УДК 517.91:004.42

Д. О. Кирик
Н. Б. Дубова

«Розробка програмного комплексу для візуалізації та аналізу еліптичних кривих у формах Монтгомері та Едвардса»

Вінницький національний технічний університет

Анотація

Реалізований програмний комплекс є повноцінним навчально-дослідним інструментом. Він наочно демонструє, як абстрактні алгебраїчні структури перетворюються на реальні криптографічні механізми. Програма доводить, що вибір форми кривої (Монтгомері чи Едвардса) залежить від конкретної інженерної задачі, хоча математично вони залишаються еквівалентними.

Ключові слова: Еліптичні криві, крива Монтгомері, скручена крива Едвардса, біраціональна еквівалентність, криптографія з відкритим ключем, візуалізація, програмний комплекс, комп'ютерне моделювання, [1] прикладна криптологія, криптографія на еліптичних кривих, [2] факоризація, метод Полларда.

Abstract

The implemented software package is a full-fledged educational and research tool. It clearly demonstrates how abstract algebraic structures are transformed into real cryptographic mechanisms. The program proves that the choice of curve shape (Montgomery or Edwards) depends on the specific engineering problem, although mathematically they remain equivalent.

Keywords: Elliptic curves, Montgomery curve, twisted Edwards curve, birational equivalence, public-key cryptography, visualization, software package, computer modeling, [1] applied cryptology, elliptic curve cryptography, [2] factorization, Pollard's method.

Вступ

Дана задача є ключовою для розуміння того, як працюють сучасні протоколи безпеки, такі як **Curve25519** (використовується в WhatsApp, Signal, Tor) та **Ed25519** (для цифрових підписів). В основі програми лежить механізм побудови неявних функцій та обчислення біраціональної еквівалентності між різними алгебраїчними формами.

У програмі реалізовано дві основні моделі еліптичних кривих та математичний зв'язок між ними.

Крива Монтгомері

Визначається рівнянням:

$$\mathrm{B}y^2 = x^3 + \mathrm{A}x^2 + \mathrm{x} \tag{1}$$

Ці криві оптимізовані для швидкого скалярного множення точок (алгоритм Montgomery Ladder), що робить їх ідеальними для обміну ключами.

Скручена крива Едварса

Визначається рівнянням:

$$x^2 + y^2 = 1 + \mathrm{d}x^2y^2 \tag{2}$$

Вони мають властивість "повних формул додавання", що робить програмні реалізації стійкими до атак через сторонні канали (side-channel attacks).

Біраціональна еквівалентність

Найскладніша частина програми доводить, що ці дві форми є ізоморфними. Показник x та y на кривій Едвардса можна отримати з координат (u, v) кривої Монтгомері за формулами:

$$x = u/v \tag{3}$$

$$y = u - 1/u + 1 \tag{4}$$

Основні функції програми

Програма побудована за принципом модульності, де кожна функція відповідає за свій математичний етап.

1. **Функція _init_plot_layout()**: Створює універсальний контейнер для графіків, забезпечуючи динамічне оновлення інтерфейсу без мерехтіння.
2. **Методи plot_mont() та plot_edw()**: Виконують генерацію координатної сітки за допомогою np.ogrid та розраховують значення функцій у кожній точці простору.
3. **Функція _render_canvas()**: Виконує фінальну побудову графіка, налаштовує колірну схему (неонові лінії на темному фоні) та інтегрує об'єкт Figure у вікно програми.
4. **Функція calc()**: Реалізує інтерактивний обчислювач перетворення координат, що дозволяє користувачу перевірити математичний зв'язок між кривими в реальному часі.

```
import customtkinter as ctk
import numpy as np
import matplotlib.pyplot as plt
from matplotlib.backends.backend_tkagg import FigureCanvasTkAgg
from matplotlib.figure import Figure

# Налаштування стилю інтерфейсу
ctk.set_appearance_mode("dark")
ctk.set_default_color_theme("blue")


class ECCLaboratory(ctk.CTk):
    def __init__(self):
        super().__init__()

        self.title("Montgomery & Edwards Curves")
        self.geometry("1100x700")

        # Створення сітки вікна
        self.grid_columnconfigure(1, weight=1)
        self.grid_rowconfigure(0, weight=1)

        # --- Бокова панель (Sidebar) ---
        self.sidebar_frame = ctk.CTkFrame(self, width=200, corner_radius=0)
        self.sidebar_frame.grid(row=0, column=0, sticky="nsew")

        self.logo_label = ctk.CTkLabel(self.sidebar_frame, text="Montgomery \n&\n Edwards Curves",
font=ctk.CTkFont(size=22, weight="bold"))
        self.logo_label.pack(padx=20, pady=(20, 30))

        self.btn_mont = ctk.CTkButton(self.sidebar_frame, text="Крива Монтгомері",
command=self.show_montgomery)
        self.btn_mont.pack(padx=20, pady=10)

        self.btn_edw = ctk.CTkButton(self.sidebar_frame, text="Крива Едвардса",
command=self.show_edwards)
        self.btn_edw.pack(padx=20, pady=10)
```

```
        self.btn_map = ctk.CTkButton(self.sidebar_frame, text="Відображення точок",
command=self.show_mapping)
        self.btn_map.pack(padx=20, pady=10)

        self.btn_exit = ctk.CTkButton(self.sidebar_frame, text="Вийти", fg_color="#cc3333",
hover_color="#992222",
                                      command=self.quit)
        self.btn_exit.pack(padx=20, pady=(450, 20))
```

Алгоритм програми

Програма виконує обчислення та візуалізацію покроково.

Крок 1. Введення вхідних даних

Користувач обирає тип кривої та вводить параметри (наприклад, A та B для Монтгомері). Програма автоматично перевіряє коректність введених даних.

Крок 2. Генерація обчислювального простору

Обчислюється двовимірна область значень:

$$(x, y) \in [-L, L] \times [-H, H] \tag{5}$$

Використовується щільність у 500 точок на кожну вісь для забезпечення високої плавності кривої.

Крок 3. Розрахунок неявної функції

Програма обчислює матрицю значень Z, де:

$$Z_{i,j} = f(x_i, y_j) \tag{6}$$

де f(x, y) = 0 — цільове рівняння кривої.

Крок 4. Побудова ізоліній (Contouring)

Алгоритм знаходить усі пари точок, де функція змінює знак, і проводить через них плавну лінію. Це дозволяє коректно відобразити складні розриви та "краплі", характерні для еліптичних кривих.

Крок 5. Відображення та взаємодія

Готовий графік виводиться на екран. Користувач може перейти до розділу "Відображення точок", ввести координати u, v та миттєво отримати їх відповідники на еквівалентній кривій Едвардса.

Результати роботи програми

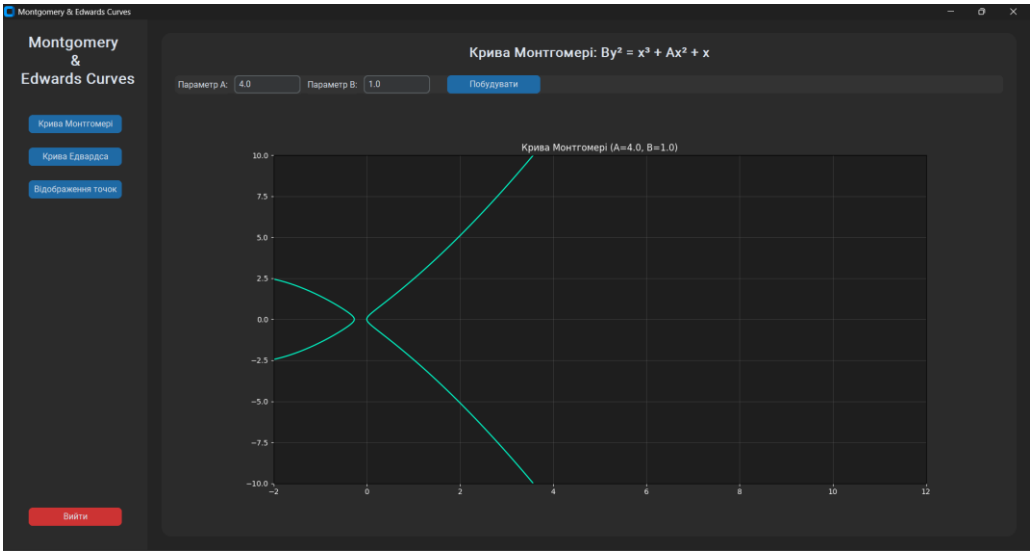

Рис.1: Приклад побудови графіку кривої Монтгомері.

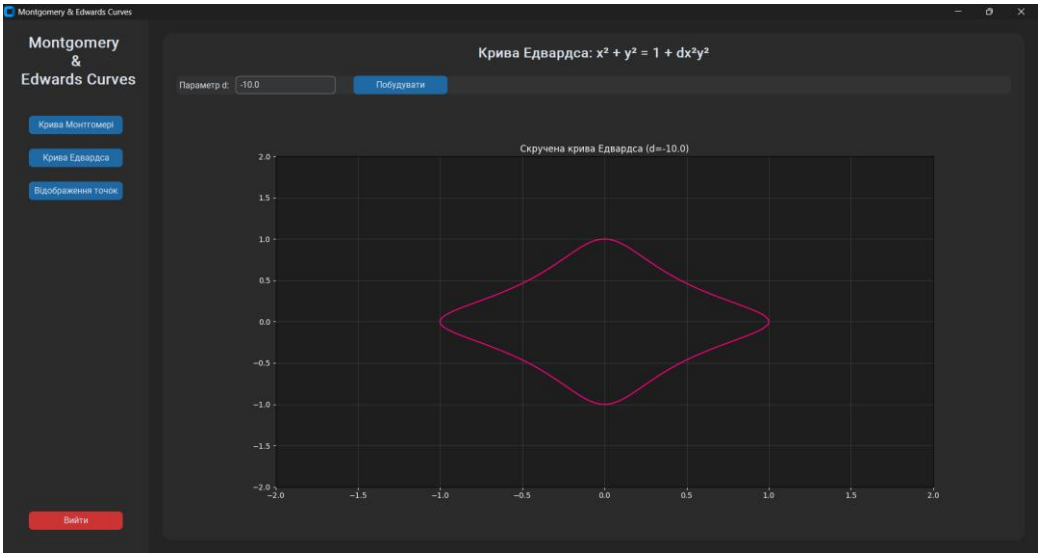

Рис.2: Приклад побудови графіку кривої Едварса.

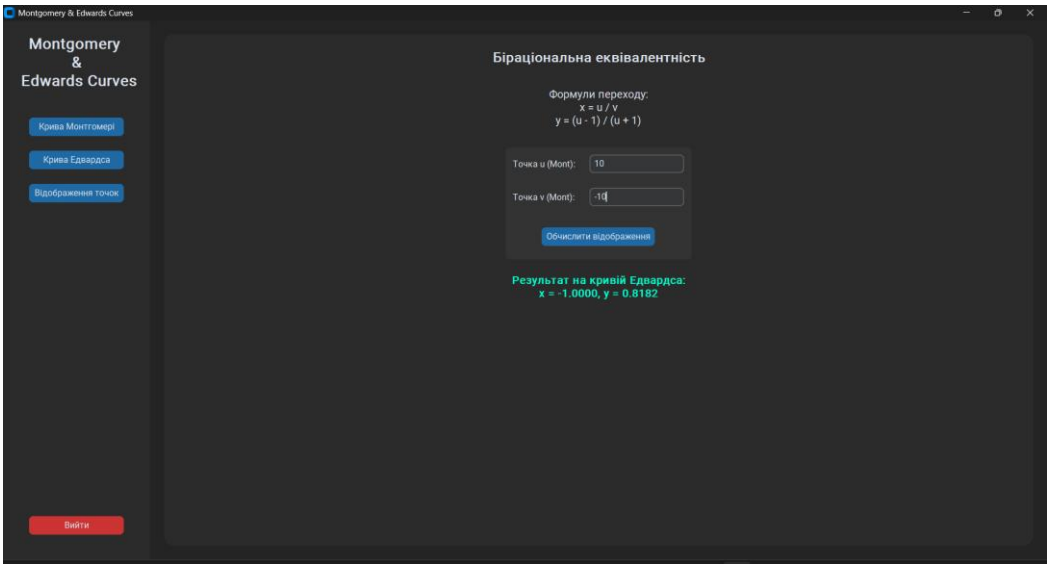

Рис.3: Приклад обчислення біраціональної еквівалентності.

Висновок

Програмний комплекс розроблений для візуалізації та дослідження геометричних властивостей еліптичних кривих (ECC), які є фундаментом сучасної криптографії з відкритим ключем. Програмний комплекс дозволяє працювати з двома найбільш ефективними формами кривих: Монтгомері та Едвардса.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. **Горбенко І. Д., Горбенко Ю. І.** Прикладна криптологія : підручник. — Харків : Форт, 2012. — 868 с.
2. **Montgomery P. L.** Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 1987. Vol. 48, No. 177. P. 243–264.
3. **Bernstein D. J., Birkner P., Joye M., Lange T., Peters C.** Twisted Edwards Curves. *Progress in Cryptology – AFRICACRYPT 2008*. Lecture Notes in Computer Science, vol. 5023. Springer, Berlin, Heidelberg. P. 389–405.
4. **Hankerson D., Menezes A., Vanstone S.** *Guide to Elliptic Curve Cryptography*. — New York : Springer-Verlag, 2004. — 312 p.

Кирик Дар'я Олександрівна *– студентка факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, Хмельницьке шосе, 95, e-mail: daruakuruk@gmail.com*
Дубова Надія Борисівна *– старший викладач, кафедра вищої математики, Вінницький національний технічний університет, м. Вінниця, Хмельницьке шосе, 95, e-mail: dubova_n_b@vntu.edu.ua*

Kyryk Daria O. *– student of the Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Khmelnytske Shosse, 95, e-mail: daruakuruk@gmail.com*
Dubova Nadiya B. *– Senior Lecturer, Department of Higher Mathematics, Vinnytsia National Technical University, Vinnytsia, Khmelnytske Shosse, 95, e-mail: dubova_n_b@vntu.edu.ua*