Анализ алгоритмов обмена ключами над эллиптическими кривыми

Кытманов А.А., Ильин Г.С., Пихтилькова О.А., Пронина Е.В.

РТУ МИРЭА

2025

Цели и задачи

Цель работы

Сравнительный анализ протоколов обмена ключами на эллиптических кривых:

- Классический ECDH (Диффи-Хеллман для двух участников)
- Протокол Бурместера-Десмедта (BD) для групповой коммуникации

Критерии сравнения

- Криптографическая стойкость
- Вычислительная эффективность
- Коммуникационная эффективность
- Функциональные возможности

Методология и актуальность

Методология

Количественные расчёты для группы из 5 участников на кривой P-256

Актуальность темы

- Взрывной рост IoT и распределенных систем
- Угроза со стороны квантовых вычислений
- Требования к устройствам с ограниченными ресурсами
- Недостатки классических систем (RSA, DH)

Преимущества ECC

Ключевые преимущества

- Высокая стойкость: 256 бит ECC $\approx$ 3072 бит RSA
- Меньшие вычислительные затраты
- Экономия памяти и пропускной способности
- Идеально для мобильных устройств и IoT

ECDH как стандарт

Основа TLS, SSH, защищенных мессенджеров

Проблема групповой коммуникации

Требования к групповым протоколам

- Эффективность
- Идеальная прямая секретность (PFS)
- Стойкость к атакам
- Единый общий ключ для группы

Неэффективность наивных решений

- Квадратичный рост числа соединений
- Множество ключей у каждого участника

Математические основы ЭК

Определение эллиптической кривой

$E : y^2 = x^3 + ax + b$, где $\Delta = -16(4a^3 + 27b^2) \neq 0$

Групповой закон

- Нейтральный элемент O
- Сложение точек: $P + Q = R$
- Скалярное умножение: $[k]P$

Теорема Хассе-Вейля

$|N - (p + 1)| \leq 2\sqrt{p}$, где N — число точек

ECDLP — основа безопасности

Проблема дискретного логарифма

Для $Q = [k]G$ найти $k \in [0, q-1]$

Стойкость ECDLP

- Сложность лучших алгоритмов: $O(\sqrt{q})$
- Экспоненциальная сложность
- Короткие ключи при высокой стойкости

Протокол ECDH: Основы (1/2)

Общие параметры

- Кривая E над F_p
- Циклическая подгруппа $\langle G \rangle$ порядка q
- Базовая точка G

Этапы протокола

Генерация ключей:

- Алиса: $d_a \in [1, q-1]$, $Q_a = d_a G$
- Боб: $d_b \in [1, q-1]$, $Q_b = d_b G$

Обмен открытыми ключами:

- $Q_a \rightarrow$ Боб, $Q_b \rightarrow$ Алиса

Протокол ECDH: Вычисление секрета (2/2)

Вычисление общего секрета

Алиса: $S = d_a \cdot Q_b$
Боб: $S = d_b \cdot Q_a$
Результат: $S = (d_a \cdot d_b) \cdot G$

Безопасность

Основана на сложности ECDLP

Свойства

- Идеальная PFS (при одноразовых ключах)
- Уязвимость к MitM
- 1 раунд, 2 скалярных умножения

Протокол BD: Общие сведения (1/3)

Цель протокола

Групповой обмен ключами для $n \geq 3$ участников

Параметры

- Группа из n участников: $P_1, \ldots, P_n$
- Кривая (E, F_p, G, q)

Основная идея

Двухраундовый протокол для получения общего ключа:

$$K = \left(\sum_{i=1}^{n} x_i \cdot x_{i-1} \right) \cdot G$$

Протокол BD: Этапы выполнения (2/3)

Инициализация

Каждый P_i: $x_i \in [1, q-1]$, $X_i = x_i \cdot G$

Раунд 1: Обмен ключами

Рассылка X_i всем участникам

Раунд 2: Промежуточные значения

- $Z_{ij} = x_i \cdot X_j = (x_i \cdot x_j) \cdot G$
- $Y_i = Z_{i(i-1)} - Z_{i(i+1)}$ (индексы по mod n)
- Рассылка Y_i всем

Протокол BD: Вычисление ключа (3/3)

Общий групповой ключ

Каждый P_i вычисляет:

$$K_i = x_i \cdot X_{i-1} + \sum_{j=1}^{n-1} (n-j) \cdot Y_{i+j}$$

Корректность

Все K_i равны: $K = \left(\sum_{i=1}^{n} x_i \cdot x_{i-1}\right) \cdot G$

Свойства

- Единый групповой ключ
- Идеальная PFS
- 2 раунда, $(n+1)$ скалярных умножений

Сравнение DH и ECDH

Протокол	Параметры	Размер p	Размер g	Данные	Безопасность
DH (Classical)					
DH	ffdhe2048	2048 бит	2048 бит	512 Б	112 бит
DH	ffdhe2048	3072 бит	3072 бит	768 Б	128 бит
DH	ffdhe2048	4096 бит	4096 бит	1024 Б	152 бит
ECDH (Elliptic Curve)					
ECDH	secp256r1	256 бит	512 бит	96 Б	128 бит
ECDH	X25519	255 бит	255 бит	64 Б	128 бит
ECDH	secp384r1	384 бит	768 бит	144 Б	192 бит
ECDH	X448	448 бит	448 бит	112 Б	224 бит

Анализ сравнения DH и ECDH

Эффективность использования битов

- DH: 5.5% (112 бит при 2048 битах)
- ECDH: 50% (128 бит при 256 битах)

Объем передаваемых данных

- DH (128 бит): 768 байт
- ECDH (128 бит): 96 байт (в 8 раз меньше)
- X25519: 64 байта при 128 битах

Преимущества ECDH

- Экономия трафика для веб-серверов
- Ускорение соединения
- Экономия энергии для мобильных устройств

Сравнение ECDH и BD (n=5)

№	Параметр	ECDH	BD
1	Вычислит. нагрузка	4 SM	6 SM
2	Количество раундов	1	2
3	Сообщений	20	50
4	Объём данных	1280 Б	3200 Б
5	Ключевой результат	4 парных ключа	1 групповой ключ
6	Управление ключами	Сложное	Простое
7	PFS	Да (если новые)	Да
8	Уязвимость к MitM	Да	Да

Примечание

SM — скалярное умножение

Выводы сравнения ECDH и BD

Фундаментальное различие

- **ECDH**: для парных каналов ("один-на-один")
- **BD**: для группового пространства ("многие-ко-многим")

Компромисс

- **ECDH**: лучше по количественным метрикам
- **BD**: лучше по качественным характеристикам

Общие ограничения

- Уязвимость к MitM
- Требуют аутентификации
- Основаны на сложности ECDLP

Рекомендации по выбору

Выбирать ECDH, если:

- Нужны индивидуальные защищённые каналы
- Скорость установления критична
- Ресурсы ограничены
- Группа небольшая и фиксированная

Выбирать BD, если:

- Требуется групповое шифрование
- Удобство важнее оптимизации
- Состав группы динамический
- Готовы к большей нагрузке

Перспективы и заключение

Перспективы

- Гибридные подходы для больших групп
- Использование BD внутри подгрупп
- Иерархические структуры

Заключение

- ECDH — фундаментальный инструмент для парного взаимодействия
- BD — специализированный механизм для групповой безопасности
- Выбор определяется архитектурными требованиями

Спасибо за внимание!

Вопросы?