УДК 681.3.06

О.Є. ІЛЯСОВА

Харківський національний університет радіоелектроніки, Україна

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ОБЧИСЛЕННЯ ПОРЯДКУ ЕЛІПТИЧНОЇ КРИВОЇ ПРИ ГЕНЕРАЦІЇ ПАРАМЕТРІВ КРИПТОСИСТЕМ НА ЕЛІПТИЧНИХ КРИВИХ

В роботі розглянуто методи обчислення порядку еліптичної кривої, здійснено аналіз обчислювальної складності даних методів. На основі цього запропоновано оптимальний метод для програмної реалізації генерації параметрів криптосистем на еліптичних кривих.

загальносистемні параметри, обчислювальна складність, порядок кривої, слід відображення ендоморфізму Фробеніуса

Вступ

Групи точок еліптичної кривої можуть бути використані для криптографічних додатків, а саме алгоритмів формування цифрового підпису та алгоритмів спрямованого шифрування. Використання еліптичних кривих дозволяє генерувати ключі для симетричних криптосистем та перевіряти числа на простоту. Основна перевага еліптичних кривих для криптографічних додатків полягає у відсутності властивостей, що полегшують здійснення криптоаналізу, за умови виконання певних вимог до них. Для роботи вказаних алгоритмів необхідно виконати генерацію загальносистемних параметрів криптосистем на еліптичних кривих. В результаті виникає задача побудови ефективного алгоритму генерації загальносистемних параметрів. Під ефективністю алгоритму будемо розуміти виконання наступних вимог:

- алгоритм повинен мати поліноміальну складність;
- генерування параметрів повинно здійснюватися за найменший час.

Одним з основних етапів генерування параметрів вважається побудова еліптичної кривої над вказаним полем та обчислення її порядку. Цей етап є одним з трудомістких етапів за просторовою та часовою складністю. Тому його оптимізація є однією з важливих задач для здійснення процесу генерування параметрів криптосистеми.

У зв‘язку з цим **мета роботи полягає** в:

1. Проведенні порівняльного аналізу обчислювальної складності існуючих методів обчислення порядку випадково генерованої кривої;

2. Виборі метода, програмна реалізація якого відповідає критерію ефективності.

Загальний підхід до знаходження порядку еліптичної кривої

Існують такі основні способи обчислення порядку кривої [1]: *l*-адичний та *p*-адичний. Алгоритми, що базуються на вказаних способах обчислення порядку кривої мають поліноміальну складність та можуть знаходити порядок кривої над полем $GF\left(2^n\right)$, $GF(p)$ та $GF\left(p^n\right)$. До *l*-адичного способу обчислення відносяться методи P. Shoof‘a, SEA [1, 2]. До *p*-адичного способу належить метод T. Satoh‘a та його модифікація, яка наведена в роботі [3]. Крім того існує метод, який має назву метод baby-step-gigant-step [1], який також обчислює порядок кривої над полем $GF(p)$.

Для здійснення порівняльного аналізу методів обчислення порядку еліптичної кривої розглянемо еліптичну криву над полем $GF(p)$ наступного виду:

$$y^2 \equiv x^3 + ax + b \bmod p,$$

де a, b її параметри, які належать полю $GF(p)$.

Еліптична крива над полем $GF(2^n)$ має вигляд:

$$y^2 + xy \equiv x^3 + ax^2 + b \bmod(2, f(x)),$$

де $a, b \in GF(2^n)$ – параметри кривої, а $f(x)$ – незведений поліном, що генерує поле $GF(2^n)$.

Раціональні точки еліптичної кривої утворюють абелеву групу.

Порядком еліптичної кривої $(\#E)$ називають число точок еліптичної кривої разом з нескінченно віддаленою точкою О-нейтральним елементом групи точок.

Порядком базової точки називають число n, яке задовольняє умові $n \cdot P = \mathrm{O}$. Операція $n \cdot P$ – це операція скалярного множення точок еліптичної кривої.

Точка $P = (x, y)$ є точкою l-крутіння, якщо $l \cdot P = \mathrm{O}$.

Порядок еліптичної кривої над полем $GF(q)$ обчислюють за формулою:

$$\#E = q + 1 - t,$$

де число t називають слідом відображення ендоморфізму Фробеніуса φ, яке діє на координати точок еліптичної кривої за правилом:

$$\varphi(x, y) = \left(x^q, y^q\right).$$

Для обчислення порядку кривої, згідно формули наведеної в роботі [1], необхідно обчислити слід t відображення ендоморфізму Фробеніуса [1] з рівняння

$$\left(x^{p^2}, y^{p^2}\right) - t \cdot \left(x^p, y^p\right) + p \cdot (x, y) = 0. \quad (1)$$

Значення сліду t може бути достатньо великим цілим числом, це пов‘язано з розмірністю поля $GF(p)$. Якщо знаходити значення t, застосовуючи рівняння (1), то необхідно спочатку знайти координати (x, y) – базової точки еліптичної кривої, а потім обчислити $\left(x^{p^2}, y^{p^2}\right)$, та $\left(x^p, y^p\right)$. Крім того, необхідно виконати дві операції скалярного множення точок еліптичної кривої $p \cdot (x, y)$ та $t \cdot \left(x^p, y^p\right)$. Ці операції виконують доти, доки рівняння:

$$\left(x^{p^2}, y^{p^2}\right) + p \cdot (x, y) = t \cdot \left(x^p, y^p\right) \quad (2)$$

не буде вірним для деякого значення t з проміжку $\left[1, \sqrt{p}\right)$.

Значеннях t та p є достатньо великими числами. Стандарт FIPS 186-2-2000 [5] пропонує використовувати поле $GF(p)$ з мінімальним значенням $p = 2^{192} - 2^{64} - 1$. Перевірка виконання рівняння (2) перебором усіх значень числа t не є прийнятним, тому що вимагає виконати приблизно $\left(p^2\right)$ операцій множення в полі $GF(p)$.

Аналіз методів обчислення порядку еліптичної кривої

Оптимізацією метода наведеного вище є метод, який був запропонований P. Shoof [1].

Алгоритм, що базується на методі P. Shoof‘а, був першим алгоритмом з поліноміальною складністю, який обчислює порядок еліптичної кривої над полем $GF(p)$, де p – велике просте число. Цей метод дозволяє обчислювати порядок кривої, коефіцієнти рівняння якої є випадковими і належать полю $GF(p)$. Метод P. Shoof‘а наведений в роботі [1] полягає в пошуку значень $t_l : t_l \equiv t \bmod l$, де $l = 2,3,5,7,...$, які задовольняють рівнянням (3):

$$\left(x^{p^2}, y^{p^2}\right) - t_l \left(x^p, y^p\right) + p_l (x, y) = 0. \quad (3)$$

Використання рівняння (3) у вигляді:

$$\left(x^{p^2}, y^{p^2}\right) + p_l \cdot (x, y) = t_l \cdot \left(x^p, y^p\right) \quad (4)$$

зменшує обчислювальну складність пошуку значення t з рівняння (2). Співвідношення (3), (4) виконується тільки для точок l-крутіння еліптичної кривої. Використання рівняння (4) дозволяє знайти лише $t_l : t_l \equiv t \bmod l$, *де* $l = 2,3,5,7,...$ в тому випадку коли відомі координати точок l-крутіння. Після отримання значення t_l, де l – прості числа, які менше

p, обчислюють t – значення сліду ендоморфізму Фробеніуса за допомогою теореми з роботи [4].

Теорема 1. Нехай $m_1, m_2, ..., m_s$ – взаємно прості числа, $\prod_{i=1}^{s} m_i = M$. Якщо числа $y_i, i = 1,2,...,s$ задовольняють співвідношенню: $\frac{M}{m_i} y_i = 1 (\mathrm{mod}\, m_i)$, тоді розв'язок системи порівнянь:

$$t \equiv t_1 \bmod m_1;$$
$$t \equiv t_2 \bmod m_2;$$
$$t \equiv t_s \bmod m_s$$

має вигляд $t = \sum_{i=1}^{s} \frac{M}{m_i} y_i t_i$.

Для отримання координат точки l-крутіння використовують поліноми ділення, які визначені співвідношенням (5):

$$\begin{aligned}
&\psi_{-1}(x) = -1, \psi_0(x,y) = 0, \psi_1(x,y) = 1;\\
&\psi_2(x) = 2\left[x^3 + ax + b\right];\\
&\psi_3(x) = 3x^4 + 6ax^2 + 12bx - a^2;\\
&\psi_4(x) = 4\left[x^3 + ax + b\right]\times\\
&\times\left(x^6 + 5ax^4 + 20bx^3 - 5(ax)^2 - 4bx - 8b^2 - a^3\right);\\
&\psi_{2n}(x) = \psi_n(x)\frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n+1}^2\psi_{n-2}}{2\left[x^3 + ax + b\right]},\ n \geq 3;\\
&\psi_{2n+1}(x) = \psi_{n+2}(x)\psi_n^3(x) -\\
&-\psi_{n+1}^3(x)\psi_{n-1}(x),\ n \geq 2.
\end{aligned} \quad (5)$$

Коефіцієнти a, b в співвідношенні (5) є параметрами еліптичної кривої, яка задана над полем $GF(p)$. Поліноми ділення дозволяють побудувати поліноми виду:

$$f_n(x) = \begin{cases} \psi_n(x), n = 2l; \\ \dfrac{\psi_n(x)}{x^3 + ax + b}, n = 2l + 1. \end{cases} \quad (6)$$

Доцільність застосування поліномів (6) основана на теоремі, яка наведена в роботі [1]:

Теорема 2. Нехай точка $P = (x, y)$ – це точка еліптичної кривої, ордината якої не дорівнює нулю. Рівність вигляду $nP = \mathrm{O}, n \geq 3$ виконується тоді і лише тоді, коли $f_n(x) = 0$.

З властивості поліномів (6) випливає, що корені цих поліномів є абсцисами точок l-крутіння. Для пошуку координати точки l-крутіння необхідно знайти корінь полінома $f_n(x)$ степені $\frac{l^2 - 1}{2}$.

Основна причина того, що метод P. Shoof'a не набув широкого використання, полягає саме в великій степені поліномів ділення. В табл. 1 наведено взаємозв'язок між розмірністю поля та степенем поліномів ділення. Розрахунки проводилися на основі обмеження представленого в роботі [5].

Таблиця 1

Взаємозв'язок розмірності поля Галуа та степені поліному ділення.

значення p	максимальне значення l	степінь поліномів ділення
$< 2^{10}$	7	24
$< 2^{200}$	191	18240

Згідно даних представлених в роботі [5] запис одного полінома ділення для $l = 191$ вимагає використання одного Мбайту пам'яті. В зв'язку з вказаним недоліком метод P. Shoof'a, незважаючи на поліноміальну складність алгоритму, не вважається доцільним для використання для полів з великою характеристикою.

Алгоритм, який засновано на методі SEA [2], є оптимізацією метода P. Shoof'a. Метод SEA базується також на пошуку значення сліду ендоморфізму Фробеніуса з рівняння (4). Оптимізація здійснюється за рахунок використання поліномів степені $\frac{l-1}{2}$ та $l+1$ для обчислення координат точок l-крутіння. Для побудови поліномів вказаних ступенів розглядають прості числа Elkies'a [2] для даної еліптичної кривої. Числа Elkies'a можна отримати за допомогою рівняння (3). Спочатку обчислюють значення $\Delta = t_l^2 - 4p_l (\mathrm{mod}\, l)$. Якщо Δ є квадратичним лишком тоді в векторному просторі існує значення λ, яке задовольняє умові:

$$\left(x^p, y^p\right) = \lambda \cdot (x, y). \quad (7)$$

Умова (7) дозволяє спростити обчислення значення t_l за допомогою рівняння (3).

Як зазначалося вище, рівняння (3) виконується для точок l-крутіння. Для пошуку координат даних точок для простих чисел Elkies'а існує поліном степені $\frac{l-1}{2}$ виду:

$$g(x)=\prod_{P\in E[l]}(x-x(P)), \qquad (8)$$

де точки $P\in E[l]$ є точками з підгрупи l-крутіння точок еліптичної кривої. Поліном $g(x)$ є дільником поліномів (6). Крім того, для простих чисел Elkies'а можна використовувати модулярні поліноми $\Phi_l(x,y)$, означення яких наведено в роботі [6]. Модулярні поліноми $\Phi_l(x,y)$, степінь яких дорівнює $l+1$ мають наступну властивість:

Твердження. Нехай E – еліптична крива над полем $GF(p)$, j інваріант якої – j_E. Модулярний поліном $\Phi_l(x,j_E)=0$ має корені в $GF(p)$ тоді і лише тоді, коли l є простим числом Elkies'а.

Наведена властивість дозволяє знаходити корені полінома $g(x)$. Елементами поля $GF(p)$ є корені полінома $q(x)=x^p-x$. Корені найбільшого спільного дільника поліномів $\Phi_l(x,j_E)$ та $q(x)$ і будуть x координатами точок $P\in E[l]$. Недоліком цього метода є зростання коефіцієнтів поліномів $\Phi_l(x,y)$ при зростанні значення l. Наприклад вільний член полінома $\Phi_2(x,y)$ дорівнює 157 000 000 000, а вільний член полінома $\Phi_3(x,y)$ дорівнює 1855 425 871 872 000 000 000.

Наступний метод має назву baby-step-gigant-step [1]. Цей метод для пошуку порядку еліптичної кривої використовує оцінку H. Hasse з роботи [7]. Теорема 3 (оцінка H. Hasse)**.** Нехай p – просте число, крива E задана над полем $GF(p)$. Тоді $\#E$ – порядок кривої E належить проміжку

$$\left(p+1-2\sqrt{p},p+1+2\sqrt{p}\right). \qquad (9)$$

На початковому етапі алгоритму обирають випадкову точку еліптичної кривої G. Потім обирають число m з інтервалу (9) так, щоб виконувалася умова $mG=\mathrm{O}$. Якщо число m єдине, тоді порядок кривої $\#E$ дорівнює числу m. Для пошуку числа m використовують метод, наведений в роботі [8]. Розглянемо основні етапи цього методу.

Спочатку обчислюють координати точок $G,2G,3G,...,SG, S\approx\sqrt[4]{p}$, використовуючи формули додавання та подвоєння точок еліптичної кривої, наведені в роботі [7]. Далі знаходять координати точок $Q=(2S+1)G, R=(p+1)G$ та виконують обчислення координат точок $R, R\pm Q, R\pm 2Q,....,$ $R\pm tQ,$ де $t\approx\sqrt[4]{p}$. Одна з точок $R\pm iQ$ буде співпадати з точкою lP. Тоді порядок кривої обчислюється за формулою

$$\#E=m=p+1+(2S+1)i-j.$$

У випадку, коли для точки G знайдено два значення m з інтервалу (9), необхідно вибрати іншу випадкову точку еліптичної кривої та провести обчислення m для цієї точки. Недоліком цього методу є великі витрати об'єму пам'яті. Він пов'язаний з необхідністю виконання $p+1$ операцій інвертування в полі $GF(p)$ при додаванні та подвоєні точок у випадку застосування афінних координат. Метод T. Satoh [3] дозволяє обчислювати порядок випадково генерованої кривої над полем $GF(p^n)$ та $GF(2^n)$. Вказаний метод для поля $GF(p^n)$ не є ефективним, як і метод SEA за рахунок використання модулярних поліномів $\Phi_p(x,y)$, коефіцієнти яких збільшуються при збільшені характеристики поля $GF(p)$. Для поля $GF(2^n)$ даний метод дозволяє здійснити програмну реалізацію з найменшою обчислювальною складністю. Його сутність полягає також в обчисленні сліду ендоморфізму Фробеніуса, як і в методах P. Shoof'а, та SEA.

Він подолав недоліки методів P. Shoof'а, та SEA за рахунок використання тільки одного модулярного полінома $\Phi_2(x,y)$. Використовуючи p-адичний запис коефіцієнтів полінома та виконуючи усі дії з заздалегідь вказаною точністю, можна зменшити

об‘єм необхідної пам‘яті для його реалізації. Метод T. Satoh та його модифікація [3] полягає в побудові циклу ізоморфних кривих заданих над полем p-адичних чисел таким чином, що значення сліду ендоморфізму Фробеніуса буде таким самим, як і для ізоморфних кривих, які задані над полем $GF\left(p^n\right)$. Побудова кривих здійснюється за допомогою:

1. Відображення ендоморфізму Фробеніуса.
2. На основі властивості модулярного полінома наведеної в роботі [3].
3. j інваріанта базової кривої, яка задана над полем $GF\left(p^n\right)$.

На другому етапі, згідно роботи [3], обчислюють коефіцієнти рівняння ізогенних кривих, які ізоморфні кривим, що отримані на першому етапі алгоритму та задані над полем p-адичних чисел. На останньому етапі обчислюється слід Фробеніуса за допомогою коефіцієнтів рівнянь побудованих еліптичних кривих.

Висновки

При проведені аналізу, існуючих на цей час методів обчислення порядку кривої, з‘ясовано, що найкращим за критерієм ефективності є метод обчислення порядку кривої T. Satoh‘а для розширення поля характеристики два та алгоритм під назвою baby-step-gigant-step для полів $GF(p)$. Перевага модифікації методу T. Satoh‘а полягає в мінімальності обчислювальної складності методу в порівнянні з іншими методами. Вона дозволяє здійснити ефективну за часом програмну реалізацію. Недоліком усіх методів обчислення порядку еліптичної кривої вважається неспроможність їх відбирати криві, які не придатні для застосування в криптографічних перетвореннях. В результаті чого при створенні алгоритму необхідно після обчислення порядку кривої перевіряти чи є її порядок майже простим числом. Складність обчислення порядку кривої для кожного метода наведена в табл. 2. Множення двох цілих чисел, що складаються з n біт здійснюються за $\mathrm{O}\left(n^{\mu}\right)$ операцій.

Таблиця 2

Складність методів обчислення порядку еліптичної кривої

Еліптична крива, яка задана над полем	Метод	Обчислювальна складність
$GF(p)$, p – просте число	P. Shoof	$\mathrm{O}\left((\log p)^{3\mu+2}\right)$
$GF(p)$, p просте число	SEA	$\mathrm{O}\left((\log p)^{2\mu+2}\right)$
$GF\left(p^n\right)$, $p \geq 5$, p – просте число	T. Satoh	$\mathrm{O}\left(n^{2\mu+1}\right)$
$GF\left(2^n\right)$	T. Satoh	$\mathrm{O}\left(n^{2\mu+1}\right)$
$GF(p)$, p – просте число	baby-step-gigant-step	$\mathrm{O}\left(p^{1+\mu}\right)$

Література

1. Schoof R. Counting points on elliptic curve over finite fields, Proc. Journees Arithmetiques, 93, 1995. – P. 219-252.

2. Elkies E. Elliptic and modular curves over finite fields and related computational issues. Computational perspectives in number theory 1998, P. 21-76.

3. Fouquet M., Gaudry P. and. Harley R. An extension of Satoh’s algorithm and its implementation, J. Ramanujan Math. Soc. 15 2000, P. 281-318.

4. Бухштаб А.А. Теория чисел. – М.: Просвещение, 1996. – 386 с.

5. Бессалов А.В., Тележненко А.Б. Криптосистемы на эллиптических кривых. – К.: Политехника, 2004. – 223 с.

6. Silverman J.H. The arifmetic of Elliptic Curve, GTM 106, Springer – Verlad, New-York, 1986. – 385 p.

7. Dale Husemoler Elliptic curve Springer. Graduate text in mathemetics 111. – 529 p.

8. Silverman J. The arithmetic of elliptic curve, Graduate Texts in mathematics 106, Shringer - Verlag, New York, 1986. – 868 p.

9. Shanks D. Class number a theory of factorization, and genera, AMS, Providence RL 1971. – P. 415-440.

Надійшла до редакції 22.02.2007

Рецензент: д-р техн. наук, проф. І.Д. Горбенко, Харківський національний університет радіоелектроніки, Харків.