УДК 681.3. 06

МОДЕЛЮВАННЯ ТА АНАЛІЗ МЕТОДІВ ГЕНЕРАЦІЇ ЗАГАЛЬНИХ ПАРАМЕТРІВ ДЛЯ СТАНДАРТУ ДСТУ 4145-2002

К.А. ПОГРЕБНЯК, О.Є. ПЕТРЕНКО, О.С. ФРОЛОВ

В роботі розглянуто способи зменшення обчислювальної складності методу Т. Сато обчислення порядку еліптичної кривої. Наведено методику тестування програмного комплексу генерації загальносистемних параметрів для криптографічних перетворень на еліптичних кривих, який застосовує вдосконалений метод обчислення порядку кривої.

The paper considers some ways of minimizing computational complexity of the T. Sato method of computing the elliptic curve order and provides methods of testing the software complex of generating general system parameters for cryptographic elliptic curve transformations which uses the improved curve order computation method.

ВСТУП

Криптографічні системи на еліптичних кривих набули поширеного використання в сучасних криптографічних додатках. В Україні криптоперетворення на еліптичних кривих використовують для формування цифрового підпису та при розробці протоколів управління ключами. Державний стандарт ДСТУ 4145-2002 [1] при формуванні цифрового підпису використовує базові точки, максимальний порядок яких дорівнює 2^{431}. У зв'язку з постійно триваючим удосконаленням методів та засобів криптоаналізу виникає необхідність в побудові загально системних параметрів з певним запасом стійкості. З огляду на це виникає необхідність в поповненні бази криптографічно стійких еліптичних кривих для стандарту ДСТУ 4145-2002. Для поповнення бази криптографічно стійких еліптичних кривих необхідно розробити математичну модель генерації загальносистемних параметрів, яка дає можливість подолати існуючи обмеження та виконувати обчислення порядку кривих, які визначені на полях вимірністю від 2^{431} до 2^{1024}. Трудомістким етапом даної моделі є етап генерації криптографічно стійких еліптичних кривих. Вказаний етап включає наступні кроки:

випадково обирають коефіцієнти рівняння кривої;

обчислюють її порядок;

перевіряють криву на придатність до застосування в криптоперетвореннях.

Етап визначення порядку кривої є одним з трудомістких кроків при побудові еліптичних кривих. Для здійснення вказаного етапу в роботі [2] було проаналізовано існуючі методи обчислення порядку випадкової кривої. Метод Т. Сато [3] по показникам обчислювальної складності, просторової складності та швидкодії є найкращим, в порівнянні з усіма іншими [2].

Зменшення обчислювальної складності перетворень завжди було актуальним питанням, а при здійснені перетворень в полі $GF\left(2^n\right)$, для значення $n \geq 431$ це питання стає особливо важливим. Метою даної роботи є зменшення обчислювальної складності обчислення порядку кривої, яка визначена на полі $GF\left(2^n\right)$ для значення $n \geq 431$. Розробка програмного комплексу генерації загальносистемних параметрів для криптосистем на еліптичних кривих, який оснований на даної моделі. Генерація загальних параметрів для криптографічних перетворень на полях $GF\left(2^n\right)$ для значення $n \geq 431$.

1. СПОСОБИ ЗМЕНШЕННЯ ОБЧИСЛЮВАЛЬНОЇ СКЛАДНОСТІ МЕТОДУ ОБЧИСЛЕННЯ ПОРЯДКУ КРИВОЇ

Метод Т. Сато, який покладено в основу програмно-технічного комплексу подано у роботі [3] не в повному обсязі. Відомості про основні етапи методу, які наведено в роботі [3], не містять обгрунтувань щодо дійсності та справжності перетворень, які виконують на етапі обчислення сліду відображення ендоморфізма Фробеніуса. В результаті використання вказаного методу для генерації криптографічно стійких еліптичних кривих без додаткових досліджень неможливо. При здійснені аналізу складності виконання кожного етапу даного методу [3] було знайдено напрямки зменшення обчислювальної складності перетворень при обчисленні сліду відображення ендоморфізму Фробеніуса.

Згідно математичної моделі, наведеної в роботі [4], підняття еліптичних кривих до кільця Z_{2^n} виконують за допомогою підняття j-их інваріантів даних кривих. На основі отриманих значень j-их інваріантів обчислюють коефіцієнти піднятих кривих. Рівняння даних кривих в результаті перетворень має наступний вид:

$$y^2 + xy = x^3 + a, \qquad (1)$$

де $a \in Z_{2^n}$.

Для обчислення сліду відображення ендоморфізму Фробеніуса необхідно, щоб рівняння еліптичної кривої мало вид:

$$y^2 + xy = x^3 + Ax + B, \qquad (2)$$

де $A \in Z_{2^n}$, $B \in Z_{2^n}$. Отримати рівняння (2), використовуючи рівняння (1), можливо за допомогою ізоморфного відображення між еліптичними кривими [5]. В роботі [3] пропонують для виконання вказаного обчислення застосовувати рівняння виду:

$$y^2 = x^3 - \frac{1}{48}x + \frac{1}{864} + a\,. \qquad (3)$$

Слід зазначити, що рівняння (1) та (2) – це рівняння кривих, які визначені на розширенні поля характеристики два, а рівняння (3) – це рівняння еліптичної кривої, яка визначена на простому полі. Здійснений аналіз складності методу знаходження порядку кривої, запропонованого в роботі [3] з використанням рівняння (3), показав, що складність обчислення порядку кривої дорівнює

$$(17nk + 10n)M + I + L\,, \qquad (4)$$

де M – це операція множення в кільці Z_{2^n}, k – це 2-адична точність, $L = \left(2^{n+1} - 2^2\right)$ – кількість операцій піднесення до квадрату в полі $GF\left(2^n\right)$.

Рівняння (3) – це рівняння кривої, яка визначена на полі характеристики p, де p – просте число, яке не дорівнює двом. Ніяких обґрунтувань щодо існування ізоморфізму між кривими (1) та (3) робота [3] не містить. Також немає ніяких доведень можливості використання кривої (3) для знаходження порядку кривої (1). Тому, при побудові математичної моделі генерації загальносистемних параметрів криптосистем на еліптичних кривих питання можливості застосування еліптичної кривої (3) не вирішено. Вирішити дане питання можливо за допомогою доведення існування ізоморфізма між кривими (1) та (3), або за допомогою пошуку альтернативного перетворення рівняння кривої (1) до кривої виду (2).

Рівняння кривої (1) можна привести до кривої виду (2) завдяки використанню рівняння еліптичної кривої, наведеної в роботі [5] виду:

$$y^2 + xy \equiv x^3 - \frac{36}{J - 1728}x - \frac{1}{J - 1728}\,, \qquad (5)$$

де J – j-ий інваріант кривої, яка визначена в кільці Z_{2^n}. Крива виду (5) має той же самий j-ий інваріант, що і крива виду (1). Згідно роботи [5] дані криві ізоморфні.

При використанні рівняння (5) складність обчислення порядку кривої дорівнює:

$$(13nk + 10n)M + I + L\,, \qquad (6)$$

де M – це операція множення в кільці Z_{2^n}, k – це 2-адична точність, $L = n$ – кількість операцій піднесення до квадрату в полі $GF\left(2^n\right)$.

2. ВИБІР ПАРАМЕТРІВ ДЛЯ РЕАЛІЗАЦІЇ КОМПЛЕКСУ, ОПИС ВХІДНИХ ТА ВИХІДНИХ ДАНИХ

Використовуючи вдосконалений метод обчислення порядку кривої та умови придатності еліптичних кривих для криптографічних перетворень, було розроблено програмний комплекс, який спроможний генерувати загальносистемні параметри з певним запасом стійкості.

До вхідних даних програмного комплексу належать поле, на якому визначена крива та коефіцієнти рівняння еліптичної кривої. Поля, на яких визначають еліптичні криві, це розширення поля характеристики два. Степень розширення поля, з огляду на існуючі вимоги безпеки, належать проміжку від 163 до 1024. Поле задають за допомогою незведеного полінома виду:

$$f(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0\,, \qquad (7)$$

де n – ступень розширення поля, a_i дорівнюють або нулю або одиниці. Коефіцієнти рівняння еліптичної кривої $y^2 + xy = x^3 + ax^2 + b$ обирають таким чином:

1) коефіцієнт a згідно стандарту [1] дорівнює або нулю або одиниці;

2) коефіцієнт b є випадковим елементом розширення поля характеристики два заданого ступеня n. Даний елемент задають за допомогою полінома виду:

$$f(t) = t^m + b_{m-1}t^{m-1} + \ldots + b_0\,, \qquad (8)$$

де m – ступень полінома, який належить проміжку від 1 до n, b_i дорівнюють або нулю або одиниці ($i = 0,1,\ldots,m-1$).

Вибір незведеного полінома здійснюють за допомогою стандарту x9.62[6]. Далі обирають коефіцієнти рівняння еліптичної кривої a, b для здійснення ініціалізації алгоритму.

Вибір коефіцієнта a одразу дозволяє визначити кофактор криптографічно стійкої еліптичної кривої. Якщо $a = 1$, тоді кофактор кривої дорівнює двом. Якщо $a = 0$, тоді кофактор дорівнює чотирьом. Значення коефіцієнта b обирають випадковим чином. При виборі коефіцієнту b бажано використовувати генератор випадкових послідовностей, тому що результат виконання залежить від випадковості даного коефіцієнту. Значення b не перевищує порядку обраного незведеного полінома.

До вихідних даних програмного комплексу належать порядок даної еліптичної кривої, координати та порядок базової точки кривої, інформація стосовно можливості використовування даної кривої в криптографічних додатках.

Порядок визначеної кривої обчислюють за допомогою метода Т. Сато, з урахуванням запропонованої в даній роботі засобу зменшення обчислювальної складності.

Час обчислення порядку кривої безпосередньо залежить від ступеня розширення поля. В табл. 1 наведено дані про залежність часу обчислення порядку кривої від ступеня незведеного полінома.

Таблиця 1

Залежність часу обчислення порядку від ступеня незведеного полінома

Ступень незведеного полінома	Час обчислення порядку кривої (год.)
163	0.05
367	0.5
509	2
577	4
617	8
1024	52

При виконанні обчислення порядку кривої було використано ПЕОМ Intel core 2140 1,6 Ghz 512 Mb ОЗУ Windows SP2. Програма була реалізована на мові С#. В результаті роботи даного програмного комплексу було виконано обчислення порядку випадкових кривих, які визначені над полями $GF\left(2^{509}\right), GF\left(2^{577}\right), GF\left(2^{617}\right)$. Кожна з цих кривих проходила тестування на придатність застосування в криптографічних перетвореннях.

Як приклад, наведемо загальні параметри для поля $GF\left(2^{617}\right)$.

```
Parameter a = 1
Parameter b = 209cd3e7553532151a3a997c89
72000f38dbedc7a3cf094f72e9ccdd9cfe4fd2ab
078611b2491b63d4edbc8f573ff75bd32804ebde
55dbb205cd5c02c22b338590b81453bfedeef8c1
a90f16dd
Polinom  = 617 200 0
Field  = 617
cofactor = 2
Base Point
X = 50ffdb84720b88f88dbdbf49b965f886d181
234027dbec67fd2b3adafd2e5e95e1f9b
d6f00de11883ded2bc86c14f05a499d93
9d07ce31b02f253a69f85129e8a753115
b4852473ee21eae9f9d
Y  =  13e268b3ed7e50310c1e23d59316fea40
a64
83c3484b7dc1433b327c056fe31f6435c
0c9afaa224c5d59a5b1e35bc0ba65f162
bc205d95670470f2585bd10bcba2ae425
7d6a1fbfd4de71e538cb
Order of Point = fffffffffffffff
ffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffff3cc72
214f9d3105cbb8d877641d14c04f16a01
d3f7a643a5747fc3887ff21b92e4b15e2
437099
Order of Curve = 1ffffffffffffff
ffffffffffffffffffffffffffffffff
fffffffffffffffffffffffffffffe798e
4429f3a620b9771b0eec83a29809e2d40
3a7ef4c874ae8ff8710ffe43725c962bc
486e132
```

3. МЕТОДИКА ТЕСТУВАННЯ ЕЛІПТИЧНИХ КРИВИХ НА ПРИДАТНІСТЬ ЗАСТОСУВАННЯ В КРИПТОПЕРЕТВОРЕННЯХ

Методика тестування надає порядок перевірки правильності програмної реалізації усіх етапів генерації загальносистемних параметрів. Наведена методика передбачає, що на попередньому етапі була здійснена перевірка правильності реалізації алгоритмів виконання основних арифметичних операцій в розширенні кільця 2 – адичних цілих степені n та в розширенні поля характеристики два степені n, які складають основу реалізації методу обчислення порядку кривої. Крім того, методика тестування була перевірена на кривих, запропонованих в роботі [1].

Методика тестування загальносистемних параметрів, отриманих за допомогою еліптичної кривої на придатність застосування в криптографічних перетвореннях, здійснювалася за наступними етапами:

- перевірка на простоту порядку випадково генерованої еліптичної кривої;
- перевірка виконання mov- умови;
- перевірка кривої на аномальність;
- перевірка кривої на виродженість.

На першому етапі тестування здійснювали перевірку порядку кривої на простоту. Здійснення перевірку на простоту можливо завдяки детермінованим та імовірносним алгоритмам. Детерміновані алгоритми дозволяють однозначно з'ясувати чи є число простим. Детермінований алгоритм, наведений в роботі [7] при перевірці числа на простоту, обчислює порядки еліптичних кривих визначених на полі характеристики p. В зв'язку з тим, що в теперішній час не існує швидкодіючих алгоритмів обчислення порядку еліптичних кривих, визначених на простому полі, використання детермінованого алгоритму не є доцільним. Використовуючи імовірнісні алгоритми при перевірці числа на простоту, зробити висновок просте чи складене число, можна з деякою імовірністю. Багатократне його повторення для того ж самого числа, але з різними параметрами дозволяє зменшити ймовірність помилки до малої величини. При тестуванні еліптичних кривих було використано імовірністний тест Міллера – Рабіна, наведений в роботі [7].

Наступним етапом тестування є етап перевірки MOV умови. Згідно даним, наведеним в роботі [6], еліптична крива проходить тест на MOV атаку, якщо виконана умова:

$$2^{nt} - 1 \neq 0 \bmod r, \qquad (9)$$

де n – ступень розширення поля, $t = 1, 2, ..., B$, верхня границя безпеки для значення $B \in [20, 30]$, r – порядок базової точки .

Далі виконують перевірку кривої на аномальність. Якщо крива визначена на розширені поля характеристики два, тоді вона не є аномальною, якщо ступень розширення n є простим числом. Згідно діючого стандарту [1], в Україні розглядають тільки прості степені розширення.

Останній етап тестування є етап виконання перевірки кривої на виродженість. Крива є не виродженою, якщо виконана наступна умова:

$$j \equiv 0 \bmod 1728, \qquad (10)$$

де j є j-им інваріантом еліптичної кривої.

Якщо еліптична крива задовольняє усім умовам тестування, її вважають придатною до застосування в криптографічних додатках. В такому випадку обчислюють порядок базової точки. Процес генерації загальносистемних параметрів завершено. У випадку не виконання хоча б однієї з наведених умов, обирають нові значення коефіцієнтів еліптичної кривої, обчислюють її порядок та перевіряють виконання усіх етапів тестування. Ме-

тодику тестування було перевірено на еліптичних кривих, які запропоновані стандартом [1]. Крім того, в процесі тестування випадкових кривих отримано нові загальносистемні параметри над полями $GF\left(2^{509}\right), GF\left(2^{577}\right), GF\left(2^{617}\right)$.

ВИСНОВКИ

З огляду на те, що на теперішній час не існує відкритих публікацій про нові алгоритми обчислення порядку кривої та програмні продукти, які дозволяють отримувати загальносистемні параметри для криптографічних перетворень в групах точок еліптичних кривих, розробка даного програмного комплексу дозволяє вирішити деякі актуальні питання. А саме питання, які пов'язані з генерацією загальних параметрів для криптоперетворень в групах точок еліптичних кривих з певним запасом стійкості. Крім того, здійснений порівняльний аналіз складності обчислення порядку кривої (4), (6) показав, що при застосуванні запропонованого рівняння (5) кількість операцій множення в кільці Z_{2^n} зменшено в 1,3 рази. А це в свою чергу зменшило складність обчислення порядку кривої в порівнянні з методами, наведеними в відкритих публікаціях.

Література.

[1] *ДСТУ 4145–2002* Національний стандарт України. Інформаційні технології Криптографічний захист інформації цифровий підпис, що грунтується на еліптичних кривих.

[2] *О.Є. Ілясова.* Порівняльний аналіз методів обчислення порядку еліптичної кривої при генерації параметрів для криптосистем на еліптичних кривих //Радіоелектронні і комп'ютерні системи. –2007. – № 7 (26). – С. 129–133.

[3] *Fouquet M., Gaudry P. and. Harley R* . An extention of Satoh's algorithm and its implementation, J. Ramanujan Math. Soc. 15 2000, p. 281–318.

[4] *Горбенко І.Д., Ілясова О.Є.* Математичне моделювання процесів побудови параметрів еліптичних кривих для криптографічних перетворень // Радіоелектронні і комп'ютерні системи. – 2006. – № 6 (18). – С. 27–31.

[5] *Silverman J.H.* The arifmetic of Elliptic Curve // GTM 106, Springer – Verlad, New–York, 1986. – 385 p.

[6] *X9.62* Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). ANSI, 1998.

[7] *Н. Коблиц.* Курс теории чисел и криптографии // М.: Научное изд-во ТВП, 2001. – 254 с.

Надійшла до редколегії 10.08.2008

Погребняк Константин Анатолійович, аспірант каф. БІТ ХНУРЕ, математик ЗАТ «ІІТ». Область наукових інтересів: елиптична криптографія.

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

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