

РОЗРОБКА МЕТОДУ ОБЧИСЛЕННЯ ПОРЯДКУ ЕЛІПТИЧНОЇ КРИВОЇ ДЛЯ ПОБУДОВИ ПАРАМЕТРІВ НАДВИСОКОГО РІВНЯ СТІЙКОСТІ

М.Ф. БОНДАРЕНКО, О.Є. ПЕТРЕНКО, О.С. ФРОЛОВ

В даній роботі здійснено аналіз перспективних методів обчислення порядку еліптичної кривої. На його основі розроблено метод, спроможний обчислювати порядок еліптичної кривої, що визначена на полях вимірності від 2^{677} та вище, який має найменшу в порівнянні з методом Сато обчислювальну складність.

The analysis of perspective methods of calculating the order of an elliptic curve is carried out in this paper. A method is developed on its base which is capable of calculating the order of an elliptic curve that is determined on the fields of dimension from 2^{677} and higher and which has the lowest calculation complexity compared to the Sato method.

ВСТУП

В теперішній час криптографічні перетворення в групах точок еліптичних кривих завдяки своїм перевагам, в порівнянні з перетворенням в полях та кільцях, застосовують в різних криптографічних додатках. Побудова загальносистемних параметрів з необхідним рівнем стійкості є першим етапом такого застосування. Одночасне використання симетричних та асиметричних криптографічних перетворень вимагає узгодження при виборі загальносистемних параметрів. Дане узгодження передбачає застосування параметрів, що забезпечують еквівалентні рівні стійкості. В Україні для симетричних перетворень розроблено блокувий симетричний шифр з довжиною блоку 512 бітів. При використанні даного шифру в комбінованих криптосистемах необхідно застосовувати параметри надвисокого рівня стійкості. На цей час прийнятих до використання вітчизняних та міжнародних стандартів, загальносистемних параметрів для криптографічних перетворень в групі точок еліптичних кривих не існує. Слід зазначити, що деякі параметри наведено в інших стандартах [1, 2], але їх використання забезпечує тільки добрий та високий рівні стійкості для даних перетворень.

Проблемність питання побудови параметрів надвисокого рівня стійкості полягає в трудомісткості розв'язання задачі обчислення порядку еліптичної кривої, яка має базову точку порядку 2^{1024} . Вдосконалений метод Сато, який наведений в роботах [3, 4] спроможний обчислювати порядок еліптичних кривих з визначеною властивістю. Застосування даного методу передбачає обчислення порядку випадкової еліптичної кривої, яка не обов'язково буде придатною до застосування. Крім того, априорно визначити, яка по черзі з випадкових кривих буде придатна до застосування неможливо. В результаті чого для побудови загальносистемних параметрів необхідно виконувати обчислення порядку великого числа еліптичних кривих, що визначені на полях вимірності більше ніж 2^{1024} . З огляду на це, зменшення часової та просторової складностей методу обчислення порядку кривої є актуальною та необхідною задачею.

Мета даної роботи полягає в розробці методу обчислення порядку кривої, який спроможний з прийнятними просторовою та часовою складностями знаходити порядки еліптичних кривих, що визначені на полях вимірності більше ніж 2^{1024} .

1. АНАЛІЗ ПЕРСПЕКТИВНИХ МЕТОДІВ ОБЧИСЛЕННЯ ПОРЯДКУ КРИВОЇ

В процесі побудови загальносистемних параметрів усіх рівнів стійкості необхідно із множини кривих, що задані на обраному полі, вибрати еліптичну криву, властивості якої дозволяють застосовувати її для криптографічних перетворень або довести, що на обраному полі таких кривих немає. Для цього випадковим чином обирають коефіцієнти рівняння еліптичної кривої із елементів обраного поля. Далі обчислюють її порядок. Потім перевіряють криву на придатність застосування в криптографічних перетвореннях. Слід зазначити, що умови придатності обирають згідно з властивостями еліптичної кривої та концепцією безпеки. В результаті чого для побудови параметрів необхідно обчислювати порядки достатньо великої кількості еліптичних кривих. Це є складною і трудомісткою задачею особливо для полів, вимірність яких більше ніж 2^{1024} .

В теперішній час розроблено декілька методів, які спроможні здійснювати обчислення на полях даної вимірності. До них відносяться метод Сато, який докладно розглянутий в роботі [5], його різні модифікації [3, 4] та метод алгебраїчно геометричних значень [6]. Дані методи для обчислення порядку передбачають здійснення підняття еліптичної кривої, яка визначена на полі характеристики два до кривої, яка визначена на полі характеристики нуль. В якості поля характеристики нуль обрано розширення поля 2-адичних цілих.

Вдосконалений метод, в порівнянні з відомим методом Сато, спроможний обчислювати порядок еліптичної кривої зі зменшеною складністю. Згідно з роботою [4] запропоноване вдосконалення дозволило зменшити кількість операцій множення в розширенні кільця 2-адичних цілих в 1,3 рази, що зменшило обчислювальну складність метода в цілому. Так кількість операцій множення в розширенні нормованого кільця 2-адичних цілих Z_{2^n} ,

що є включенням поля 2-адичних цілих степені n при застосуванні метода Сато $D_1(n)$ дорівнює $\frac{17n^2}{2} + 10n$, а кількість операцій множення $D_2(n)$ при застосуванні запропонованого вдосконаленого метода Сато дорівнює $\frac{13n^2}{2} + 10n$. На рис. 1 показано, що кількість операцій множення в кільці Z_{2^n} при використанні вдосконаленого методу зменшено при побудові параметрів високого та надвисокого рівнів стійкості. Крім того, різниця в кількості операцій множення відомого та вдосконаленого методів зростає при зростанні ступеня розширення кільця. Таким чином, запропоноване вдосконалення скоротило час, витрачений на побудову параметрів високого та надвисокого рівнів стійкості за рахунок зменшення часу виконання операцій множення в кільці.

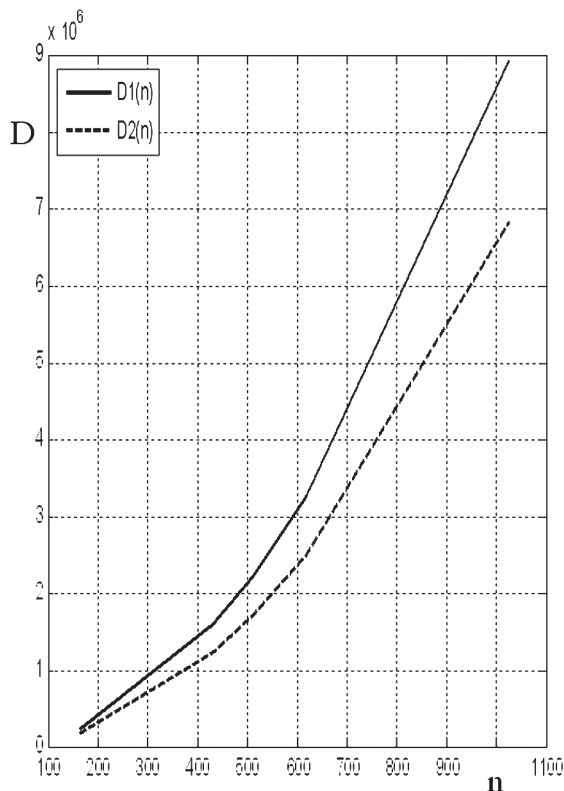


Рис. 1. Залежність кількості операцій множення від ступеня розширення поля

Запропоноване в роботах [3, 4] вдосконалення методу не є ефективним при побудові параметрів надвисокого рівня стійкості при умові необхідності обчислення порядку великої кількості еліптичних кривих при перевірці їх на придатність до застосування. Це відбувається в тому випадку, коли із 100 випадково вибраних кривих, які визначені на полях вимірності більше ніж 2^{1024} , жодна не є придатною для використання. В процесі побудування параметрів з порядком базової точки 2^{1024} необхідно вибрати криві, які згідно з діючим в Україні стандартом [1] придатні до застосування. Їх множина складається із 2^{2062} еліптичних

кривих. В зв'язку з випадковим вибором кривих із даної множини апріорно не можна визначити, для якої кількості кривих необхідно обчислювати порядки. В деяких випадках перевіряють усі криві множини для вибору той, що потрібна. Для побудови загальносистемних параметрів надвисокого рівня стійкості в рік можна обчислити порядки 2^{10} еліптичних кривих, використовуючи ЕОМ за допомогою вдосконаленого метода Сато. Обчислення було здійснено з використанням процесора celeron 900 МГц. З огляду на це даний метод не є зручним для застосування в описаному випадку.

Другий з перспективних методів обчислення порядків еліптичних кривих є метод, який застосовує алгебраїчно геометричних значення для обчислення порядку еліптичної кривої, що визначена на полі характеристики нуль [6].

Сутність даного методу полягає в застосуванні двох послідовностей $\{a_n\}, \{b_n\}$, які мають спільну границю, де $a_n = \frac{a_{n-1} + b_{n-1}}{2}$ та $b_n = \sqrt{a_{n-1}b_{n-1}}$.

Виходячи з даних виразів, еліптичні криві, що визначені на полі дійсних чисел, мають рівняння наступного вигляду:

$$y^2 = x(x-1) \left(x - \frac{a_n^2}{b_n^2} \right). \quad (1)$$

Слід ендоморфізму Фробеніуса для кривої (1) дорівнює $tr(Fr) = \prod \frac{2a_i}{a_i + b_i}$.

За допомогою алгебраїчних та геометричних значень, а також їх зв'язку з еліптичними кривими, що визначені на полях характеристики нуль, можливо застосування даного методу для обчислення порядку еліптичної кривої визначеної на розширенні кільця 2-адичних цілих Z_{2^n} , яке належить полю Q_{2^n} . В зв'язку з тим, що усі обчислення здійснені в розширенні поля 2-адичних цілих, необхідно використовувати 2-адичну точність також само, як і у методі Сато [3].

Розглянемо рівняння еліптичної кривої у вигляді

$$y^2 + xy \equiv x^3 - \alpha \pmod{2^k, f(x)}, \quad (2)$$

де $\alpha \in Z_{2^n}$, k – 2-адична точність, а $f(x)$ – незведений поліном, що генерує поле $GF(2^n)$. Застосовуючи значення $\alpha \in Z_{2^n}$, визначимо послідовність $\{a_i\}, \{b_i\}$ на основі даних, наведених в роботі [6] наступним чином:

$$a_0 = 1 + 8\alpha, b_0 = 1, \\ a_{i+1} = \frac{a_i + b_i}{2}, b_{i+1} = \sqrt{a_i b_i}.$$

Значення сліду відображення ендоморфізму Фробеніуса в даному випадку дорівнює $\prod \frac{a_i}{a_{i+1}}$.

Здійснити обчислення значення сліду ендоморфізму Фробеніуса можливо, використовую-

ючи бібліотеку алгоритмів виконання основних операцій в розширенні кільця 2-адичних цілих, розроблену на основі запропонованих в роботі [7] правил. Кількість операцій множення, здійснених в кільці Z_{2^n} при цьому дорівнюють $\frac{n^2 + 3n}{2}$.

Недоліком даного методу є необхідність виконання попередніх обчислень. Пов'язано це з тим, що при побудові загальносистемних параметрів застосовують поля характеристики p (p – просте число), а метод обчислення порядку еліптичної кривої заснований на алгебраїчно геометричних значеннях працює на полях характеристики нуль.

2. РОЗРОБКА МЕТОДУ ОБЧИСЛЕННЯ ПОРЯДКУ ЕЛІПТИЧНОЇ КРИВОЇ ДЛЯ ПОБУДОВИ ЗАГАЛЬНОСИСТЕМНИХ ПАРАМЕТРІВ НАДВИСОКОГО РІВНЯСТІЙКОСТІ

На основі здійсненого аналізу перспективних методів обчислення порядку еліптичної кривої метод, що спроможний працювати на полях вимірності більше, ніж 2^{1024} , передбачає виконання наступних етапів:

1. Вибір випадковим чином елемента $\bar{\alpha}$, який належить полю $GF(2^n)$, як коефіцієнта рівняння наступного виду:

$$y^2 + xy \equiv x^3 - \bar{\alpha} \pmod{(2^k, f(x))},$$

де k – 2-адична точність, а $f(x)$ – незведений поліном, що генерує поле $GF(2^n)$.

2. Підняття елемента $\bar{\alpha} \in GF(2^n)$ до елемента $\alpha \in Z_{2^n}$.

3. Побудови послідовності $\{a_i\}, \{b_i\}$.

4. Обчислення значення сліду відображення ендоморфізму Фробеніуса на основі отриманих даних.

5. Обчислення порядку еліптичної кривої.

Пункти 3 та 4 здійснюються із застосуванням основних положень методу, який заснований на алгебраїчно геометричних значеннях.

В пункті 2 здійснення підняття елемента виконано аналогічно підняттю елементів в методі Сато.

Згідно з відомим методом Сато [3] для обчислення порядку необхідно здійснити канонічне підняття еліптичної кривої E з j -им інваріантом j_E , яка визначена на полі $GF(2^n)$ до еліптичної кривої E' з j -им інваріантом $j_{E'}$, яка визначена в кільці Z_{2^n} . Дане підняття базується на тому, що $\Phi_2(j_E, j_{E'}) = 0$ та $End(E) \cong End(E')$. На відміну від метода Сато, в розробленому методі здійснюється підняття лише одного елемента, використовуючи модулярний поліном $\Phi_2(x, y)$ із роботи [3].

Підняття еліптичної кривої (1) до еліптичної кривої (2) здійснюється за допомогою j -ого інваріанта j_E . Спочатку, використовуючи іте-

рації Ньютона, обчислюється значення кореня рівняння $\Phi_2(j_E, x) = 0$. Початковим коренем для ітерацій Ньютона є значення j_E . Ітераційний процес здійснюється з 2-адичною точністю k , яка визначає кількість елементів частинної суми

ряду $\sum_{i=0}^{+\infty} a_i 2^i$, де a_i приймають значення або нуль

або один аналогічно ітераційному процесу методу Сато з тією різницею, що в розробленому методі використовується функція з однією змінною $f(x) = \Phi_2(x, j_E)$. В результаті невідомий корінь x обчислюють за допомогою формули:

$$x = x - \frac{f(x)}{f'(x)}. \quad (3)$$

Формулу (3) застосовано для елементів поля 2-адичних цілих. Інверсійний елемент $\frac{1}{f'(x)}$ обчислюють за формул із роботи [7].

Складність процесу підняття еліптичної кривої визначимо кількістю здійснених операцій множення в кільці Z_{2^n} , вона дорівнює $9kM$, де M – це операція множення в кільці Z_{2^n} при умові, що 2-адична точність дорівнює k .

Виходячи з оцінки Хассе [8], обмеження значення сліду відображення ендоморфізму Фробеніуса 2-адична точність має таке саме значення, що і у методі Сато та дорівнює $\left\lfloor \frac{n}{2} \right\rfloor$.

На третьому етапі розробленого методу необхідно обчислити не тільки інверсійний елемент, а і значення квадратного кореня в кільці Z_{2^n} . Пошук квадратного кореня за допомогою ітерацій Ньютона як кореня полінома $g(x) = a - x^2$ здійснювати недоцільно. Це пов'язано із застосуванням інверсії при даному обчисленні. Використовуючи формулу (3) для пошуку кореня полінома $g(x)$, отримано наступну формулу:

$$x = x + \frac{a - x^2}{2x}. \quad (4)$$

Позбутися інверсії в полі при обчисленні квадратного кореня можливо, якщо шукати обернене значення квадратного кореня елемента, використовуючи поліном $g(x) = 1 - (ax)^2$. Ітераційний процес в такому випадку, виходячи з роботи [6], здійснено за наступною формулою:

$$x = x + \frac{x(1 - ax^2)}{2}. \quad (5)$$

Використовуючи той факт, що $\sqrt{a} = \frac{a}{\sqrt{a}}$ та формулу (5), значення квадратного кореня знаходиться за формулою:

$$x = ax + \frac{x(a - (ax)^2)}{2}. \quad (6)$$

Виходячи з наведеного, кількість операцій множення в розширенні кільця 2-адичних цілих

$D_3(n)$ при обчисленні значення сліду відображення ендоморфізму Фробеніуса запропонованим методом, дорівнює $\frac{n^2 + 12n}{2} = \frac{n^2}{2} + 6n$.

На рис. 2 показано, як зменшена кількість операцій множення розробленого методу обчислення порядку кривої в порівнянні з вдосконаленим методом Сато [4].

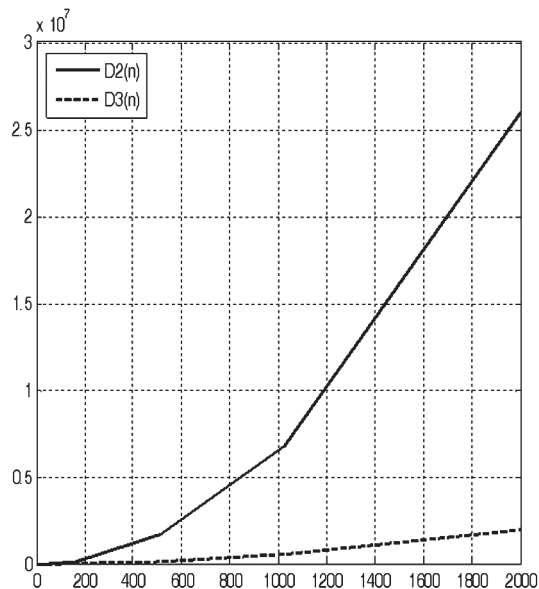


Рис. 2. Залежність кількості операцій множення від ступеня розширення поля

ВИСНОВКИ

Запропоновано метод обчислення порядку еліптичної кривої, який в 13 разів зменшує кількість операцій множення в розширенні кільця 2-адичних цілих степені n в порівнянні з вдосконаленим методом Сато, що дозволяє значно скоротити час побудови загальносистемних параметрів високого та особливо надвисокого рівнів стійкості.

Література.

- [1] Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка ДСТУ 4145-2002 – [Чинний від 2003-07-01]. – К.: Держстандарт України, 2003. – 31 с.
- [2] X9.62 Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). ANSI, – 1998.

- [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] Погребняк К.А. Моделирование та аналіз методів генерації загальних параметрів для стандарту ДСТУ 4145-2002 / К.А. Погребняк, О.Є. Петренко, О. С. Фролов // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения информационной безопасности. – 2008. – том 7, №3. – с.248-252.
- [5] Satoh T. Canonical lifting of elliptic curves and p – adic point counting. (theoretical background) / Satoh T. // Department of Mathematics, Faculty of Science, Saitame University. – 2001. – P. 1–21.
- [6] Henri Cohen Handbook of Elliptic and Hyperelliptic Curve Cryptography / Henri Cohen Gerhard Frey.- Taylor & Francis Group, LLC, 2006 - 843 P.
- [7] Лясова О.Є. Обчислення порядку еліптичної кривої за допомогою p – адичного представлення / О. Є. Лясова, К. А. Погребняк, О. С. Фролов // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения информационной безопасности. – 2007. – том 6, №3. – с.334-339.
- [8] Silverman J.H. The arithmetic of Elliptic Curve, GTM 106, Springer – Verlad, New–York, 1986. – 385 p.

Надійшла до редколегії 10.09.2009



Бондаренко Михайло Федорович, член-кореспондент НАН України, Лауреат державної премії України, доктор технічних наук, професор, ректор Харківського національного університету радіоелектроніки.



Петренко Ольга Євгенівна, викладач ХБІ УАБС НБУ. Область наукових інтересів: генерування загальносистемних параметрів в криптосистемах, що базуються на перетвореннях в групі точок ЕК.



Фролов Олег Сергійович, інженер-програміст ЗАТ «ІТ», аспірант каф. БІТ ХНУРЕ.