УДК 681.3.06

О.Є. ПЕТРЕНКО, О.С. ФРОЛОВ

Харківський національний університет радіоелектроніки, Україна

ПОБУДОВА ЗАГАЛЬНОСИСТЕМНИХ ПАРАМЕТРІВ НА ПОЛЯХ ХАРАКТЕРИСТИКИ Р ДЛЯ КРИПТОСИСТЕМ НА ЕЛІПТИЧНИХ КРИВИХ

Розглянуто засоби скорочення часу, який витраченого на побудову загальносистемних параметрів для криптосистем на еліптичних кривих. Запропоновано метод обчислення модулярних поліномів, за допомогою яких досягнуто скорочення часу.

Ключеві слова: *загальносистемні параметри, модулярні поліноми, решітки, поліноми ділення.*

Вступ

Актуальним проблемним питанням сьогодення є розробка методів та створення алгоритмів побудови загальносистемних параметрів, що базуються на перетвореннях в групах точок еліптичних кривих для полів характеристики p, де p – просте число. Задача, яка пов'язана з створенням на їх основі відповідних стандартів пригортає увагу спеціалістів в багатьох країнах світу. Стандарти побудови загальносистемних параметрів для перетворень на еліптичних кривих існують лише в проекті. Проблемність їх створення пов'язана з неприйнятною обчислювальною складністю існуючих методів обчислення порядку еліптичних кривих, які визначені на полях $GF(p), GF(2^n), GF(p^n)$. Дані методи є самою трудомісткою складовою, що використовують при даному процесі. В теперішній час використовують в криптографічних системах на еліптичних кривих загальносистемні параметри, що частково наведені в стандартах [1 – 4], вони мають певні обмеження на порядок базової точки для полів $GF(2^n)$ та полів $GF(p)$. Постійно триваюча робота спеціалістів в цьому напрямку спрямована на зменшення обчислювальної складності методів та підвищення швидкодії алгоритмів та програмних продуктів, що на них базуються. Розроблений та представлений в роботі [5] метод обчислення порядку еліптичної кривої на відміну від інших [6 – 8] спроможний за прийнятний час обчислити порядки еліптичних кривих, які мають базові точки, порядок яких від 2^{509} до 2^{1024}. Слід зазначити, що і він має недоліки, а саме низьку швидкодію алгоритмів, які створено за його допомогою при роботі з полями вимірності, що перебільшує 2^{509} та неможливість його застосування на полях $GF(p)$.

Мета роботи: розробка методу та засобу, які спроможні підвищити швидкодію алгоритмів, що на них базуються та зменшити час, який витрачено на побудову загальносистемних параметрів.

1. Засоби підвищення швидкодії процесу побудови загальносистемних параметрів

Розроблені методи побудови загальносистемних параметрів передбачають отримання еліптичної кривої придатної для застосування в криптографії, а потім побудови за її допомогою загальносистемних параметрів. Можна виділити два способи отримання необхідної кривої. Їх сутність полягає в наступному:

1) здійснення генерації простого числа і потім отримання відповідного рівняння еліптичної кривої для подальшої перевірки її на придатність застосування в крипто перетвореннях;

2) випадковим чином вибір еліптичної кривої, з'ясування чи має вона базову точку простого порядку, потім перевірки її на стійкість до крипто аналітичних атак.

Другий спосіб має певні переваги у порівнянні з першим. Це пов'язано з тим, що застосовуючи перший спосіб не завжди є можливість отримати криву на визначеному полі. В зв'язку з чим другий спосіб частіше використовується. До головного недоліку другого способу слід віднести то, що при випадковому виборі еліптичної кривої неможливо сказати заздалегідь придатна еліптична крива до застосування чи ні, не виконав обчислення її порядку. Обчислення порядку є самим трудомістким етапом при побудові параметрів. Наприклад, здійснюючи побудову параметрів на полях $GF(2^n)$ необхідно здійснити вибір із 2^{n+1} кривих, при цьому невідомо яка по черзі крива буде придатною для використання в криптографічних додатках. В зв'язку з тим, що дані

поля при $n > 509$ не досліджувалися на наявність кривих придатних до застосування, тому в деяких випадках доведеться перевіряти усі криві вид яких передбачений стандартом [4]. Дана перевірка займає багато часу та використовує значні ресурси. Прискорити процес побудови параметрів на полях $GF(p), GF(2^n), GF(p^n)$ можливо шляхом відбраковування кривих з малими простими порядками на початковому етапі, не здійснюючи пошук її порядку. Для отримання абсцис точок l крутіння слідуючи роботі [6] використовують поліноми ділення наступного виду:

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

де коефіцієнти a, b в співвідношенні є параметрами еліптичної кривої. За їх допомогою отримано поліноми:

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

Доцільність застосування поліномів (2) основана на властивості, яка полягає в тому, що точка еліптичної кривої $P = (x,y)$, ордината якої не дорівнює нулю є точкою n крутіння тоді і лише тоді, коли $f_n(x) = 0$ для усіх $n > 3$. Основний недолік використання поліномів два полягає в тому, що його степінь $\frac{l^2 - 1}{2}$. Виходячи з цього, наприклад, для значення $p \approx 2^{200}$ максимальне значення l дорівнює 191, а степінь поліномів ділення 18240.

Використовуючи стратегію представленою в роботі [9], можливо здійснити інший підхід для отримання координат точок l крутіння. Її сутність полягає в застосуванні модулярних поліномів для відбракування еліптичних кривих, які мають малий простий порядок не виконуючи його обчислення, який. Крім того її можливо застосовувати для будь-якого з полів. Модулярні поліноми $\Phi_l(x,y)$, означення яких наведено в роботі [6], мають ступень $l+1$ та наступний вигляд:

$$\Phi_l(X,Y) = X^{l+1} + Y^{l+1} - X^l Y^l + \\ + \sum_{\substack{0<i<l-1 \\ 0<j<l-1}} a_{ij}\left(X^i Y^j\right) + F, \quad , \quad (3)$$

де $i + j < 2l$, $a_{ij}, F \in Z$. Властивість даних поліномів дозволяє з'ясувати має обрана еліптична крива точку крутіння порядку l чи ні. не виконуючи обчислення її порядку. Якщо еліптична крива, яка визначена на полі $GF(q)$, має jінваріант j_E і рівняння $\Phi_l(x, j_E) = 0$ не має коренів в цьому полі, тоді дана крива не має точок крутіння порядку l. Виходячи з цього можливо не виконуючи обчислення порядку відбракувати криві, які мають малий простий порядок базової точки.

Для здійснення даної стратегії необхідно побудувати модулярні поліноми для значення $l = 2,3,5,7,...,\hat{A}$. Далі вибрати еліптичну криву та обчислити її j-ий інваріант. Підставити отримане значення в рівняння $\Phi_l(x, j_E) = 0$ та знайти його корені в полі, на якому дана крива визначена. На основі отриманих результатів вирішити обчислювати порядок еліптичної кривої чи генерувати нову криву та повторювати операцію.

Недоліком застосування модулярних поліномів слід вважати зростання їх коефіцієнтів при зростанні значення l, так вільний член полінома $\Phi_2(x,y)$ дорівнює 157 000 000 000, а вільний член полінома $\Phi_3(x,y)$ дорівнює 1855425871872000000000.

Позбутися вказаного недоліку можливо шляхом використання канонічних модулярних поліномів, які мають значно менші коефіцієнти. Так, наприклад, поліном $\Phi_2(x,y)$ має вигляд:

$$\Phi_2(X,Y) = X^3 + Y^3 - X^2Y^2 + \\ +2^4 \cdot 3 \cdot 31\left(X^2Y + XY^2\right) - \\ -2^4 3^4 5^3\left(X^2 + Y^2\right) + 3^4 5^3 \cdot 4027XY \\ +2^8 3^7 5^6 \cdot (X + Y) - 2^{12} 3^9 5^9,$$

а відповідний йому канонічний модулярний поліном:

$$\Phi_2(x, j_E) = (x + 16)^3 - j_E x.$$

Для здійснення даної стратегії необхідно розробити метод спроможній обчислювати модулярні поліному для будь-якого простого значення $l = 5,7,...,\hat{A}$, де $\hat{A}$ – граничне просте число.

Далі скласти із них базу даних, яку в подальшому застосовувати для відбір кування еліптичних кривих з малим простим порядком базової точки.

2. Метод побудови модулярних поліномів

Розглянемо множину усіх лінійних комбінацій комплексних чисел $1, \tau = \frac{\varpi_1}{\varpi_2}$, які не належать одній прямій та проходять через початок координат (грати). Їх вибір здійснимо таким чином, щоб $\operatorname{Im}\tau = \operatorname{Im}\frac{\varpi_1}{\varpi_2} > 0$.

Будь-яка еліптична крива, що визначена на полі комплексних чисел ізоморфна решітці. Також розглянемо спеціальну групу матриць другого порядку, які мають одиничний детермінант $\left(SL_2(Z)\right)$.

Елементу $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(Z)$ поставимо в відповідність дробово-лінійне відображення $\tau g = \frac{a\tau + b}{c\tau + d}$, яке описує множину лінійних комбінацій комплексних чисел (грати).

За допомогою даного відображення можливо визначити еліптичні криві на решітках.

Використовуючи $\gamma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ побудуємо базис решіток $(1,\tau),(1,\gamma\tau)$ його використання надає можливість побудувати для еліптичних криві мероморфних функції j-их інваріантів таким чином, що в першому випадку $j(\tau) = j(-1/\tau)$, а в другому $j(\tau) = j(\tau + 1)$.

В останньому випадку дана

$$j(q) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \ldots, \quad (4)$$

де $q = \exp(2\pi i\tau), n \in Z$.

Властивість модулярних поліномів (3) полягає в тому, що їх корені є j-ми інваріантами $l+1$ ізогенних еліптичних кривих [13].

Застосовуючи формулу (4) для ізогенних кривих з j-ми інваріантами $j(\tau l), j\left(\frac{\tau + k}{l}\right)$, $k = 0,1,\ldots,l-1$ отримаємо наступний вигляд мінімального полінома для j-х інваріантів [13]:

$$H_l(x, j(\tau)) = (x - j(l\tau)) \prod_{k=0}^{l-1} \left(x - j\left(\frac{\tau + k}{l}\right)\right). \quad (5)$$

Згідно з теоремою, доведеною в [10], даний поліном можна привести до полінома, що зберігає властивості модулярного полінома має корені

$$j(\tau l), j(\tau + k/l), k = 0,1,\ldots,l-1$$

та вигляд:

$$\Phi_l(X, j_E) = \sum\sum a_{ik} j^i(E)\left(X^k\right), \quad (6)$$

де $a_{ik} \in Z$. Для обчислення коефіцієнтів полінома (6) застосовують функцію Дедекінда [11] виду

$$\eta(\tau) = \frac{1}{24}\prod\left(1 - q^n\right). \quad (7)$$

Використовуючи (5) та (6), можливо отримати цілі значення коефіцієнтів модулярного полінома (3) для кожного простого значення l. Для отримання коефіцієнтів канонічних модулярних поліномів необхідно застосовувати функцію $\omega = \eta\left(\frac{\tau}{l}\right)/\eta(\tau)$.

Висновки

Застосування модулярних поліномів, дозволяє зменшити час, що використовується при обчисленні параметрів за рахунок відбору еліптичних кривих з малим простим порядком не виконуючи самого обчислення порядку. Самі модулярні поліноми згідно з обраним способом їх побудування можна обчислити окремо та скласти з них базу даних з подальшим її застосуванням.

Напрямок подальших досліджень є розробка методу та засобів обчислення коефіцієнтів канонічн медулярних поліномів для простих значень $l > 2$.

Література

1. IEEE P 1363-2000. Standard Specification for public key cryptography, 2000.

2. 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.

3. American National Standard X9.63-2000. Public key cryptography for the financial services industry: Key agreement and key transport using elliptic curve cryptography, 2000.

4. ISO/IEC 15946. Information technology – Security techniques – Cryptographic techniques based on elliptic curves.

5. Бондаренко М.Ф., Розробка методу обчислення порядку еліптичної кривої для побудови параметрів надвисокого рівня стійкості / М.Ф. Бондаренко, О.Є. Петренко, О. С. Фролов // Прикладная радиоэлектроника. Тематический выпуск. – 2009.

6. Schoof R. Counting points on an elliptic curve over finite fields / R. Schoof // Proc. Journees Arithmetiques, 1995. – № 93. – P. 219-252.

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

8. Fouquet M. An extension of Satoh's algorithm and its implementation / M. Fouquet, P. Gaudry, R. Harley // Ramanujan Math. Soc., 2000. – Vol. 15. – P. 281-318.

9. Fouquet M. Finding secure curves with the Satoh-FGH algorithm and an Early-abort strategy. / M. Fouquet, P. Gaudry and R. Harley // In proceedings of Eurocrypt, LNCS 2045. – Sprenger Verlag, 2001. – P. 14-29.

10. Muller V. Die Berechnund der puntanzach ellipticher kurven uber endlichen korpern de characterictih grober / V. Muller // In proceedings of Eurocrypt, LNCS 2095. – Sprenger Verlag, 2002. – P. 35-79.

11. Коблиц Н. Курс теории чисел и криптографии / Н. Коблиц // М.: ТВП, 2001. – 254 с.

Надійшла до редакції 8.02.2010

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

ПОСТРОЕНИЕ ОБЩЕСИСТЕМНЫХ ПАРАМЕТРОВ НА ПОЛЯХ ХАРАКТЕРИСТИКИ P ДЛЯ КРИПТОСИСТЕМ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

О.Е. Петренко, О.С. Фролов

Рассмотрены способы сокращения времени при построении общесистемных параметров для криптографических систем на эллиптических кривых. Предложен метод построения модулярных полиномов, с помощью которых улучшено время построения параметров.

Ключевые слова: модулярные полиномы, решетки, полиномы деления.

CONSTRUCTION OF PARAMETERS IN THE FIELDS OF CHARACTERISTIC P FOR CRYPTOSYSTEMS ON THE ELLIPTIC CURVES

O.E. Petrenko, O.S. Frolov

Approaches have been considered of cancellation of time by construction of parameters for cryptosystems by elliptic curves. The method of construction modular polynomial has been proposed with assistance of which the time of construction of parameters was improved.

Keywords: modular polynomials, lattice, polynomial of division.

Петренко Ольга Евгеньевна – канд. техн. наук, ст. преподаватель кафедры высшей математики Харьковского института банковского дела, младший научный сотрудник Харьковского национального университета радиоэлектроники, Украина.

Фролов Олег Сергеевич – аспирант кафедры безопасности информационных технологий Харьковского национального университета радиоэлектроники, Украина email: frolovoleg85@gmail.com.