УДК 681.3.06

І.Д. ГОРБЕНКО, О.Є. ІЛЯСОВА

ЗАТ "Інститут інформаційних технологій", Україна

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ПРОЦЕСІВ ПОБУДОВИ ПАРАМЕТРІВ ЕЛІПТИЧНИХ КРИВИХ ДЛЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

Розглянуто математичну модель обчислення порядку еліптичної кривої над полем $GF\left(2^n\right)$ для криптографічних додатків. Обгрунтовано умову вибору коректного значення сліду ендоморфізму Фробеніуса над полем $GF\left(2^n\right)$.

еліптична крива, слід ендоморфізму Фробеніуса, модулярний поліном, порядок кривої

Вступ

Бурхливий розвиток комп'ютерної техніки та комп'ютерних мереж сприяв розповсюдженню інформаційних технологій та їх використанню в усіх галузях діяльності сучасного суспільства. Завдяки мережі Internet виникли нові технологічні можливості, які підвищують ефективність виробничих процесів та сприяють поширенню ділових операцій в сфері бізнесу. Виник новий спосіб ділової взаємодії – електронний бізнес. А разом з виникненням електронного бізнесу актуальною стала задача захисту інформаціїї, яка формується та зберігається в електронному вигляді. Для забезпечення цілісності, справжності, неспростовності, конфіденційності інформаціїї та протидії несанкціонованому доступу використовують криптографічні системи захисту інформації. На сьогодні перспективними є криптосистеми, що використовують перетворення в групі точок еліптичної кривої. Поширення використання криптосистем, що базуються на перетвореннях в групі точок еліптичної кривої пов'язано з забезпеченням необхідного рівня безпеки та швидкодією таких систем, а також з можливістю їх використання для систем, що реалізують інфракструктуру відкритих ключів. Однак, для подальшого розповсюдження таких криптосистем необхідно проводити роботу в напрямку удосконалення методів перетворень та генерації загальних параметрів, які мінімізують обчислювальну складність перетворень та в одночас забезпечують необхідну стійкість системи до криптоаналізу.

Математичний аппарат, який використовують для виконання перетворень в группі точок елліптичної кривої хоча постійно і удосконалюється але проблема зменшення обчислювальної складності перетворень залишається актуальною. Особливо проблемними є питання, які пов'язані з удосконаленням методів генерації загальносистемних параметрів над полем $GF\left(2^n\right)$. Це пов'язано з тим, що державний стандарт України ДСТУ 4145–2002 розроблено тільки для розширення полів характеристики два, а теоретичні дослідження та реалізація систем формування загальних параметрів є недостатніми. Тому однією із найбільш важливих є задача пошуку сприйнятного за просторовою та часовою складністю та криптографічною стійкостю метода обчислення порядку еліптичної кривої над розширенням поля характеристики два. Відомі дослідження в основному спрямовані на побудову математичної моделі для обчислення порядку еліптичної кривої на основі алгоритму T. Satoha [1]. Відомості про цей алгоритм, а також про математичний апарат, який застосовують в ньому, є неповними та потребують ряду уточнень і додаткових досліджень.

Мета даної статті: побудова математичної моделі обчислення загальних параметрів еліптичної кривої над полем $GF\left(2^n\right)$. Обгрунтування коректного обчислення сліду ендоморфізму Фробеніуса над розширенням поля характеристики два для кривої

$$y^2 + xy = x^3 + A\,.$$

Математична модель побудови загальних параметрів еліптичної кривої над полем $GF(2^n)$

Розглянемо декілька означень, необхідних для опису математичної моделі обчислення порядку еліптичної кривої над розширенням поля характеристики два. Якщо рівняння еліптичної кривої задано у загальному вигляді

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\,, \qquad (1)$$

де коефіцієнти $a_i, i = 1, 2, ..., 6$ є цілими числами, тоді рівняння виду

$$y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'\,, \qquad (2)$$

де $a_i', i = 1, 2, ..., 6$ є образ коефіцієнтів $a_i, i = 1, 2, ..., 6$ рівняння (1) в полі $GF(2)$ називається редукцією кривої по модулю 2. Для визначення поняття підняття еліптичної кривої та її точок, розглянемо означення, які наведено в роботі [2]. Еліптична крива $E(K)$ яка задана рівнянням Вейерштрасса

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

над числовим полем K може бути зведена по модулю p. Координати кожної кінцевої точки кривої $E(K)$ можна привести до пари дробів з цілими раціональними знаменниками. Редукція кривої по модулю p в цьому випадку задається відображенням

$$\varphi : E(K) \to E\left(GF\left(p\right)\right).$$

З іншого боку крива

$$E\left(GF\left(p\right)\right): y^2 \equiv x^3 + A'x + B' \left(\mathrm{mod}\ p\right) \qquad (4)$$

може бути вкладена в криву $E(K)$. Відображення точки $Q \in E\left(GF\left(p\right)\right)$ в точку $Q' \in E\left(K\right)$ називається підняттям точки Q з поля $GF\left(p\right)$ в поле K, при цьому порівняння (4) перетворюються в рівняння (3) над полем K [2]. Аналогічні перетворення можна виконати для підняття еліптичної кривої з розширеного поля характеристики два до кільця Z_{2^n}. В роботі [3] наведено визначення ізогенії як відображення морфізму між еліптичними кривими

$$\phi : E_1 \to E_2, \phi\left(O\right) = O\,.$$

Дуальне відображення морфізму – це відображення

$$\phi' : E_2 \to E_1\,.$$

Ядром изогенії є підгрупа скінченного порядку точок еліптичної кривої E_1. Алгоритм запропонований в [1] передбачає:

1. Обчислення j інваріанта базової кривої E_0.
2. Побудову циклу спряжених кривих

$$E_i, E_n = E_0, i = 1, 2, ..., n$$

та обчислення j інваріантів кривих.

3. Обчислення j інваріантів $J_i, i = 0, 1, ..., n-1$ піднятих кривих. Відтворення коефіцієнтів рівняння піднятих кривих за допомогою $J_i, i = 0, 1, ..., n-1$.

4. Визначення координат точки з ядра ендоморфізму Фробеніуса $V_i' : E_i' \to E_{i-1}'$, де E_i' криві отримані в результаті підняття кривих E_i.

5. Обчислення сліду ендоморфізма Фробеніуса trV з відтворених даних.

6. Знаходження порядку еліптичної кривої.

Для виконання першого етапа алгоритму розглянемо базову криву E_0, яка визначена над полем $GF\left(2^n\right)$ та обчислимо j-ий інваріант кривої з використанням формул [4]. Далі будуємо послідовність еліптичник кривих

$$E_0 \leftarrow E_1 \leftarrow E_2 \leftarrow ... \leftarrow E_{n-1} \leftarrow E_n, \mathrm{E}_0 = E_n\,. \qquad (5)$$

Послідовність (5) отримана в результаті дії малого ендоморфізму Фробеніуса $\sigma: x \mapsto x^2$ [1] на коефіцієнти попередньої кривої, тобто наведеної послідовності (5) у вказаному порядку, *j*-ії інваріанти яких пов‘язані наступним співвідношенням

$$j_i^2 = j_{i+1} \bmod 2 .$$

Третій етап підняття кривих, що складають послідовність (5) є одним з найскладніших етапів алгоритму. Результатом виконання перетворень цього етапу є послідовність кривих

$$E_0' \leftarrow E_1' \leftarrow E_2' \leftarrow ... \leftarrow E_{n-1}' \leftarrow E_n', E_0' = E_n' , \quad (6)$$

за умови, що вказані криві задовольняють $\pi\left(E_i'\right) = E_i, i = 0, 1, ..., n-1$, де π – редукція кривої. Обчислені J_i – j інваріанти кривих E_i', задовольняють співвідношенню $J_i \equiv j_i \bmod 2, i = 0, 1, 2, ..., n-1$. Для отримання рівнянь кривих з послідовності (6) необхідно знайти J_i. Знаходження J_i базується на використані властивостей модулярного полінома [1]

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

та теореми Lubin – Serre – Tate [1]:

Теорема. Нехай E еліптична крива, яка задана над полем F_{p^2}, j інваріант якої задовольняє умові $j(E) \notin F_{p^2}$. Тоді існує J з кільця p – адичних цілих Z_{p^n} такий, що $\Phi_p\left(J, \sigma^{-1}(J)\right) = 0, J \equiv j \bmod p$, де J – це j інваріант піднятої кривої.

В теоремі $\sigma^{-1}(J)$ – відображення що зворотнє, відображенню малого ендоморфизму Фробеніуса, а $\Phi_p(x, y)$ – модулярний поліном Використовучи послідовність кривих (6) у вказаному порядку можна запобігти обчислення $\sigma^{-1}(J)$ та знайти $J_i, i = 0, 1, ..., n-1$ з системи із n рівнянь наступного вигляду: $\Phi_2(J_i, J_{i+1}) = 0$. Одна з найважливіших задач на цьому етапі полягає у пошуку коренів рівнянь з якомога більшою точністю. Уточнення кореню рівняння можна виконати за допомогою ітерацій Ньютона. Після розв‘язку задачі знаходження j –их інваріантів піднятих кривих, наступний етап алгоритму пов‘язаний з пошуком коефіцієнтів піднятих кривих. Обчислення коефіцієнтів A_i, B_i рівнянь кривих

$$y^2 + xy = x^3 + A_i x^2 + B_i$$

з послідовності (6) виконується за допомогою j – их інваріантів J_i. Значення A_i згідно стандарту ДСТУ 4145 – 2002 дорівнює нуль або один, а значення B_i можна отримати в результаті розв‘язку рівняння

$$432J_i x^2 - J_i x + 1 = 0$$

у випадку коли $A_i = 0$ та рівняння

$$432J_i x^2 - 25J_i x - 125 = 0$$

у випадку коли $A_i = 1$ [4].

Послідовність кривих (5), як вже було наведено вище можна отримати в результаті дії малого ендоморфізму Фробеніуса $\sigma: x \mapsto x^2$. Відображення

$$V_i' : E_i' \to E_{i-1}'$$

в результаті якого можна отримати послідовність кривих (6), що діє над кільцем 2-адичних цілих, не є простим піднесенням до квадрату коефіцієнтів кривих. Для побудови цього відображення необхідно розглянути композицію двох відображень $V_i' = \varphi \circ \lambda$. Відображення

$$\varphi : E_i' \to E_i' / \ker V_i' ,$$

переводить точки еліптичної кривої E_i' в підгрупу точок другого порядку, які утворюють ядро ізогенії V_i' над полем $GF(2^n)$. Ізогенне відображення φ можна побудувати на основі формул наведених в роботі [5]. Але використання формул з [5] можливо лише в випадку, коли відомі нетривіальні точки з ядра V_i' ($P_i = (x_i, y_i) \in \ker V_i'$). Для того, щоб отримати координати точки необхідно виконати підняття

точки крутіння 2 порядку до кільця 2-адичних цілих. Відображення λ є відображенням точок з ядра ізогенії V_i' в точки кривої E'_{i-1}, тобто

$$\lambda : E'_i / \ker V'_i \to E'_{i-1}.$$

Даний ізоморфізм λ визначається наступним співвідношенням координат

$$(\bar{x}, \bar{y}) = \left(g_i^2 x, g_i^3 y\right)$$

[3]. Для побудови ізоморфізму необхідно знайти значення g_i. Якщо скористатися рівнянням ізогенії:

$$y^2 + xy = x^3 + Ax + B$$

та рівнянням кривої

$$E'_i : \bar{y}^2 + \bar{x}\bar{y} = \bar{x}^3 + \bar{A}_{i-1}\bar{x} + \bar{B}_{i-1},$$

тоді значення g_i можна обчислити за наступним співвідношенням [3]

$$g_i^2 = \frac{B\bar{A}_{i-1}}{A\bar{B}_{i-1}}. \qquad (7)$$

Розглядаючи перехід до формальної групи точок еліптичної кривої, можна знайти зв‘язок між коефіцієнтами g_i та слідом ендоморфізму Фробеніуса над полем $GF(2^n)$. Для цього побудуємо формальну групу точок еліптичної кривої. Нехай задано рівняння еліптичної кривої у загальному вигляді (1). Розглянемо параметри

$$z = -\frac{x}{y} \quad \text{та} \quad w = -\frac{1}{y}.$$

Рівняння (1) можна записати таким чином:

$$w = z^3 + a_1 zw + a_2 z^2 w + a_3 w^2 + \\ + a_4 zw^2 + a_6 w^3 = f(z, w). \qquad (8)$$

Використовуючи співвідношення (8) та розглядаючи послідовність [3]:

$$f_1(z, w) = f(z, w);$$
$$f_{n+1}(z, w) = f_n(z, f(z, w)),$$

отримаємо ряд. Розкладання змінних x, y в ряди, які наведено в [3]

$$x = z^{-2} - a_1 z^{-1} - a_2 - a_3 z - (a_1 a_3 + a_4) z^2 + O\left(z^3\right); \qquad (9)$$

$$y = -z^{-3} + a_1 z^{-2} + a_2 z^{-1} + a_3 + \\ + (a_1 a_3 + a_4) z + O\left(z^2\right) \qquad (10)$$

дає змогу побудувати формальну групу точок еліптичної кривої. Пара $(x(z), y(z))$ є формальним розв‘язком рівняння (1).

Використовуючи відображення λ із заданим співвідношенням координат

$$(\bar{x}, \bar{y}) = \left(g_i^2 x, g_i^3 y\right)$$

та формули (9), (10), знайдемо вплив λ на параметр $z = -\frac{x}{y}$

$$\lambda(z) = -\frac{g_i^2\left(z^{-2} + O\left(z^{-1}\right)\right)}{g_i^3\left(-z^{-3} + O\left(z^{-2}\right)\right)} = \frac{1}{g_i} z + O\left(z^2\right). \qquad (11)$$

Згідно з твердженням 1.2 з [3] маємо, що у формальній групі точок еліптичної кривої

$$z \circ \lambda = \sum_{n=1}^{\infty} c_n z^n \quad \text{та} \quad tr\lambda = c_1, i + \frac{1}{c_1, i}.$$

З співвідношення (11)

$$\frac{1}{g_i} = c_1, i \ . \qquad (12)$$

Відомо, що ізоморфне відображення та ізогенне відображення не змінює порядок еліптичної кривої, а це означає, що не змінюється і слід ендоморфізму Фробеніуса. Використовуючи (5), можна знайти слід ендоморфізму Фробеніуса над полем $GF\left(2^n\right)$ як добуток з n множників кожний з яких дорівнює сліду відображення малого ендоморфізму Фробеніуса між кривою E'_{i-1} та кривою E_i', $i = 1, 2, ..., n-1$.

Слід ендоморфізму Фробеніуса (trV) над полем $GF\left(2^n\right)$ обчислюється за формулою:

$$trV = \prod_{i=0}^{n-1} c_{1,i} \ . \qquad (13)$$

Зрозуміло, що обчислення проводиться за відповідним модулем.

В зв‘язку з тим, що формула (12) дає два значення g_i, виникає необхідність обрання коректного

значення. Обґрунтуємо вибір значення g_i кривої, яка задана рівнянням

$$y^2 + xy = x^3 + A. \qquad (14)$$

Згідно оцінки Хассе [4] порядок еліптичної кривої E $(\#E)$ обчислюється за формулою

$$\#E = 2^n + 1 - trV, \qquad (15)$$

де trV дорівнює сліду ендоморфізму Фробеніуса над полем $GF\left(2^n\right)$.

Твердження. Точка P з координатами $\left(\sqrt[4]{A}, \sqrt{A}\right)$ еліптичної кривої

$$y^2 + xy = x^3 + A$$

є точка, порядок якої дорівнює чотирьом.

Доведення. Точка $P_1 = \left(0, \sqrt{A}\right)$, яка належить кривій (14), це точка другого порядку, тому що вона задовольняє умові $P_1 = -P_1$, згідно правилу обчислення координат точки, зворотної даної, над розширенням поля характеристики два. Для доведення існування точки четвертого порядку необхідно знайти точку $B = (x, y)$, яка задовольняє співвідношенню

$$2B = P_1.$$

Визначення координат точки $B = (x, y)$ над полем $GF\left(2^n\right)$ здійснюється за допомогою формул [4]:

$$\begin{aligned} 0 &= v^2 + v; \\ \sqrt{A} &= x^2. \end{aligned} \qquad (16)$$

Абсциса точки $B = (x, y)$ згідно з формулою (16) дорівнює $\sqrt[4]{A}$.

Використовуючи рівняння кривої (14) знайдемо ординату точки. Ордината дорівнює $\sqrt{A}$. Порядок точки з координатами $\left(\sqrt[4]{A}, \sqrt{A}\right)$ дорівнює 4.

Відомо, що порядок кривої ділиться на порядок точки, яка належить даній кривій, тоді порядок кривої (14) ділиться на 4.

Це означає, що вираз

$$(1 - trV)$$

з формули (15) можна поділити на 4, тому для вибору коректного значення сліду ендоморфізму Фробеніуса достатньо перевірити умову

$$trV \equiv 1 \pmod 4. \qquad (17)$$

Перевіривши умову (17) порядок кривої обчислюється за формулою (15) .

Висновки

Запропоновано обґрунтування математичної моделі обчислення порядку еліптичної кривої, що дозволяє обчислювати порядок випадково згенерованої еліптичної кривої. Роботу по подальшому вдосконаленню наведеної моделі необхідно спрямувати на пошук значень j інваріантів піднятих кривих.

Література

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

2. Ростовцев А.Г. Логарифмирование через поднятие // Проблемы информационной безопасности. Компьютерные системы. – С.-Пб. – 2000. – № 2. – С. 49-54.

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

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

5. Velu J. Isogenies entre courbes elliptiques // C.R. Acad. Sc. Paris. – 1971. – 273. – P. 238-241.

Надійшла до редакції 15.02.2006

Рецензент: д-р техн. наук, проф. В.І. Долгов, Харківський національний університет радіоелектроніки.