ЕЛІПТИЧНІ КРИВІ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №1
"Реалізація арифметики на еліптичних кривих"

Недождій Максим, Буржимський Ростислав

ФІ-42мн

1 Мета роботи

Отримання практичних навичок програмної реалізації арфиметики на еліптичних кривих, закріплення теоретичного матеріалу, отриманого на лекційних заняттях.

ВАРІАНТ 3

2 Хід роботи

Використовували бібліотеку для роботи з великими числами. Реалізували класи точки еліптичної кривої та еліптичної кривої, реалізували операції додаваання, подвоєння точки, скалярний добуток сходами Монтгомері. Реалізували операції перевірки належності точки кривій та переведення афінних у проєктивні координати та навпаки. Реалізували пошук символу Лежандра. Реалізували алгоритм Тонеллі-Шенкса для розв'язку квадратного кореня за модулем, який використовуємо для пошуку відповідного y для випадково згенерованого x на еліптичній кривій.

Час роботи функцій:

Заміри робились для операцій на P-256 згідно варіанту. Час на виконання операцій взято середній для 1000 випадкових точок.

Функція	Час роботи
Перевірка належності	96.689 мікросекунд
Подвоєння	23.594 мікросекунд
Додавання	25.355 мікросекунд
Скалярний добуток	19.147 мілісекунд

3 Труднощі і подолання

Найскладніше було зібратись докупи після роботи, сісти і почати робити лаби, іншою трудністю було зрозуміти навіщо Ростиславу Rust, і як його використовувати.

У реалізації виникли проблеми з алгоритмом Тонеллі-Шенкса, які були згодом вирішені. Також під час роботи з сходинками Монтгомері певна неточність у псевдокоді ускладнила реалізацію.

4 Висновки

Арифметика на еліптичних кривих працює достатньо швидко на великих числах, а самі алгоритми не дуже сильно відрізняються від більш звичних нам структур. Лабораторна робота допомогла освіжити знання з еліптичних кривих і трошки їх поколупати.