УДК 519.515

В.В. Драченко
М.А. Фурман

ДОСЛІДЖЕННЯ РОЗБІЖНИХ ПАРАБОЛ (ЕЛІПТИЧНИХ ФУНКЦІЙ)

Вінницький національний технічний університет

Анотація

Досліджуються алгебраїчні кубічні рівняння ліній, зокрема один випадок рівняння ліній, що називаються еліптичними, які використовуються у кодуванні інформації.

Ключові слова: алгебраїчні кубічні рівняння ліній, еліптичні функції, кодування.

Abstract

Algebraic cubic line equations are investigated, in particular one case of line equations called ellipticals, which are used in information encoding.

Key words: algebraic cubic equations of lines, elliptic functions, coding.

Вступ

В останні роки в криптографії інтенсивно почали використовувати еліптичні криві (ЕК). Еліптична криптографія – це розділ криптографії, який вивчає асиметричні криптосистеми, що використовують еліптичні криві в кінцевих полях [2]

Еліптичні криві – це математичні об'єкти, які математики вивчають, починаючи з 17 ст. Слід зазначити, що саме теорія еліптичних кривих була використана Ендрю Уайлзом для доведення великої теореми Ферма.

Еліптичною кривою на деякій множині K називають сукупність точок (*x, y*), де *x, y* ∈ *K* і задовольняють рівняння:

$$y^2 = x^3 + ax + b$$

Є також загальний вигляд рівняння еліптичних кривих над довільним кільцем:

$$y^2 + a_1xy + a_3y = x^3 + a_4x^2 + a_5x + a_6 \qquad (2)$$

яке в кільці *K* характеристики ≠2 можна записати у вигляді $y^2 = x^3 + ax^2 + bx + c$ (або $y^2 = x^3 + ax + b$, коли характеристика >3).

Можемо переписати попередні рівняння у вигляді *F(x,y)*=0. В цих випадках *F(x,y)* буде мати вигляд: $F(x, y) = y^2 - x^3 - ax - b$ (або $F(x, y) = y^2 - x^3 - ax^2 - bx - c$ і т.д.). Будемо говорити, що точку, яка лежить на еліптичній кривій, називають *неособливою* (або *гладкою*), якщо щонайменше одна з часткових похідних $\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}$ у цій точці набуває значення, відмінного від нуля.

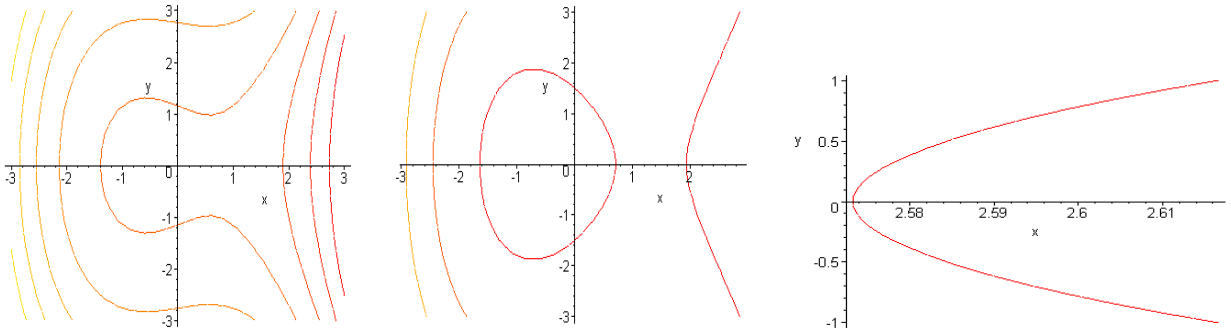

Рисунок 1. Еліптичні функції

Програмна реалізація відображає можливість «прозорого» використання системи у разі передавання даних в Інтернет-застосуваннях. Саме завдяки властивостям та складності

вирішення проблеми дискретного логарифма криптосистеми з еліптичними кривими запропоновані для задач обміну інформацією через відкриті інформаційні структури, а сам алгоритм вже запропонований як стандарт шифрування. Криптосистеми з еліптичними кривими також можна розглядати як одну з альтернатив майбутнього державного стандарту щодо захисту інформації.

Висновки

Еліптичні криві останнім часом щораз частіше використовують у криптографії. Причиною цього є те, що еліптичні криві над скінченними полями утворюють скінченні групи, які, навіть коли великі, легко піддаються арифметичним операціям завдяки багатій структурі Однією з проблем криптографічного застосування еліптичних кривих є вибір надійної випадкової кривої. Вирішення цієї проблеми визначає стійкість результуючої криптосистеми. Процес формування надійної випадкової кривої складається з декількох етапів.Для забезпечення високого рівня захищеності криптографічних систем на еліптичних кривих необхідно певних вимог.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.Завало С.Т. Курс алгебри. – К.:Вища школа, 1985 – 503с.
2.Мишина А.П., Проскуряков И.В. Высшая алгебра. М., 1984.
3. Смарт Н. Криптография / Н. Смарт. – К.: Техносфера, 2005. – 528 с.
4. Клочко В.І. Лінійна алгебра: навч. посібник / В.І. Клочко, В.П. Литвинюк –Вінниця: ВНТУ, 2007.– 126 с.
5. Михалевич В.М. Maple. Комп’ютерна підтримка курсу вищої математики в технічному вузі. Частина 1. Лінійна й векторна алгебра. Аналітична геометрія. Навч. посібник / В.М. Михалевич. – Вінниця: ВНТУ, 2004. – 111 с.
6. Edwards H.M. A normal form for elliptic curves. Bulletin of the American Mathematical Society, Volume 44, Number 3, July 2007, Pages 393-422.
7. Миллер В. Использование эллиптических кривых в криптографии .: -1986.

Науковий керівник ***Віталій Іванович Клочко*** – доктор педагогічних наук, професор кафедри вищої математики, Вінницький національний технічний університет, м. Вінниця, e-mail: klochko@vntu.edu.ua;
Владислав Володимирович Драченко – студент групи СП-19б, факультет інформаційних технологій і комп’ютерної інженерії, Вінницький національний технічний університет, м. Вінниця;
Максим Андрійович Фурман– студент групи СП-19б, факультет інформаційних технологій і комп’ютерної інженерії, Вінницький національний технічний університет, м. Вінниця;

Klochko Vitaliy I. – Dr. Sc. (Eng), Professor of mathematics, Vinnytsia National Technical University, Vinnytsia;
Drachenko VladislavV. – D Vinnytsia National Technical University, Vinnytsia.
Furman Maxim A. – D Vinnytsia National Technical University, Vinnytsia.