БФУ им. И. Канта – Компьютерный практикум по криптографии на эллиптических кривых

Преподаватель С. Новоселов Осень 2026

Лабораторная работа № 1

Опубликована **01.09.2026**

Дедлайн **15.09.2026**

Задание 1

Разработать программу в системе компьютерной алгебры Sage, реализующую следующие функции:

1. `jInvariant`(a_1, a_2, a_3, a_4, a_6), где a_1, a_2, a_3, a_4, a_6 – коэффициенты кривой, заданной уравнением Вейерштрасса. Если кривая является эллиптической, функция возвращает j-инвариант кривой, иначе сообщение о том, что кривая сингулярна.

2. `randIsomorphic`($a_1 = 0$, $a_2 = 0$, $a_3 = 0$, $a_4 = 0$, $a_6 = 0$), где a_1, a_2, a_3, a_4, a_6, a, b – коэффициенты эллиптической кривой E_1 в общем случае, или в случае $char(K) \neq 2, 3$. Функция возвращает коэффициенты кривой E_2, изоморфной E_1 над $\mathbb{Q}$ путём случайного выбора параметров (u, r, s, t). Если коэффициенты a_1, a_2, a_3, a_4, a_6 задают сингулярную кривую, функция терминирует с соответствующим сообщением.

3. `isIsomorphic`(a_1, a_2, a_3, a_4, a_6, $\_a_1$, $\_a_2$, $\_a_3$, $\_a_4$, $\_a_6$, p), где a_1, a_2, a_3, a_4, a_6 – коэффициенты эллиптической кривой E_1, $\_a_1$, $\_a_2$, $\_a_3$, $\_a_4$, $\_a_6$ – коэффициенты эллиптической кривой E_2, p – простое число (означает кривые заданы над $\mathbb{F}_p$) или 0 (кривые заданы над $\mathbb{Q}$). Функция определяет, являются ли кривые изоморфными над $\mathbb{F}_p$ (или $\mathbb{Q}$), и возвращает одно из значений $\in$ {isomorphic, non-isomorphic}. Если коэффициенты a_1, a_2, a_3, a_4, a_6 или $\_a_1$, $\_a_2$, $\_a_3$, $\_a_4$, $\_a_6$ задают сингулярную кривую, функция терминирует с соответствующим сообщением.

4. `findExtension`(a_1, a_2, a_3, a_4, a_6, $\_a_1$, $\_a_2$, $\_a_3$, $\_a_4$, $\_a_6$, p), коэффициенты эллиптической кривой E_1, $\_a_1$, $\_a_2$, $\_a_3$, $\_a_4$, $\_a_6$ – коэффициенты эллиптической кривой E_2, заданные над $\mathbb{F}_p$ (p интерпретировать аналогично предыдущей функции).Функция определяет, над каким полем кривые $E_1 \simeq E_2$ и возвращает степень расширения этого поля над $\mathbb{F}_p$. Если коэффициенты a_1, a_2, a_3, a_4, a_6 или $\_a_1$, $\_a_2$, $\_a_3$, $\_a_4$, $\_a_6$ задают сингулярную кривую, функция терминирует с соответствующим сообщением.

Задание 2

Разработать программу в Sage, проверяющую для кривой над полем $\mathbb{F}_{p^6}$ возможность изоморфного преобразования в форму Шолтена (Scholten): $y^2 = ax^3 + bx^2 + b^{p^3}x + a^{p^3}$. Если такое преобразование существует, вывести его в явном виде в виде коэффициентов (u, r, s, t), задающих изоморфизм.

Кривые над полем $\mathbb{F}_{p^6}$ используются в классической криптографии на билинейных отображениях в доказательствах с нулевым разглашением (основное приложение – криптовалюты). Кривые в форме Шолтена уязвимы к атакам с помощью накрытий [1] и таким образом мы проверяем уязвимость кривой к атаке.

Пример кривой, которая приводится в форму Шолтена:

- $E : y^2 = x^3 + (6\alpha^5 + 4\alpha^4 + 9\alpha^3 + 10\alpha^2 + 4)x + (5\alpha^5 + 8\alpha^4 + \alpha^2 + 10\alpha + 7)$
- $\mathbb{F}_{11^6} \simeq \mathbb{F}_{11}[\alpha] / \langle \alpha^6 + 3\alpha^4 + 4\alpha^3 + 6\alpha^2 + 7\alpha + 2 \rangle$

Требования к сдаче

- Исходный код должен содержать комментарии к каждой из функций с описанием входных и выходных параметров
- Лабораторную следует выполнять модификацией файла с тестами, заменяя строку
  `# your code here.`
  на код, реализующий функцию.
- Функции должны работать на всех примерах, что проверяется запуском команды:
  `sage -t file_with_tests.sage`
- Студент должен понимать, что он написал, зачем, а также ответить на теоретические вопросы по лекции.

Список литературы

[1] Joux, A., Vitse, V.: Cover and decomposition index calculus on elliptic curves made practical: Application to a previously unreachable curve over. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 9–26. Springer (2012)