УДК 004.7
Лізунов С.І.[1]
Вовкостріл А.І.[2]
[1] канд. техн. наук, професор ЗНТУ
[2] студентка магістратури ЗНТУ

# ПОСТКВАНТОВА КРИПТОГРАФІЯ. МАЙБУТНЄ ЕЛІПТИЧНИХ КРИВИХ

Крім своїй первозданності, криптографічні алгоритм цікаві тим, що незважаючи на те, що можуть застарівати "складні" завдання, що лежать в основі його безпеки, їх можна успішно замінювати новими. Спочатку це була задача дискретного логарифмування в мультиплікативної групі кінцевого поля (Discrete Logarithm Problem, скор. - DLP), зараз на практиці широко використовується задача дискретного логарифмування в групі точок еліптичної кривої (Elliptic Curve DLP - ECDLP) [1]. У майбутньому передбачається використовувати інші "складні" завдання, які будуть мати експонентну складність не тільки на класичному, а й на квантовому комп'ютері. Вони називаються постквантовими. Однією з таких задач є задача знаходження ізогенії між еліптичними кривими.

Ізогенія - це раціональне відображення, що переводить точки однієї еліптичної кривої в точки ізогенної кривої, залишаючи нерухомою нескінченно віддалену точку. Нехай маємо дві ізогенні еліптичні криві $E_1$ і $E_2$. Ізогенними вони називаються тоді, коли задані над одним полем і мають однакове число точок.

Ядром ізогенії називається безліч точок на кривій $E_1$, які переходять в нескінченно віддалену точку кривої $E_2$. Для кожної ізогенії існує єдина дуальна ізогенія, що виконує зворотне перетворення. Тобто, якщо ізогенія має наступний вигляд $\varphi: \mathrm{E}_1 \to \mathrm{E}_2$, то дуальна до неї $\hat{\varphi}: \mathrm{E}_2 \to \mathrm{E}_1$.

Якщо перемножити ізогенію і дуальну до неї, отримаємо точку кривої $E_2$ помножену на ціле число *l*, яку називають ступенем ізогенії. Ізогенії простих ступенів можуть задавати перестановки на безлічі *j*-інваріантів ізогенних кривих. Послідовне накладення графів ізогенних еліптичних кривих дозволяє отримати зірку ізогенних кривих, як на малюнку нижче [2].

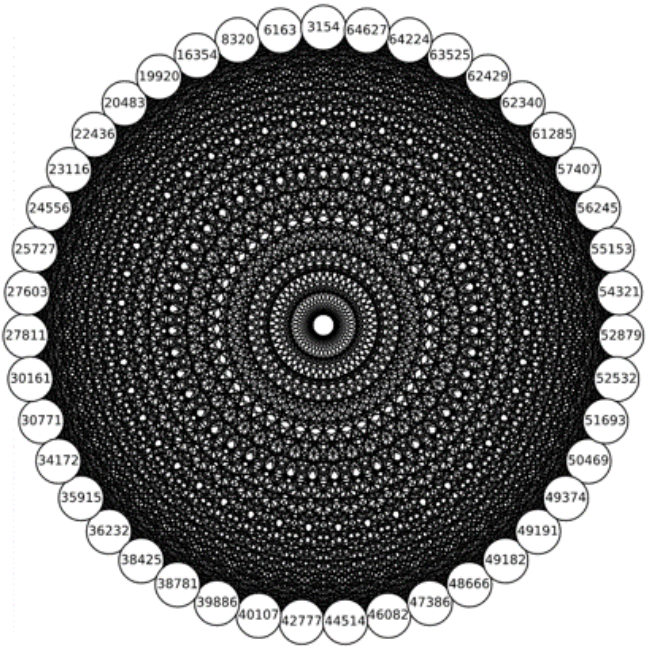


Рис 1. - Зірка ізогенних кривих

Можливість застосування ізогенії для побудови криптосистем була запропонована порівняно недавно. У 2003 році автором Е. Теске була опублікована робота, де ізогенія використовувалися в схемі з можливістю депонування ключів. У 2006 році (А. Г. Ростовцева і А. Столбунова) схема шифрування Ель-Гамаля була адаптована під ізогенні еліптичні криві. У тому ж 2006 році для побудови хеш-функцій було запропоновано використовувати графи ізогенних суперсингулярних кривих. Важливим і, можна сказати, переломним моментом в дослідженні ізогенії є робота, опублікована в 2010 році, де пропонується квантовий алгоритм, що вирішує завдання знаходження ізогенії несуперсінгулярних кривих за субекспоненціальній час. З цього моменту дослідження стали більше орієнтовані на суперсінгулярні криві. Так, в мережі вже можна знайти схеми шифрування з відкритим ключем, докази з нульовим розголошенням, схему незаперечного підпису і підпису наосліп [2].

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone “Handbook of Applied Cryptography”

2. Lawrence C. Washington “Elliptic Curves: Number Theory and Cryptography, Second Edition”