УДК 621.391

ВИКОНАННЯ ОПЕРАЦІЙ У ГРУПАХ ТОЧОК ЕЛІПТИЧНИХ КРИВИХ НАД СКІНЧЕННИМИ ПОЛЯМИ

Людмила Завадська, Анатолій Кочубінський*
Національний технічний університет України "КПІ"
**МП "Дина"*

Анотація: **Наведено способи виконання операцій в скінченних полях та на еліптичних кривих, потрібних для реалізації Національного стандарту цифрового підпису. Наведено приклади таких обчислень.**
Summary: **Operations in finite fields and on elliptic curves are a key tool to implement the National digital signature standard DSTU 4145-2002. Rules to perform such operations are explained. Some examples of these computations are provided.**
Ключові слова: **Скінченні поля, еліптичні криві, обернений елемент, додавання точок еліптичної кривої, подвоєння точки еліптичної кривої, множення точки на ціле число.**

І Деякі відомості про скінченні поля

Полем називається множина елементів з двома заданими на ній бінарними операціями, додаванням та множенням, для яких виконуються умови:

щодо операції додавання – елементи поля утворюють абелеву групу з нейтральним елементом 0,

щодо операції множення – всі елементи, крім 0, також утворюють абелеву групу з нейтральним елементом 1.

Додавання та множення пов'язані між собою законом дистрибутивності: для будь-яких елементів поля x, y, z виконується $x(y+z)=xy+xz$.

Число елементів поля називається *порядком* поля. Поле називається *скінченним* (або *полем Галуа*), якщо воно має скінченну кількість елементів. Скінченне поле порядку q позначається $GF(q)$. Порядок скінченного поля завжди є степенем деякого простого числа, $q = p^m$, число m називається *степенем* поля, а просте число p – його *характеристикою*.

Абелева група ненульових елементів поля з операцією множення називається *мультиплікативною групою поля*. Мультиплікативна група скінченного поля є циклічною групою порядку $p^m - 1$, її твірний елемент називається *примітивним* елементом поля.

Скінченне поле степеня 1 називається *простим*. Просте поле можна ототожнити з множиною класів лишків за модулем числа p з операціями додавання та множення за модулем p. Наприклад, скінченне поле $GF(2)$ складається з двох елементів 0 і 1. У цьому полі операції додавання й множення виконуються наступним чином: 0+0=0, 0+1=1+0=1, 1+1=0, 0·0=1·0=0·1=0, 1·1=1, тобто за модулем 2.

Многочленом $f(t)$ степеня m над полем $GF(p)$ є вираз вигляду

$$f(t) = t^m + f_{m-1}t^{m-1} + \cdots + f_0,$$

де коефіцієнти многочлена $f_i \in GF(p)$, $i = 0, \mathrm{K}, m-1$, а t – змінна, деякий символ, що не належить полю.

Операції над такими многочленами виконуються як операції над звичайними многочленами, тільки операції над коефіцієнтами здійснюються в полі $GF(p)$. Зокрема, многочлен $g(t)$ ділиться з залишком $r(t)$ на многочлен $f(t)$, $f(t) \neq 0$, якщо $g(t)=h(t)f(t)+r(t)$, де степінь многочлена $r(t)$ менша за степінь многочлена $f(t)$. Операція обчислення залишку від ділення многочлена $g(t)$ на многочлен $f(t)$ називається зведенням многочлена $g(t)$ за модулем $f(t)$, а залишок $r(t)$ позначається $g(t) \bmod f(t)$. Якщо $r(t)=0$, то многочлен $g(t)$ ділиться на многочлен $f(t)$ без залишку.

Многочлен $f(t)$ ненульового степеня називається *незвідним* над полем $GF(p)$, якщо він ділиться без залишку над цим полем тільки на самого себе і на многочлени нульового степеня. Елемент x скінченного поля $GF(p^m)$ називається коренем многочлена $f(t)$, якщо $f(x)=0$. Незвідний многочлен $f(t)$ називається *примітивним*, якщо його корені є примітивними елементами поля.

Будь-яке скінченне поле $GF(p^m)$ є m-вимірним векторним простором над полем $GF(p)$.

Якщо x – корінь незвідного многочлена $f(t)$ степеня m над $GF(p)$, то елементи $(x^{m-1},\ldots,x,1)$ утворюють *базис* скінченного поля $GF(p^m)$ як векторного простору над полем $GF(p)$. Цей базис називається *поліноміальним*. Будь-який елемент основного поля однозначно виражається через елементи поліноміального базису. Найзручніше поліноміальний базис задавати примітивним многочленом.

Якщо x – такий елемент поля $GF(p^m)$, що елементи $(x, x^p,\ldots,x^{p^{m-1}})$ лінійно незалежні над $GF(p)$, то ці елементи утворюють базис поля $GF(p^m)$, який називається *нормальним*. Нормальний базис існує для кожного скінченного поля.

Для будь-яких елементів x, y скінченного поля $GF(p^m)$ мають місце рівності:

$$x^{p^m} = x,\ (x+y)^p = x^p + y^p.$$

Таким чином, операція піднесення до степеня p у полі $GF(p^m)$ лінійна над $GF(p)$:

$$(ax+by)^p = ax^p + by^p,$$

для довільних $a, b \in GF(p)$, $x, y \in GF(p^m)$.

Детальний виклад теорії скінченних полів подано у монографії [1].

II Операції у полі $GF(2^m)$

II.1 Виконання операцій у поліноміальному базисі

У поліноміальному зображенні елементи поля $GF(2^m)$ являють собою многочлени степеня, що не перевищує $m-1$, над $GF(2)$ або, що те саме, двійкові вектори довжини m, які складаються з їх коефіцієнтів.

Додавання у $GF(2^m)$ є звичайним додаванням поліномів над $GF(2)$, що відповідає покомпонентному додаванню за модулем 2 відповідних векторів.

При множенні елементів $GF(2^m)$ відповідні їм многочлени перемножуються з наступним зведенням результату за модулем незвідного многочлена $f(x)$, який використовується для побудови $GF(2^m)$ як розширення $GF(2)$.

Наприклад, для побудови $GF(2^3)$ використаємо примітивний многочлен 3-го степеня

$$f(x) = x^3 + x + 1. \tag{1}$$

Елементами $GF(2^3)$ є поліноми

$0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$ або, інакше, відповідні їм вектори

(000), (001), (010), (011), (100), (101), (110), (111).

Приклад додавання:

(011) + (101) = (110).

Приклад множення:

$(011) \cdot (101) = (x+1)\cdot(x^2+1) \bmod f(x) = x^3 + x^2 + x + 1 \bmod (x^3 + x + 1) = x^2 = (100)$.

Множення та ділення можна виконувати, використовуючи зображення елементів поля через степені примітивного елемента. У нашому прикладі примітивним елементом поля $GF(2^3)$ є $x = (010)$:

$$x^1 = (010),\ x^2 = (100),\ x^3 = (011),\ x^4 = (110),\ x^5 = (111),\ x^6 = (101),\ x^7 = (001), \tag{2}$$

де для підрахунку степенів x використана операція множення у $GF(2^3)$, що описана вище. Елементи x^2 та $x^2 + x$ (два інших кореня многочлена $f(x)$) також є примітивними.

Позначимо примітивний елемент поля $GF(2^m)$ через g. Внаслідок того, що $g^{2^m-1} = 1$, маємо $g^k g^s = g^{(k+s) \bmod (2^m-1)}$, $0 \le k, s \le 2^m - 1$. Так як $g^k g^{2^m-1-k} = 1$, то оберненим елементом до g^k є елемент g^{2^m-1-k}, а $g^k / g^s = g^k g^{-s} = g^{(k-s) \bmod (2^m-1)}$. Тому, маючи таблицю індексів, тобто показників степенів примітивного елемента і відповідних їм многочленів (векторів), можна швидко виконувати як множення, так і ділення у полі $GF(2^m)$. Але для великих значень m скласти таку таблицю практично неможливо, і для ділення (тобто обчислення оберненого елемента) використовується узагальнений алгоритм Евкліда знаходження найбільшого спільного дільника (НСД) двох поліномів. Ця операція набагато трудомісткіша за множення і, тим більше, за додавання елементів $GF(2^m)$.

Нехай треба знайти $c(x)^{-1}$, де $c(x)$ – елемент поля $GF(2^m)$, записаний у поліноміальному базисі, що визначається многочленом $f(x)$. Оскільки многочлен $f(x)$ – незвідний, то НСД $(c(x), f(x)) = 1$. Узагальнений алгоритм Евкліда дозволяє виразити НСД у вигляді

$$1 = a(x)f(x) + b(x)c(x), \tag{3}$$

де $a(x)$ і $b(x)$ – деякі многочлени. Після зведення обох частин рівності (3) за модулем $f(x)$ одержуємо: $b(x)\,c(x) = 1 \bmod f(x)$, отже, $c(x)^{-1} = b(x)$.

Наприклад, знайдемо $(x^2 + x + 1)^{-1}$ у поліноміальному базисі $GF(2^3)$, що визначається многочленом (1). За алгоритмом Евкліда обчислюємо:

$$x^3 + x + 1 = (x + 1)(x^2 + x + 1) + x,$$
$$x^2 + x + 1 = (x + 1)x + 1.$$

Розгортаючи цей ланцюжок рівностей у зворотньому порядку, маємо:

$1 = x^2 + x + 1 + (x + 1)x = x^2 + x + 1 + (x + 1)[x^3 + x + 1 + (x + 1)(x^2 + x + 1)] =$

$= (x + 1)(x^3 + x + 1) + x^2(x^2 + x + 1),$

звідки $(x^2 + x + 1)^{-1} = x^2$.

II.2 Виконання операцій в оптимальному нормальному базисі

Крім поліноміального базису у скінченних полях існують і інші базиси, у яких можна виразити елементи поля. Зокрема, для багатьох значень m у полях $GF(2^m)$ існує *гаусівський оптимальний нормальний базис*. Повний опис умов існування гаусівського оптимального нормального базису наведено в [2]. Ми будемо розглядати (у відповідності до стандарту [3]) поля з непарним значенням степеня m які мають гаусівський оптимальний нормальний базис другого типу. Це має місце, якщо число $p = 2m + 1$ – просте і для найменшого натурального числа k, такого що $2^k \equiv 1 \bmod(p)$, виконується одна з наступних умов:

а) $k = 2m$;

б) $p \equiv 3 \bmod 4$ і $k = m$.

Надалі гаусівський оптимальний нормальний базис типу 2 будемо називати просто *оптимальним нормальним базисом.*

Наприклад, у $GF(2^3)$ існує оптимальний нормальний базис, бо число 3 задовольняє наведеним вище умовам.

Елементи оптимального нормального базису $GF(2^m)$ є коренями деякого незвідного многочлена $p_m(t)$, що називається *нормальним многочленом* даного скінченного поля і будується за рекурсивною формулою:

$$p_0(t) = 1,\ p_1(t) = t + 1,$$
$$p_{i+1}(t) = t\,p_i(t) + p_{i-1}(t),\ i = 1, \ldots, m - 1.$$

Для $GF(2^3)$ $p_3(t) = t^3 + t^2 + 1$ і оптимальний нормальний базис виписується у вигляді x, x^2, x^4, де x – корінь $p_3(t)$.

Елементи $GF(2^m)$ зображуються двійковими векторами, що відповідають їх розкладу за базисними елементами, причому крайній лівий розряд зображення елемента поля відповідає елементу базису x, а крайній правий – елементу $x^{2^{m-1}}$. Одиниці поля у оптимальному нормальному базисі відповідає зображення (1, 1,..., 1).

Перевага використання оптимального нормального базису особливо відчутна при виконанні операції піднесення до квадрата. Дійсно, для довільного елемента $y = \sum_{i=0}^{m-1} y_i x^{2^i} = \in (y_0, \ldots, y_{m-1})\ GF(2^m)$ з того, що $y_i \in GF(2)$ та з лінійності операції піднесення до квадрата у полі характеристики 2 випливає, що

$$y^2 = (\sum_{i=0}^{m-1} y_i x^{2^i})^2 = \sum_{i=0}^{m-1} (y_i x^{2^i})^2 = \sum_{i=0}^{m-1} y_i x^{2^{i+1}} = (y_{m-1}, y_0, \ldots, y_{m-2}).$$

Отже, піднесення до квадрата в оптимальному нормальному базисі зводиться до циклічного зсуву компонент векторного зображення елемента.

Множення в оптимальному нормальному базисі виконується складніше. Для виконання множення спочатку треба обчислити мультиплікативну матрицю M, яка складається з рядків, які є розкладом в оптимальному нормальному базисі m добутків елементів базису вигляду $x \cdot x^{2^j}$, $j = 0, \text{K}, m-1$, тобто

$$M = \begin{Bmatrix} x \cdot x \\ \dots \\ x \cdot x^{2^j} \\ \dots \\ x \cdot x^{2^{m-1}} \end{Bmatrix}.$$

Перший зліва розряд добутку z двох елементів поля u і v обчислюється за формулою

$$z_0 = uMv^T,$$

де u – вектор-рядок, а v^T – вектор-стовпчик. Наступні розряди добутку обчислюються за цією самою формулою, тільки замість самих векторів u і v^T використовуються їх послідовні циклічні зсуви на один розряд вліво. Нагадаємо, що при використанні оптимального нормального базису крайній правий розряд зображення елемента поля відповідає елементу базису $x^{2^{m-1}}$. Складність множення визначається числом ненульових елементів у матриці M. В загальному випадку в цій матриці не менше $2m-1$ ненульових елементів. Якщо нормальний базис оптимальний, то ненульових елементів рівно $2m-1$. Власне, з цієї причини такий базис і називається оптимальним.

Так, у $GF(2^3)$, зважаючи на те, що x – корінь $p_3(t)$,

$$x \cdot x = x^2 = (010),$$
$$x \cdot x^2 = x^3 = x^2 + 1 = (010) + (111) = (101),$$
$$x \cdot x^4 = x^5 = x + 1 = (100) + (111) + (011),$$

і, таким чином, $M = M_3 = \begin{Bmatrix} 010 \\ 101 \\ 011 \end{Bmatrix}$.

Якщо $u = (011)$, $v = (101)$ – розклад елементів u, v поля $GF(2^3)$ за оптимальним нормальним базисом, то компоненти розкладу добутку $z = u \cdot v$ обчислюються як

$$\begin{aligned} z_0 &= (011)\, M_3\, (101)^{\mathrm{T}} = 1, \\ z_1 &= (110)\, M_3\, (011)^{\mathrm{T}} = 0, \\ z_2 &= (101)\, M_3\, (110)^{\mathrm{T}} = 0. \end{aligned} \qquad (4)$$

(У нашому прикладі неважко перевірити, що це дійсно так, бо $u = x^5$, $v = x^3$, $u \cdot v = x^8 = x$).

Практично замість мультиплікативної матриці обчислюються явні формули, які виражають один розряд добутку через розряди співмножників. Для $GF(2^3)$ ці формули мають вигляд:

$$z_0 = (u_0, u_1, u_2)\, M_3\, (v_0, v_1, v_2,)^{\mathrm{T}} = u_1v_0 + (u_0 + u_2)\, v_1 + (u_1 + u_2)\, v_2,$$
$$z_1 = u_2v_1 + (u_0 + u_1)\, v_2 + (u_0 + u_2)\, v_0,$$
$$z_2 = u_0v_2 + (u_1 + u_2)\, v_0 + (u_0 + u_1)\, v_1.$$

Підставляючи значення компонент векторів u і v, одержуємо той же результат, що й y (4).

Обернений елемент в оптимальному нормальному базисі знаходиться за формулою $y^{-1} = y^{2^m-2}, \quad y \neq 0.$ Для обчислення правої частини цієї формули існує ефективний алгоритм [4]. Він спирається на той факт, що $2^m - 2 = 2^{m-1} + 2^{m-2} + \dots + 2^2 + 2$, тобто $y^{-1} = y^{2^{m-1}} y^{2^{m-2}} \dots y^2.$

Нехай m_r, K, m_0 – двійковий розклад цілого числа $m-1$. Тоді обчислення оберненого елемента виконується таким чином:

1) $b \leftarrow y;\ k \leftarrow 1;$
2) для i від $r-1$ до 0 обчислюють
   2.1 $c \leftarrow b;$
   2.2 для j від 1 до k обчислюють
      2.2.1 $c \leftarrow c^2;$

2.3 $b \leftarrow bc$;

2.4 $k \leftarrow 2k$;

2.5 якщо $m_i = 1$, то $b \leftarrow b^2 y$ і $k \leftarrow k+1$;

3) $y^{-1} = b^2$.

Найпростіше проілюструвати роботу цього алгоритму у випадку $m = 2^r + 1$, коли двійковий розклад числа $m - 1$ має вид: $m_r = 1, m_{r-1} = 0, \ldots, m_0 = 0.$ Робиться наступний ланцюжок перетворень, де $(\wedge k)$ означає k-кратне піднесення до квадрата, а (*) – перемноження двох попередніх значень у ланцюжку:

$$y \xrightarrow{(\wedge 1)} y^2 \xrightarrow{(*)} y^2 y \xrightarrow{(\wedge 2)} y^{2^3} y^{2^2} \xrightarrow{(*)} y^{2^3} y^{2^2} y^2 y \xrightarrow{(\wedge 4)}$$
$$\xrightarrow{(\wedge 4)} y^{2^7} y^{2^6} y^{2^5} y^{2^4} \xrightarrow{(*)} y^{2^7} y^{2^6} y^{2^5} y^{2^4} y^{2^3} y^{2^2} y^2 y \xrightarrow{(\wedge 8)} \ldots \xrightarrow{(*)}$$
$$\xrightarrow{(*)} y^{2^{2^r-1}} y^{2^{2^r-2}} \ldots y^2 y \xrightarrow{(\wedge 1)} y^{2^{m-1}} y^{2^{m-2}} \ldots y^2$$

(останній крок є відмінним від попередніх).

Оскільки піднесення до квадрата в оптимальному нормальному базисі практично не потребує часу, то алгоритм працює досить швидко.

II.3 Заміна базису

Основне поле можна задавати поліноміальними базисами з різними примітивними многочленами або оптимальним нормальним базисом. Іноді може виникнути потреба перейти від одного базису до іншого. Робиться це так само, як і в загальному випадку заміни базису у векторному лінійному просторі, – через матрицю переходу, рядки якої є розкладом базисних елементів першого базису по другому базису.

Нехай скінченне поле задане базисом B_1, якому відповідає многочлен $p_1(t)$, та базисом B_2, якому відповідає многочлен $p_2(t)$ (кожен з многочленів $p_1(t)$, $p_2(t)$ – примітивний многочлен у разі поліноміального базису або нормальний многочлен у разі оптимального нормального базису). Для переходу від базису B_1 до базису B_2 обчислюють корінь u многочлена $p_1(t)$ в базисі B_2, а потім в базисі B_2 обчислюють елементи $u_k = u^k, 0 \le k \le m-1$, якщо базис B_1 поліноміальний, або елементи $u_k = u^{2^k}, 0 \le k \le m-1$, якщо базис B_1 оптимальний нормальний. З цих елементів будують матрицю U, що складається з їх розкладів у базисі B_2:

$$U = \begin{Bmatrix} u_0 \\ \ldots \\ u_k \\ \ldots \\ u_{m-1} \end{Bmatrix} = \begin{Bmatrix} u_{00} & \ldots & u_{0m-1} \\ \ldots & \ldots & \ldots \\ u_{m-1,0} & \ldots & u_{m-1,m-1} \end{Bmatrix}$$

Ця матриця є матриця переходу від базису B_1 до базису B_2, а обернена матриця U^{-1} є матриця переходу від базису B_2 до базису B_1, тобто елемент поля в базисі B_1 (позначимо його x) та базисі B_2 (позначимо його y) пов'язані співвідношенням

$$y = xU,\ x = yU^{-1}.$$

При цьому розклад елемента у поліноміальному базисі треба записувати у зворотньому порядку: крайньому лівому розряду відповідає 1, а крайньому правому – x^{m-1}.

Розглянемо приклад. Нехай у $GF(2^3)$ базис B_1 поліноміальний і задається многочленом $p_1(t) = t^3 + t + 1$, а базис B_2 – оптимальний нормальний, тобто задається многочленом $p_2(t) = t^3 + t^2 + 1$. Тоді $B_1 = \{u^2, u, 1\}$, де u – корінь $p_1(t)$, $B_2 = \{x, x^2, x^4\}$, де x – корінь $p_2(t)$. Неважко бачити, що $x + 1$ –

корінь $p_1(t)$, бо (враховуючи, що x – корінь $p_2(t)$) $(x+1)^3 + (x+1) + 1 = 0$. Отже, можемо покласти $u = x + 1$, і у базисі B_2 маємо: $u = (100) + (111) = (011)$, $u^2 = (101)$.

Таким чином, матриця переходу $U = \begin{Bmatrix} 111 \\ 011 \\ 101 \end{Bmatrix}$.

Нехай елемент y має у базисі B_1 розклад (011). Щоб знайти його розклад у базисі B_2, записуємо y у зворотньому порядку і множимо на матрицю переходу:

$$(110) \begin{Bmatrix} 111 \\ 011 \\ 101 \end{Bmatrix} = (100).$$

<u>III Еліптичні криві над скінченними полями</u>

III.1 Означення та приклади

Загальне рівняння еліптичної кривої над довільним полем F зводиться до рівнянь більш простого виду в залежності від характеристики основного поля F. У криптографії використовуються еліптичні криві над простими полями $GF(p), p \neq 2,3$, та полями $GF(2^m)$. Наведемо їх означення.

Нехай характеристика поля F не дорівнює 2 або 3.

Еліптичною кривою над полем F є множина пар (x, y) елементів цього поля, що задовольняють *афінне рівняння еліптичної кривої* в нормальній формі Вейєрштрасса

$$y^2 = x^3 + Ax + B, \text{ де } A, B \in F, 4A^3 + 27B^2 \neq 0,$$

разом із приєднаною *нескінченно віддаленою точкою* O.

Нехай характеристика поля F дорівнює 2.

Еліптичною кривою над полем F є множина пар (x, y) елементів цього поля, що задовольняють афінне рівняння еліптичної кривої в нормальній формі Вейєрштрасса

$$y^2 + y = x^3 + Ax + B, \text{ де } A, B \in F, \tag{5}$$

або

$$y^2 + xy = x^3 + Ax^2 + B, \text{ де } A, B \in F, \ B \neq 0, \tag{6}$$

разом із приєднаною нескінченно віддаленою точкою O.

Рівняння (5) визначає так звані суперсингулярні криві, використання яких у криптографії небажане. Тому ми (згідно з [3]) будемо розглядати над $GF(2^m)$ лише несуперсингулярні криві, що визначаються рівняннями типу (6).

Уперше використовувати еліптичні криві в криптографічних цілях було запропоновано в [5] і [6]. Найкращим посібником з теорії еліптичних кривих є книги Дж. Сільвермана [7] і [8]. Простіший виклад цієї теорії з описом криптографічних застосувань міститься у книгах [9] і [10].

Пара (x, y) елементів основного поля, що задовольняють афінне рівняння еліптичної кривої, називається *афінними координатами* точки еліптичної кривої. Нескінченно віддалена точка O не має афінних координат. Координати точки P еліптичної кривої позначають (x_P, y_P). Число точок еліптичної кривої (враховуючи і нескінченно віддалену точку) називається *порядком* еліптичної кривої.

Розглянемо приклад еліптичної кривої над простим скінченним полем. Нехай

$$y^2 = x^3 + x + 1, \tag{7}$$

– рівняння еліптичної кривої E над полем $GF(11)$. Знайдемо всі точки даної еліптичної кривої. Для того, щоб точка $P = (x_P, y_P)$ належала кривій E, потрібно, щоб значення виразу в правій частині (7) при $x = x_P$ являло

собою квадратичний лишок за модулем 11. У нашому маленькому прикладі неважко знайти всі квадратичні лишки, піднісши всі елементи $GF(11)$ до квадрата. Квадратичними лишками за модулем 11 є: 1, 3, 4, 5, 9.

Підставимо елементи $GF(11)$ у праву частину (4) і підрахуємо відповідні значення *y,* якщо у правій частині одержали квадратичний лишок:

x	0	1	2	3	4	5	6	7	8	9	10
x^3+x+1	1	3	0	9	3	10	3	10	4	2	10
y	1,10	5, 6	0	3, 8	5, 6	-	5, 6	-	2, 9	-	-

Таким чином, еліптична крива E складається з точок: (0, 1), (0, 10), (1, 5), (1, 6), (2, 0), (3, 3), (3, 8), (4, 5), (4, 6), (6, 5), (6, 6), (8, 2), (8, 9) і точки на нескінченності O. Тож порядок її дорівнює 14, і криву E можна зобразити на площині так; як показано на рис.

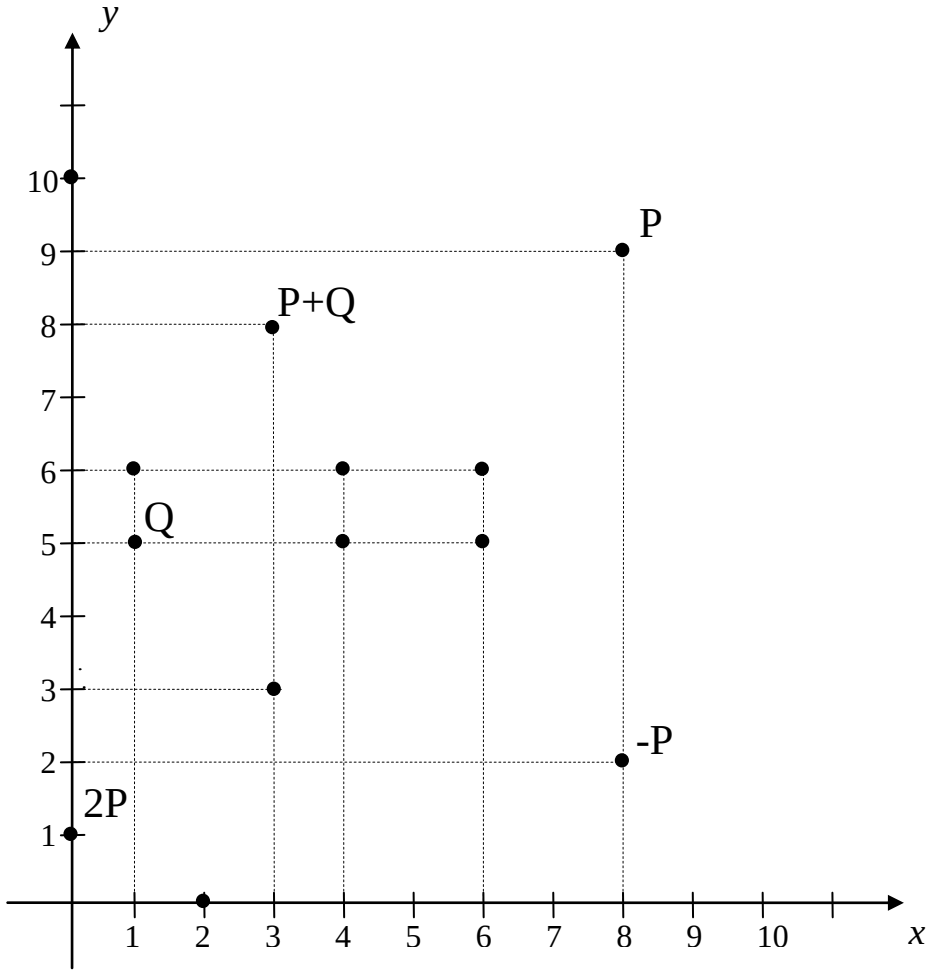

Рисунок – Графічне зображення еліптичної кривої $y^2 = x^3 + x + 1$ над полем *GF*(11)

Так само можна побудувати і еліптичну криву над полем $GF(2^m)$. Нехай

$$y^2 + xy = x^3 + x^2 + g^4 \qquad (8)$$

– афінне рівняння еліптичної кривої E_2 над полем $GF(2^3)$, де $g = (010)$ - примітивний елемент $GF(2^3)$, корінь примітивного многочлена (1) (див. п. 2.1). Прямим перебором знаходимо всі пари (x,y), $x \in GF(2^3)$, $y \in GF(2^3)$, що задовольняють (8):

$(0, g^2), (1, g), (1, g^3), (g^2, 1), (g^2, g^6), (g^4, g), (g^4, g^2), (g^5, g^2), (g^5, g^3), (g^6, g^2), (g^6, g^3)$.

Отже, еліптична крива E_2 складається з усіх перелічених точок плюс точка на нескінченності O. Розташувавши елементи $GF(2^3)$ вздовж осей координат у порядку зростання степенів g, можна зобразити і цю криву подібно до того, як це зроблено на рис.

III.2 Групова операція на точках еліптичних кривих над скінченними полями

Точки еліптичної кривої утворюють скінченну абелеву групу відносно відповідно визначеної операції додавання точок. Конкретні правила виконання цієї операції наведено нижче. *Сума* точок P і Q еліптичної кривої позначається $P+Q$, при цьому $P+Q=Q+P$. Нейтральним (або нульовим) елементом цієї групи є нескінченно віддалена точка O: для будь-якої точки *P* еліптичної кривої виконується $P+O=O+P$. Точка $(-P)$, така, що $(-P)+P=P+(-P)=O$, називається точкою, *протилежною* для точки P. Точка $2P=P+P$ називається *подвоєнням* точки P.

III.2.1 Групова операція на точках еліптичних кривих над полями характеристики p ≠ 2, 3

Нехай $P=(x_P, y_P), P \neq O$ і $Q=(x_Q, y_Q), Q \neq O$ – дві точки еліптичної кривої в афінних координатах.

Координати точки, протилежної до P, визначаються як $-P=(x_P, -y_P)$.

Сума точок $R=P+Q$ обчислюється за такими правилами.

Якщо $Q \neq \pm P$, то координати (x_R, y_R) точки R обчислюються за формулами:

$$x_R = \left(\frac{y_P - y_Q}{x_P - x_Q}\right)^2 - x_P - x_Q,$$
$$y_R = -y_P + \left(\frac{y_P - y_Q}{x_P - x_Q}\right)(x_P - x_R). \qquad (9)$$

Координати (x_R, y_R) подвоєної точки $R=2P$ обчислюються за формулами:

$$x_R = \left(\frac{3x_P^2 + A}{2y_P}\right)^2 - 2x_P,$$
$$y_R = -y_P + \left(\frac{3x_P^2 + A}{2y_P}\right)(x_P - x_R). \qquad (10)$$

Всі операції в наведених формулах виконуються в основному полі.

Як приклад порахуємо суму точок еліптичної кривої E_1 над $GF(11)$ $P = (8,9)$, $Q = (1,5)$ (див. рис.).

$$x_R = \left(\frac{9-5}{8-1}\right)^2 - 8 - 1 = \left(4 \cdot 7^{-1}\right)^2 - 9 = (4 \cdot 8)^2 - 9 = 3$$
$$y_R = -9 + \left(\frac{9-5}{8-1}\right)(8-3) = 8.$$

Таким чином, $P+Q = (3,8)$.

Подвоїмо точку P:

$$x_R = \left(\frac{3\cdot 8^2+1}{2\cdot 9}\right)^2 - 2\cdot 8 = 0,$$

$$y_R = -9 + \left(\frac{3\cdot 8^2+1}{2\cdot 9}\right)(8-0) = 1.$$

Отже, $2P = (0,1)$.

Точка, протилежна до P: $-P = (8, -9) = (8, 2)$.

Точки P, Q, $P+Q$, $2P$, $-P$ зображені на рис.

III.2.2 Групова операція на точках еліптичних кривих над полями характеристики 2

Формули, що визначають групову операцію на точках еліптичних кривих над полем характеристики 2, дещо відрізняються від формул попереднього пункту. А саме, нехай $P=(x_P, y_P), P\neq O$ і $Q=(x_Q, y_Q), Q\neq O$ – дві точки еліптичної кривої над $GF(2^m)$ в афінних координатах.

Координати протилежної точки визначаються так:

$$-P = (x_P, x_P + y_P).$$

Сума точок $R = P + Q$ обчислюється за наступними правилами.

Якщо $Q \neq \pm P$, то координати (x_R, y_R) точки R обчислюються за формулами:

$$\begin{aligned} x_R &= \left(\frac{y_P + y_Q}{x_P + x_Q}\right)^2 + \frac{y_P + y_Q}{x_P + x_Q} + x_P + x_Q + A, \\ y_R &= \left(\frac{y_P + y_Q}{x_P + x_Q}\right)(x_P + x_R) + x_R + y_P. \end{aligned} \tag{11}$$

Якщо $x_P = 0$, то $2P=O$. Якщо $x_P \neq 0$, то координати (x_R, y_R) подвоєної точки $R = 2P$ обчислюються за формулами:

$$\begin{aligned} x_R &= x_P^2 + \frac{B}{x_P^2}, \\ y_R &= x_P^2 + \left(x_P + \frac{y_P}{x_P}\right)x_R + x_R. \end{aligned} \tag{12}$$

Скористаємося цими формулами для обчислень у групі точок еліптичної кривої E_2 над $GF(2^3)$, побудованої у п. 3.1. Нехай $P = (g^2, 1)$, $Q = (g^5, g^3)$. Тоді, використовуючи таблицю індексів (2), маємо:

$$-P = (g^2, g^2 + 1) = (g^2, g^6).$$

Якщо $R = P + Q$, то

$$x_R = \left(\frac{1+g^3}{g^2+g^5}\right)^2 + \frac{1+g^3}{g^2+g^5} + g^2 + g^5 + 1 = \left(g\cdot g^{-3}\right)^2 + g\cdot g^{-3} + g^2 + g^5 + 1 =$$

$$= \left(g\cdot g^4\right)^2 + g\cdot g^4 + g^2 + g^5 + 1 = g^3 + g^5 + g^2 + g^5 + 1 = g^3 + g^2 + 1 = g^4,$$

$$y_R = \left(\frac{1+g^3}{g^2+g^5}\right)\left(g^2+g^4\right) + g^4 + 1 = g^5 g + g^4 + 1 = g,$$

отже, $P + Q = (g^4, g)$.

Якщо $R = 2P$, то

$$x_R = g^4 + \frac{g^4}{g^4} = g^4 + 1 = g^5,$$

$$y_R = g^4 + \left(g^2 + \frac{1}{g^2} \right) g^5 + g^5 = g^4 + g^3 g^5 + g^5 = g^3.$$

Таким чином, $2P = (g^5, g^3)$.

III.3 Множення точки еліптичної кривої на ціле число

Операція обчислення суми k точок P еліптичної кривої $P + P + ... + P$ (k разів) називається множенням точки P на натуральне число k і позначається kP. За означенням $0P = O,\ (-k)P = k(-P)$, тому можна говорити про множення точки на довільне ціле число.

Це основна операція на точках еліптичної кривої, що використовується у криптографії. Тому її прискорення має велике практичне значення. Для множення точки $P \neq O$ на велике ціле число можна використовувати способи, цілком аналогічні тим, що застосуються для піднесення цілого числа до степеня k.

Якщо $k = \sum_{i=0}^{t-1} k_i 2^i$ – двійкове зображення числа k, то точку $Q = kP$ можна обчислити наступним чином:

1) приймають $Q \leftarrow O$;
2) для i від t-1 до 0 обчислюють $Q \leftarrow 2Q$; якщо $k_i = 1$, то додатково обчислюють $Q \leftarrow Q + P$.

Наприклад, двійковий розклад числа 100 є: $100 = 2^6 + 2^5 + 2^2$. Щоб обчислити $100P$, виконуємо таку послідовність операцій:

$$100P = 2(2(P + 2(2(2(P + 2\ P))))).$$

III.4 Проективне зображення еліптичних кривих

Поряд з афінним зображенням еліптичних кривих і точок на них відомі проективні зображення еліптичних кривих і точок на них декількох типів. Класичне проективне рівняння Вейєрштрасса несуперсингулярної еліптичної кривої над $GF(2^m)$ має вигляд:

$$y^2 z + xyz = x^3 + Ax^2 z + Bz^3,$$

а точками проективної еліптичної кривої є трійки елементів основного поля $(x : y : z)$, що задовольняють це рівняння, причому хоча б одна з цих координат відмінна від нуля. Використання двокрапки у запису проективних координат позначає, що трійки координат, отримані одна з іншої множенням на ненульовий елемент основного поля, відповідають тій самій проективній точці еліптичної кривої (і також задовольняють проективне рівняння Вейєрштрасса). В проективному зображенні нескінченно віддалена точка має координати $(0:1:0)$. Для переходу від афінних координат до проективних використовуються співвідношення:

$$(x, y) \to (x : y : 1);$$
$$O \to (0 : 1 : 0).$$

Для переходу від проективних координат до афінних використовуються співвідношення:

Якщо $z = 0$, то $(x : y : z) \to O$;

Якщо $z \neq 0$, то $(x : y : z) \to (xz^{-1}, yz^{-1})$.

Перехід до проективних координат часто дає змогу підвищити ефективність обчислень у групі точок еліптичної кривої [11]. Ми не будемо наводити формули додавання та подвоєння точок еліптичної кривої у проективних координатах. Зазначимо лише, що в них, на відміну від (9) – (12), не використовується операція обчислення оберненого елемента основного поля – найтрудомісткіша операція в скінченному полі.

Література: ***1.*** *Лидл Р., Нидеррайтер Г. Конечные поля, Т. 1 и 2. – М., Мир, 1988.* ***2.*** *Mullin R., Onyszczuk I., Vanstone S. A., Wilson R. Optimal Normal Bases in* $GF(p^n)$ *// Discrete Applied Math. V. 22, 1988/1989, 149–*

161. ***3.*** *Державний стандарт України. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. ДСТУ 4145. Київ, Держстандарт України, 2003.* ***4.*** *Itoh T., Tsijii S. A Fast Algorithm for Computing Multiplicative Inverses in* $GF(2^m)$ *Using Normal Bases. // Info. and Comput., 78(3), 1988, 171–177.* ***5.*** *Koblitz N. Elliptic Curve Cryptosystems // Mathematics of Computation, 48, 1987, 203 – 209.* ***6.*** *Miller V. S. Use of Elliptic Curves in Cryptograph y // Advances in Cryptology – Crypto'85 (LNCS 218), 1986, 417 – 426.* ***7.*** *Silverman J. The Arithmetic of Elliptic Curves. – New York: Springer, 1986.* ***8.*** *Silverman J. Advanced Topics in the Arithmetic of Elliptic Curves. – New York: Springer, 1994.* ***9.*** *Menezes A. Elliptic Curve Public Key Cryptosystems. – Boston: Kluwer Academic Publishers, 1993.* ***10.*** *Blake I., Seroussi G., Smart N. Elliptic Curves in Cryptography. – Cambridge University Press, 1999.* ***11.*** *Cohen H., Miyaji A., Ono T. Efficient Elliptic Curves Exponentiation Using Mixed Coordinates // Advances in Cryptology –Asiacrypt'98 (LNCS 1514), 1998, 51–65.*

УДК 691.3.06

МЕТОД ГЕНЕРУВАННЯ ПАРАМЕТРІВ ЕЛІПТИЧНИХ КРИВИХ

Микола Карпінський*, Ігор Васильцов, Ігор Якименко, Ярослав Кінах

**Університет в Бєльську-Бялей, Польща,*

Тернопільська академія народного господарства.

Анотація: **Розглядається проблематика генерування параметрів еліптичної кривої. Розроблено метод, що дозволяє ефективно визначати коефіцієнти еліптичної кривої. Розроблений метод базується на застосуванні еволютивного підходу. В статті наведено результати роботи програми, розробленої на основі даного методу.**

Summary: **In this paper the problem of generating of elliptic curves parameters has been considered. To obtain the coefficients of elliptic curve the method has been developed. This method is based on the usage of evolutionary approach. In the paper the results of software, developed on the proposed method, have been shown.**

Ключові слова: **Еліптична крива, еволютивний алгоритм, цифровий підпис.**

І Застосування еліптичних кривих для задач захисту інформації

Захист інформації відіграє одну з ключових ролей в забезпеченні інформаційної безпеки держави. В останні роки в зв'язку з швидким розвитком інформаційних технологій, що залучають все більше і більше користувачів, які в процесі роботи обмінюються інформацією за допомогою систем електронного зв'язку, виникає необхідність розвитку засобів захисту інформації. Вирішити задачу захисту інформації можна шляхом використання криптографічних алгоритмів [1].

Розрізняють два типи криптографічних алгоритмів: симетричні і асиметричні. В першому випадку обидва абоненти, що беруть участь в процесі передачі інформації, використовують однаковий ключ, а в другому — різні, "секретний" і "відкритий".

В останні роки інтенсивно розвивається криптографія еліптичних кривих (ЕК), де основною криптографічною операцією є пошук кратних точок еліптичної кривої, тобто множення точки еліптичної кривої на скаляр на основі операції додавання цих точок [2]. Особливий інтерес до криптографії еліптичних кривих обумовлений такими перевагами – швидкодія та невелика довжина ключа.

У сучасних криптосистемах на основі еліптичних кривих бінарної розмірності в діапазоні від 150 до 350 забезпечується рівень криптографічної стійкості, який потрібно використовувати у відомих криптографічних системах бінарної розмірності від 600 до 1400 і більше.

У приведеній нижче табл. 1 порівнюються наближені розміри параметрів еліптичних систем і криптосистеми RSA, що забезпечують однакову стійкість шифру [1]. Ці дані отримані на основі сучасних методів розв'язання задачі дискретного логарифмування еліптичної кривої (Elliptic Curve Discrete Logarithm Problem – ECDLP) та факторизації (пошуку дільників) для великих цілих чисел.

Таблиця 1 – Порівняння стійкості основних криптографічних алгоритмів.

Система на основі еліптичної кривої (базова точка P)	RSA (довжина модуля n)
1024 біт	3084 біт
3250 біт	9750 біт
15500 біт	46500 біт