

ГРУПОВІ ОПЕРАЦІЇ НА ЕЛІПТИЧНИХ КРИВИХ

О. Коссак, Я. Холявка

*Львівський національний університет імені Івана Франка,
вул. Університетська, 1, Львів, 79000
e-mail: evagata23@yahoo.com, ya_khol@franko.lviv.ua*

Розглянуто різні види еліптичних кривих (криві Вейерштрасса, Якобі, Гаффа, Хесса, Едвардса, Лежандра-Лау) та сформульовано закони додавання і подвоєння точок.

Ключові слова: еліптичні криві, кратні точки.

1. ВСТУП

Вперше застосовувати еліптичні криві в криптографії запропонували В. Міллер і Н. Кобліц [1, 2]. За час, що минув після публікації цих праць, отримали досить багато теоретичних і практичних результатів, які виявили можливість ефективного виконання групових операцій на таких кривих. Крім того, варто відзначити високу стійкість алгоритмів, побудованих на підставі еліптичних кривих – за ці роки не відбулось помітного падіння їхньої стійкості, хоча стійкість алгоритмів, побудованих на інших групах (наприклад, RSA) помітно зменшилась. Опубліковано багато статей, монографій і підручників (наприклад, [3-10]), в яких викладено необхідні властивості еліптичних і гіпереліптичних кривих, описано їхнє використання в криптографії.

2. ОСНОВНІ ТИПИ ЕЛІПТИЧНИХ КРИВИХ

Стисло опишемо основні еліптичні криві, які використовують у криптографії, та групові операції на них. Ґрунтовніше викладення цього матеріалу можна знайти, наприклад, у [11-13].

2.1. КРИВІ ВЕЙЄРШТРАССА

Еліптичною кривою у формі Вейерштрасса над полем F , характеристика якого відмінна від 2 і 3, називають криву, яка в афінних координатах задається рівнянням

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

де параметри $a, b \in F$. Позначимо через $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ різні скінчені точки цієї кривої, що задовольняють умову $P_1 \neq -P_2$, та визначимо їхню суму $P_3 = P_1 + P_2$, $P_3 = (x_3, y_3)$, так:

$$\begin{cases} x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 \\ y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right) (x_1 - x_3) - y_1. \end{cases}$$

На рис. 1 схематично зображено операцію $P_3 = P_1 + P_2$ для точок еліптичної кривої Вейерштрасса.

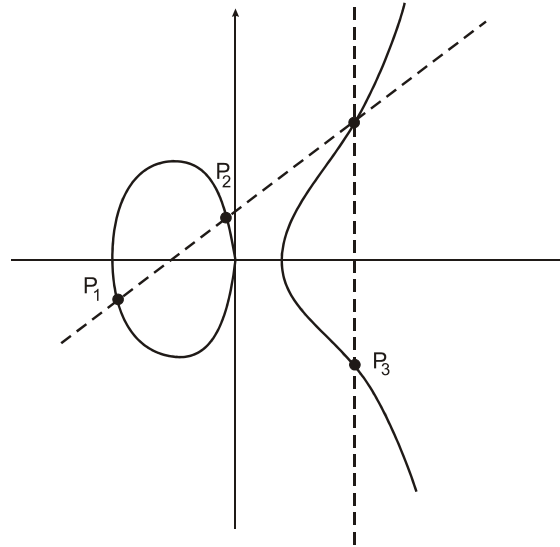


Рис. 1. Схема операції додавання точок на еліптичній кривій Вейерштрасса

Якщо $P_1 = P_2$, то $2P_1 = P_3$ і

$$\begin{cases} x_3 = \left(\frac{3x_1^2 + a}{2y_1} \right)^2 - 2x_1 \\ y_3 = - \left(\frac{3x_1^2 + a}{2y_1} \right) x_3 + \frac{x_1^3 - ax_1 - 2b}{2y_1}. \end{cases}$$

2.2. КРИВІ ЯКОБІ

Еліптичною кривою у формі перетину Якобі над полем F , характеристика якого відмінна від 2, називають криву, яка в афінних координатах задається системою

$$\begin{cases} x^2 + y^2 = 1 \\ ax^2 + t^2 = 1, \end{cases}$$

де параметр $a \in F$, $a(a-1) \neq 0$. Позначимо через $P_1 = (x_1, y_1, t_1)$, $P_2 = (x_2, y_2, t_2)$ різні точки цієї кривої, визначимо їхню суму $P_3 = P_1 + P_2$, $P_3 = (x_3, y_3, t_3)$, так:

$$\begin{cases} x_3 = \frac{x_1 y_2 t_2 + x_2 y_1 t_1}{y_2^2 + x_2^2 t_1^2} \\ y_3 = \frac{y_1 y_2 - x_1 t_1 x_2 t_2}{y_2^2 + x_2^2 t_1^2} \\ t_3 = \frac{t_1 t_2 - ax_1 y_1 x_2 y_2}{y_2^2 + x_2^2 t_1^2}. \end{cases}$$

Якщо $P_1 = P_2$, то $2P_1 = P_3$ і

$$\begin{cases} x_3 = \frac{2x_1y_1t_1}{y_2^2 + x_2^2t_1^2} \\ y_3 = \frac{y_1^2 - x_1^2t_1^2}{y_2^2 + x_2^2t_1^2} \\ t_3 = \frac{t_1^2 - ax_1^2y_1^2}{y_2^2 + x_2^2t_1^2} \end{cases}$$

Зауважимо, що можна використовувати загальний вид цієї кривої [14], що в афінних координатах задається системою

$$\begin{cases} ax^2 + y^2 = 1 \\ bx^2 + t^2 = 1, \end{cases}$$

де параметри a, b є елементами поля F , $ab(a-b) \neq 0$. Тоді $P_3 = (x_3, y_3, t_3)$ визначимо так:

$$\begin{cases} x_3 = \frac{x_1y_2t_2 + x_2y_1t_1}{y_2^2 + ax_2^2t_1^2} \\ y_3 = \frac{y_1y_2 - ax_1t_1x_2t_2}{y_2^2 + ax_2^2t_1^2} \\ t_3 = \frac{t_1t_2 - bx_1y_1x_2y_2}{y_2^2 + ax_2^2t_1^2} \end{cases}$$

Якщо $P_1 = P_2$, то $2P_1 = P_3$ і

$$\begin{cases} x_3 = \frac{2x_1y_1t_1}{y_2^2 + ax_2^2t_1^2} \\ y_3 = \frac{y_1^2 - ax_1^2t_1^2}{y_2^2 + ax_2^2t_1^2} \\ t_3 = \frac{t_1^2 - bx_1^2y_1^2}{y_2^2 + ax_2^2t_1^2} \end{cases}$$

Еліптичною кватрикою Якобі над полем F , характеристика якого відмінна від 2, 3, називають криву, яка в афінних координатах задається рівнянням

$$y^2 = k^2x^4 - (k^2+1)x^2 + 1,$$

де $k(k^2-1) \neq 0$. Часто використовують таку форму цієї кривої [15]:

$$y^2 = ax^4 + 2bx^2 + 1.$$

Тут параметри a, b є елементами поля F . Позначимо через $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ різні точки цієї кривої та визначимо їхню суму $P_3 = P_1 + P_2$, $P_3 = (x_3, y_3)$, так [16, 17]:

$$\begin{cases} x_3 = \frac{x_1y_2 + x_2y_1}{1 - ax_1^2x_2^2} \\ y_3 = \frac{(y_1y_2 + 2bx_1x_2)(1 + ax_1^2x_2^2) + 2ax_1x_2(x_1^2 + x_2^2)}{(1 - ax_1^2x_2^2)^2} \end{cases}$$

2.3. КРИВІ ХЕССА

Еліптичною кривою у формі Хесса [18] над полем F , характеристика якого відмінна від 2 і 3, називають криву, яка в афінних координатах задається рівнянням

$$x^3 + y^3 + 1 = 3dxy,$$

де параметр $d \in \text{елементу поля } F, d^3 \neq 1$. Позначимо через $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ різні точки цієї кривої та визначимо їхню суму $P_3 = P_1 + P_2, P_3 = (x_3, y_3)$, так:

$$\begin{cases} x_3 = \frac{x_2 y_1^2 - x_1 y_2^2}{x_2 y_2 - x_1 y_1} \\ y_3 = \frac{y_2 x_1^2 - y_1 x_2^2}{x_2 y_2 - x_1 y_1} \end{cases}$$

Якщо $P_1 = P_2$, то $2P_1 = P_3$ і

$$\begin{cases} x_3 = \frac{y_1(1-x_1^3)}{x_1^3-y_1^3} \\ y_3 = \frac{x_1(1-y_1^3)}{x_1^3-y_1^3} \end{cases}$$

2.4. КРИВІ ГАФФА

Еліптичною кривою у формі Гаффа [19] над полем F , характеристика якого відмінна від 2, називають криву, яка в афінних координатах задається рівнянням

$$ax(y^2-1) = by(x^2-1),$$

де $a, b \neq 0, a^2-b^2 \neq 0$. Позначимо через $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ різні точки цієї кривої та визначимо їхню суму $P_3 = P_1 + P_2, P_3 = (x_3, y_3)$, так:

$$\begin{cases} x_3 = \frac{(x_1+x_2)(1+y_1 y_2)}{(1+x_1 x_2)(1-y_1 y_2)} \\ y_3 = \frac{(y_1+y_2)(1+x_1 x_2)}{(1-x_1 x_2)(1+y_1 y_2)} \end{cases}$$

На рис. 2 схематично зображено операцію $P_3 = P_1 + P_2$ для точок еліптичної кривої Гаффа.

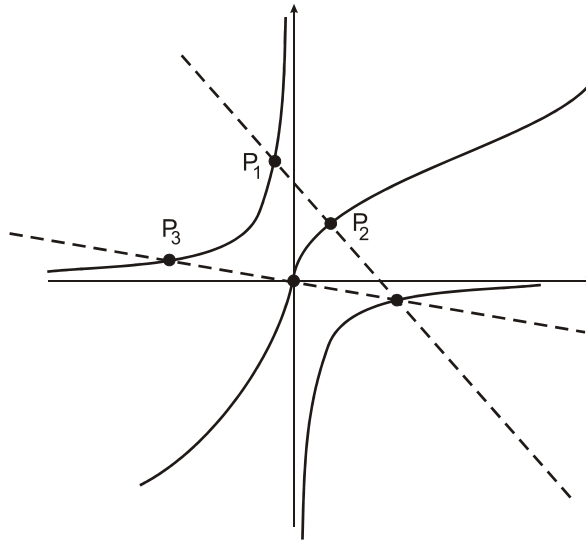


Рис. 2. Схема операції додавання точок на еліптичній кривій Гаффа

У [20] розглянуто таку форму цієї кривої:

$$x(ay^2-1) = y(bx^2-1),$$

де $ab(a-b) \neq 0$. Позначимо через $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ різні точки цієї кривої та визначимо їхню суму $P_3 = P_1 + P_2$, $P_3 = (x_3, y_3)$, так:

$$\begin{cases} x_3 = \frac{(x_1 + x_2)(1 + ay_1y_2)}{(1 + bx_1x_2)(ay_1y_2 - 1)} \\ y_3 = \frac{(y_1 + y_2)(1 + bx_1x_2)}{(bx_1x_2 - 1)(1 + ay_1y_2)}. \end{cases}$$

Якщо $P_1 = P_2$, то $2P_1 = P_3$ і

$$\begin{cases} x_3 = \frac{2x_1(1 + ay_1^2)}{(1 + bx_1^2)(ay_1^2 - 1)} \\ y_3 = \frac{2y_1(1 + bx_1^2)}{(bx_1^2 - 1)(ay_1^2 + 1)}. \end{cases}$$

2.5. КРИВІ ЕДВАРДСА

Еліптичною кривою у формі Едварса [21] над полем F , характеристика якого відмінна від 2, називають криву, яка в афінних координатах задається рівнянням

$$x^2 + y^2 = c^2(1 + x^2y^2),$$

де параметр $c \in F$. Позначимо через $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ різні точки цієї кривої та визначимо їхню суму $P_3 = P_1 + P_2$, $P_3 = (x_3, y_3)$ так:

$$\begin{cases} x_3 = \frac{x_1y_2 + x_2y_1}{c(1 + x_1y_1x_2y_2)} \\ y_3 = \frac{y_1y_2 - x_1x_2}{c(1 - x_1y_1x_2y_2)}. \end{cases}$$

У працях [21, 22] розглянуто, наприклад, таку форму цієї кривої:

$$x^2 + y^2 = 1 + d^2x^2y^2.$$

Тут параметр $d \in F$, $d^2 \neq 0, 1$. Позначимо через $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ різні точки цієї кривої та визначимо їхню суму $P_3 = P_1 + P_2$, $P_3 = (x_3, y_3)$ так:

$$\begin{cases} x_3 = \frac{x_1y_2 + x_2y_1}{1 + dx_1y_1x_2y_2} \\ y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1y_1x_2y_2}. \end{cases}$$

2.6. ЕЛІПТИЧНІ КРИВІ ЛЕЖАНДРА-ЛАУ

Еліптичною кривою у формі Лежандра-Лау над полем F , характеристика якого відмінна від 2 і 3, назвемо криву, яка в афінних координатах задається рівнянням

$$y^2 = x(x-1)(x-m),$$

де параметр $m \in F$, $m^2 \neq 0, 1$. Цю криву можна отримати за відповідних перетворень з кривої Вейерштрасса та з квадрики Якобі [24], тому вона має деякі властивості обидвох кривих. Позначимо через $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ різні скінченні точки цієї кривої, $P_1 \neq -P_2$, та визначимо їхню суму $P_3 = P_1 + P_2$, $P_3 = (x_3, y_3)$ так:

$$\begin{cases} x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 + m + 1 \\ y_3 = \frac{y_1 - y_2}{x_2 - x_1} x_3 - \frac{y_1 x_2 - x_1 y_2}{x_2 - x_1} \end{cases}$$

На рис. 3 схематично зображено операцію додавання точок еліптичної кривої Лежандра-Лау.

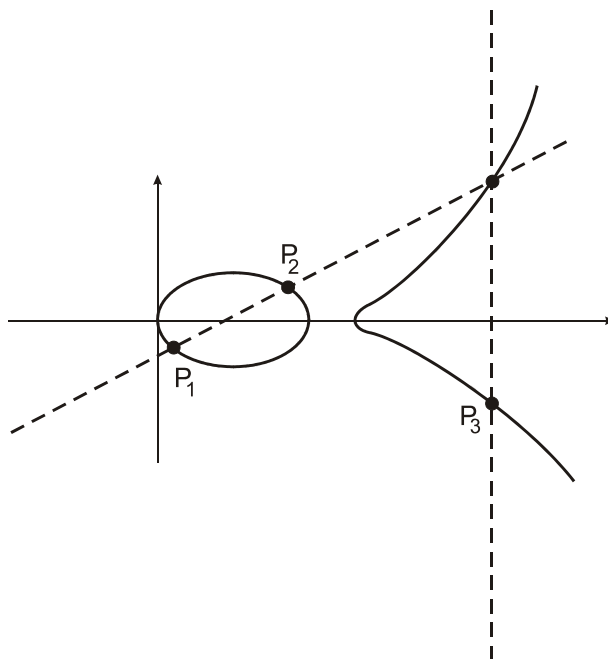


Рис. 3. Схема операції додавання точок на еліптичній кривій Лежандра-Лау

Якщо $P_1 = P_2$, то $2P_1 = P_3$ і

$$\begin{cases} x_3 = \left(\frac{3x_1^2 - 2(m+1)x_1 + m}{2y_1} \right)^2 - 2x_1 + (m+1) \\ y_3 = - \left(\frac{3x_1^2 - 2(m+1)x_1 + m}{2y_1} \right) x_3 + \frac{x_1^3 - mx_1}{2y_1} \end{cases}$$

3. ВИСНОВКИ

Група точок еліптичної кривої над скінченим полем задовольняє декілька основних властивостей: групова операція досить проста в реалізації; нескладно обчислити порядок групи [25]; побудова груп та обчислення їхніх параметрів не є складним завданням; існує багато еліптичних кривих; немає задовільних аналогів простих чисел і незвідних поліномів. Завдяки цим властивостям можна будувати швидкі та стійкі криптографічні алгоритми на підставі еліптичних кривих.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Miller V.S.* Use of Elliptic Curves in Cryptography / V.S. Miller // CRYPTO'85, LNCS. – 1986. – Vol. 218. – P. 417–426.
2. *Koblitz N.* Elliptic Curve Cryptosystems / N. Koblitz // Math. Comp. – 1987. – Vol. 48. – P. 203–209.
3. *Avanzi R.* Handbook of elliptic and hyperelliptic curve cryptography / R. Avanzi, H. Cohen, C. Doche, G. Frey, K. Nguyen, T. Lange, F. Vercauteren. – Chapman and Hall/CRC, 2005. – 808 p.
4. *Blake I.* Elliptic curves in cryptography / I. Blake, G. Seroussi, N. Smart. – Cambridge: Cambridge Univ. Press, 1999. – 204 p.
5. *Болотов А.А.* Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых / А.А. Болотов, С.Б. Гашков, А.Б. Фролов. – М.: КомКнига, 2006. – 280 с.
6. *Василенко О.В.* Теоретико-числовые алгоритмы в криптографии / О.В. Василенко. – М.: МЦНМО, 2006. – 334 с.
7. *Вербицкий О.В.* Вступ до криптології / О.В. Вербицкий. – Л.: ВНТЛ, 1998. – 247 с.
8. *Долгов В.И.* Ускорение криптографических преобразований на гиперэллиптических кривых третьего рода над малым полем / В.И. Долгов, А.В. Неласая, А.Н. Дорожкин // Системи обробки інформації. Безпека та захист інформації в інформаційних і телекомунікаційних системах. – 2009. – Вип. 7 (79). – С. 59–62.
9. *Ростовцев А.Г.* Теоретическая криптография / А.Г. Ростовцев, Е.Б. Маховенко. – СПб.: Професионал, 2004. – 480 с.
10. *Кочубинский А.И.* Эллиптические кривые в криптографии / А.И. Кочубинский // Безопасность информации. – 2000. – № 2. – С. 1–14.
11. *Василенко О.Н.* О вычислении кратных точек на эллиптических кривых над конечными полями с использованием нескольких оснований систем счисления и новых видов координат / О.Н. Василенко // Матем. вопр. криптогр. – 2011. – Т. 2. – № 1. – С. 5–28.
12. *Muhammad Ashraf* On the Alternate Models of Elliptic Curves / Muhammad Ashraf, Baris Bulent Kirlar // International Journal of Information Security Science. – 2012. – Vol 1. – No 2. – P. 49–66.
13. *Bernstein D.* Explicit Formulas Database / D. Bernstein and T. Lange // Available at <http://www.hyperelliptic.org/EFD>
14. *Feng R.* Twisted Jacobi Intersections Curves / R. Feng, M. Nie, H. Wu // Available at <http://eprint.iacr.org/2009/597.pdf>
15. *Hisil H.* New formulae for efficient elliptic curve arithmetic / H. Hisil, G. Carter, E. Dawson // INDOCRYPT'2007, Lect. Notes Comput. Sci. – 2007. – Vol. 4859. – P. 138–151.
16. *Hisil H.* Jacobi Quartic Curves Revisited / H. Hisil, K. Koon-Ho Wong, G. Carter, E. Dawson // ACISP 2009. – 2009. – P. 452–468.
17. *Wang H.* Computation on Elliptic Curves of Jacobi Quartic Form / H. Wang, K. Wang, L. Zhang, B. Li // Chinese Journal of Electronics. – 2011. – Vol. – 20 (4). – P. 655–661.
18. *Smart N.* The Hessian form of an elliptic curve / N. Smart // CHES'2001, Lect. Notes Comput. Sci. – 2001. – Vol. 2162. – P. 118–125.
19. *Joye M.* Huff's Model for Elliptic Curves. Algorithmic Number Theory / M. Joye, M. Tibbouchi, D. Vergnaud // ANTS-IX, Lecture Notes in Computer Science, Springer. – 2010. – Vol. 6197. – P. 234–250.

20. *Feng R.* Elliptic curves in Huff's model / R. Feng, H. Wu // Available at <http://eprint.iacr.org/2010/390.pdf>
21. *Edwards H.* A normal form for elliptic curves / H. Edwards // Bull. Amer. Math. Soc. – 2007. – Vol. 44. – № 3. – P. 393–422.
22. *Bernstein D.* Inverted Edwards coordinates / D. Bernstein, T. Lange // Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 17th International Symposium – AAЕСС-17, Lecture Notes in Computer Science, Springer. – 2007. – Vol. 4851. – P. 20–27.
23. *Bernstein D.* Binary Edwards Curves / D. Bernstein, T. Lange, R.R. Farashahi // Cryptographic Hardware and Embedded Systems. – CHES 2008, Lecture Notes in Computer Science, Springer. – 2008. – Vol. 5154. – P. 244–265.
24. *Low A.R.* Normal elliptic function. A Normalized Form of Weierstrass's Elliptic Functions / Low A.R. – Ont.: University of Toronto Press, Toronto, 1950. – 30 p.
25. *Schoof R.* Elliptic Curves over Finite Fields and the Computation of Square Roots mod p / R. Schoof // Mathematics of Computation. – 1985. – Vol. 44. – P. 483–494.

Стаття: надійшла до редколегії 26.09.2012

доопрацьована 14.11.2012

прийнята до друку 05.12.2012

ГРУППОВЫЕ ОПЕРАЦИИ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

О. Коссаk, Я. Холявка

Львовский национальный университет имени Ивана Франко,

ул. Университетская, 1, Львов, 79000

e-mail: evagata23@yahoo.com, ya_khol@franko.lviv.ua

Рассмотрено различные виды эллиптических кривых (кривые Вейерштрасса, Якоби, Гаффа, Хесса, Эдвардса, Лежандра-Лая) и сформулированы законы сложения и удвоения точек.

Ключевые слова: эллиптические кривые, кратные точки.

GROUP OPERATIONS ON ELLIPTIC CURVES

O. Kossak, Ya. Kholavka

Ivan Franko National University of Lviv,

Universytetska Str., 1, Lviv, 79000

e-mail: evagata23@yahoo.com, ya_khol@franko.lviv.ua

In this paper we give models of elliptic curves (Weierstrass curves, Jacobi curves, Huff curves, Hessian curves, Edwards curves, Legendre-Low curves) and point addition and point doubling formulae.

Key words: elliptic curve arithmetic, elliptic curve point-by-scalar multiplication.