видам атак (включая Nonce Reuse Attack, Key Cancellation Attack, Rogue Key Attack, Virtual Machine Rewinding Attack, Replay Attack, а также с учётом рисков Side-Channel Attack при реализации).

## СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

### Публикации в рецензируемых научных изданиях, рекомендованных ВАК

1. Сабри Н. Х., Левина А. Б. Метод умножения точек на эллиптической кривой Edwards25519 для устройств с ограниченными ресурсами // Вестник компьютерных и информационных технологий. – 2025. – Т. 22, № 4. – С. 45-51.
2. Сабри Н. Х. Реализация электронной подписи ECC в ограниченных средах // Труды учебных заведений связи. – 2025. – Т. 11, № 2. – С. 101-108.

### Публикации в изданиях, входящих в международные базы цитирования

3. Sabbry, N.H., Levina, A.B. An optimized point multiplication strategy in elliptic curve cryptography for resource-constrained devices // Mathematics. – 2024. – Т. 12, № 6. – Article 881.
4. Nawras H. Sabbry, Alla Levina. Nonce generation techniques in Schnorr multi-signatures: Exploring EdDSA-inspired approaches // AIMS Mathematics. – 2024. – Т. 9, № 8. – С. 20304-20325.
5. Nawras H. Sabbry & Alla Levina. An optimized elliptic curve digital signature strategy for resource-constrained devices. Scientific Reports. – 2025. –Т. 15. – С. 22786.
6. N. H. Sabbry and A. Levina, A Resource-Efficient Edwards25519 Point Multiplication Technique for Resource-Constrained Devices // IEEE Access. – 2025. – С. 1-1.

### Свидетельства о результатах интеллектуальной деятельности

7. Свидетельство о государственной регистрации программы для ЭВМ № 2025681064 Российская Федерация. Программа для оптимизации алгоритмов электронной подписи устройств с ограниченными ресурсами // А.Б. Левина, Н.Х. Сабри; правообладатель Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)». № 2025680076; заявл. 02.07.2025; опубл. 11.08.2025.
8. Свидетельство о государственной регистрации программы для ЭВМ № 2025681382 Российская Федерация. Программа для оптимизации умножения точек эллиптической кривой устройств с ограниченными ресурсами // А.Б. Левина, Н.Х. Сабри; правообладатель Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)». № 2025680193; заявл. 02.07.2025; опубл. 13.08.2025.

### Публикации в других изданиях

9. Сабри Н. Х. Цифровые подписи в ограниченных средах: Сравнительный анализ безопасности RSA, ECDSA и EdDSA // Preprints.ru. – 2025. – 28 июля. – DOI: 10.24108/preprints-3113617.
10. Сабри Н. Х. Оптимизированный метод цифровой подписи на эллиптических кривых для устройств с ограниченными ресурсами // Preprints.ru. – 2025. – 22 июля. – DOI: 10.24108/preprints-3113629.
11. N. H. Sabbry and A. Levina, Elliptic Curve Cryptography on constrained devices: A comparative study of point multiplication methods // *2024 13th Mediterranean Conference on Embedded Computing (MECO)*. Budva, Montenegro. IEEE, 2024. P. 1-5.
12. Sabbry N. H. Digital Signatures in Constrained Environments: A Comparative Security and Performance Analysis of RSA, ECDSA, and EdDSA // Intelligent Systems. INTELS 2024. Communications in Computer and Information Science. Vol. 2604. – Cham: Springer, 2026. – P. 170-181.

Подписано в печать 05.02.2026. Формат 60×84 1/16.
1,0 а.л. Тираж 100 экз.

Отпечатано в СПбГУТ, 193232, Санкт-Петербург, пр. Большевиков, д. 22, корп. 1