АСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ – АНАЛИЗ И СИНТЕЗ

УДК 681.3.06

ПРОБЛЕМНІ ПИТАННЯ ТА МАТЕМАТИЧНІ АСПЕКТИ ПОБУДУВАННЯ ПАРАМЕТРІВ ДЛЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

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

В статті наведено математичну модель обчислення квадратного кореня в полі 2-адичних цілих, складової одного з трудомістких етапів обчислення порядку еліптичної кривої, визначеної на полі $GF\left(2^n\right)$ та здійснено обґрунтування вибору початкових умов, необхідних для виконання даної операції, що дозволяє будувати загальносистемні параметри для криптографічних перетворень надвисокого рівня стійкості.

Ключові слова: математична модель, криптографічне перетворення, стійкість, еліптична крива, поле.

ВСТУП

Сучасне ділове життя країни неможливо уявити без застосування інформаційних технологій та глобальної мережі Internet. Бурхливий розвиток електронного банкінга, електронної комерції, електронного документообігу вимагає постійного вдосконалення методів та засобів захисту інформації, яка зберігається та передається по каналам зв'язку в електронному вигляді. Криптографічні перетворення є засобом забезпечення цілісності, справжності та автентичності інформації. Побудова загальносистемних параметрів для здійснення даних перетворень, які відповідають сучасним умовам криптографічної стійкості, є актуальними практичними питаннями з одного боку та проблемними теоретичними питаннями з другого. Проблемність питання пов'язана з необхідністю забезпечення прийнятної складності перетворень та криптографічної стійкості параметрів.

Загальносистемні параметри, що застосовують перетворення в групах точок еліптичних кривих є одним з перспективних напрямків дослідження завдяки особливим властивостям їх точок. Привабливість даних кривих полягає в тому, що з їх допомогою можливо будувати параметри, які забезпечують усі прийняті в Україні рівні стійкості. Крім того, дані параметри з прийнятною часовою складністю можливо застосовувати не тільки в асиметричних, але і в комбінованих криптосистемах.

Незважаючи на зручність застосування криптографічних перетворень в групах точок еліптичних кривих існують питання, які потребують розв'язання. Одним з головних є питання розробки математичних методів побудування цих параметрів зі зменшеною часовою та просторовою складністю зі збереженням їх криптографічної стійкості. Головною складовою цих методів є методи обчислення порядків еліптичних кривих, що визначені на полях вимірності більше ніж 2^{512} та вибору серед них криптографічно стійких, з подальшим їх застосуванням для побудування параметрів. Додатковою проблемою є те, що програмні реалізації вказаних методів повинні мати прийнятну просторовою, часову складність, а параметри побудовані з їх допомогою бути криптографічно стійкими. Необхідні умови забезпечення стійкості параметрів наведені в роботах[1, 2]. Слід зазначити, що сучасні методи та засоби криптоаналізу вимагають застосовувати параметри з порядком базової точки 2^{509} та вище, а методів побудування таких параметрів з прийнятною просторовою та часовою складністю в країні не існує. Згідно з проведеним в роботі [3] аналізом методів обчислення порядку кривої обрано перспективний метод (алгебраїчно-геометричних значень), який можливо при певних умовах застосовувати для обчислення порядку кривих з порядком базової точки 2^{509} та вище. В роботах [3, 4], було розглянуто ряд питань пов'язаних зі створенням алгоритмів виконання основних етапів метода обчислення порядку кривої. Не розв'язаними залишились питання вилучення квадратного кореня та обчислення порядку кривої в розширенні поля 2-адичних чисел Q_{2^n} .

Метою даної роботи є математичне обґрунтування методу вилучення кореня в розширені поля 2-адичних чисел та введення умов, що дозволяють здійснювати вказане обчислення з одного боку та отримувати з двох можливих значень кореня таке, яке дозволить обчислити порядок кривої, яка визначена над розширенням поля $GF\left(2^n\right)$ з другого.

1. МАТЕМАТИЧНЕ ОБГРУНТУВАННЯ АЛГОРИТМУ ОБЧИСЛЕННЯ КВАДРАТНОГО КОРЕНЯ В Q_{2^n}

Порядок еліптичної кривої $\#E$, яка визначена в розширенні поля характеристики два $GF\left(2^n\right)$ та має рівняння $y^2 + xy \equiv x^3 - \bar{\alpha} \bmod\left(2^k, f(x)\right)$, обчислюється за формулою:

$$\#E = 2^n + 1 - tr(Fr),$$

де $tr(Fr)$ – це слід відображення Фробеніуса. Згідно з роботою [4] $tr(Fr) = \prod \frac{2a_i}{a_i + b_i}$. Значення a_i, b_i при застосуванні методу алгебрично-геометричних значень [3, 4] є елементами розширення поля 2-адичних цілих ступеня n та визначаються наступним чином:

$$\begin{aligned} &a_0 = 1 + 8\alpha, b_0 = 1 \\ &a_{i+1} = \frac{a_i + b_i}{2}, b_{i+1} = \sqrt{a_i b_i}, \end{aligned} \quad (1)$$

де $\alpha \in Q_{2^n}$ та задовольняє умові $\alpha = \bar{\alpha} \pmod 2$.

Елементи поля 2-адичних цілих чисел мають вид:

$$\beta = \sum_{i=0}^{\infty} a_i 2^i, \quad (2)$$

де a_i приймають значення або нуль або одиниця.

Для того, щоб вилучити $\sqrt{\beta}, \beta \in Q_2$ необхідно виконати наступні дії:

– записати β у вигляді $\sum_{i=0}^{m} a_i 2^i$, де кожне значення a_i визначено однозначно;

– представити β у вигляді $\left(\sum_{i=0}^{\infty} b_i 2^i\right)^2$;

– визначити усі b_i з рівності $\sum_{i=0}^{m} a_i 2^i = \left(\sum_{i=0}^{\infty} b_i 2^i\right)^2$.

В роботі [5] розглянуто метод пошуку квадратного кореня в полі Q_2, сутність якого полягає в пошуку усіх значень b_i таким чином:

1. Із порівняння $b_0 \equiv a_0^2 \pmod 2$ визначаємо значення b_0.

2. На основі отриманого значення b_0 знаходимо значення b_1 із порівняння відповідних коефіцієнтів при 2^2 в рівності

$$\left(b_0 + b_1 \cdot 2 + b_2 \cdot 2^2 + \ldots\right)^2 = a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \ldots$$

Отриманий результат має вигляд:

$$b_0 b_1 2^2 = a_2 2^2 \left(\bmod 2^3\right) \text{ або } b_0 b_1 = a_2 \left(\bmod 2\right). \quad (3)$$

3. Продовжуючи процес пошуку коефіцієнтів, як показано в п. 2, знаходимо коефіцієнти b_i ряду $\sum_{i=0}^{\infty} b_i 2^i$.

Слід зазначити, що коефіцієнти b_i визначені однозначно після вибору коефіцієнта b_0. Значення b_0, із порівняння обирають або 1 або 0. Вказаний метод випливає з доведення Лемми Гензеля [5], яку називають p-адичною леммою Ньютона пошуку кореня многочлена. Перевага леми Гензеля в тому, що за її допомогою завжди можливо отримати значення кореня полінома з p-адичними коефіцієнтами, що неможна сказати про метод Ньютона.

Проблемність пошуку квадратного кореня в полі p-адичних чисел полягає в тому, що не для усіх елементів цього поля існують квадратні корені. Тобто не завжди можливо отримати значення b_0 на першому кроці алгоритму. Другим проблемним питанням є те, що при обчисленні порядку еліптичної кривої ми вилучаємо квадратний корінь в розширенні поля p-адичних чисел для значення p=2. Для здійснення вказаної операції необхідно, спираючись на метод, запропонований в роботі [5], запропонувати метод вилучення квадратного кореня в розширенні поля 2-адичних цілих Q_{2^n}. В даному полі обчислити значення квадратного кореня можливо за допомогою ітераційного процесу, наведеного в леммі Гензеля. Вказана лемма дозволяє обчислити $\sqrt{\beta}, \beta \in Q_{2^n}$ як корінь полінома $g(x) = \beta - x^2$. При його застосуванні пошук квадратного кореня $\sqrt{\beta}, \beta \in Q_{2^n}$ є трудомісткою задачею та здійснювати його таким чином недоцільно. Це пов'язано з тим, що в даному випадку потрібно застосовувати операцію інвертування в полі Q_{2^n} використовуючи формулу:

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

Як відомо з роботи [3, 4], операція інвертування в розширенні поля 2-адичних цілих здійснюється за формулою:

$$g_i^{-1}(x) = g_{i-1}^{-1}(x) - g_{i-1}^{-1}(x)\left(g_{i-1}^{-1}(x) \times g(x) - 1\right), \quad (5)$$

де $g(x)$ – це елемент, для якого ведеться пошук інверсійного елементу, $g_{i-1}^{-1}(x)$ – це елемент, який було отримано на попередньому етапі з точністю 2^{i-1}. При використанні формули (5) необхідно знати, чому дорівнює $g_0^{-1}(x)$. Отримати необхідне значення можливо, виконав наступні операції:

1. Обчислити значення елемента c_0 в полі $GF(2^n)$ за правилом $c_0 \equiv \beta \bmod\left(2, f(x)\right)$;

2. Знайти значення $\sqrt{c_0} \bmod\left(2, f(x)\right)$;

3. Здійснити операцію пошуку інверсійного елементу для елемента $\sqrt{c_0} \bmod\left(2, f(x)\right)$ в полі $GF(2^n)$, застосовуючи метод, наведений в роботі [6].

В результаті $g_0(x) = \frac{1}{\sqrt{c_0}} \bmod\left(2, f(x)\right)$ – це початковий елемент ітераційного процесу (5).

Після того, як знайдено значення початкового елементу ітераційного процесу, обчислення кореня здійснюється за формулою (5). Складність даного обчислення для кривих, які визначені на полях $GF\left(2^n\right)$, дорівнює $\frac{n^2(n+1)^2}{2}$ операціям множення в розширенні поля 2-адичних цілих. На пошук інверсійного елемента з заздалегідь заданою 2-адичною точністю $k = \left\lceil \frac{n}{2} \right\rceil$ необхідно виконати $\frac{n^2}{4}$ операцій множення. На рис. 1 зображено графік, який показує, як зростає кількість

операцій множення при обчисленні квадратного кореня в полі Q_{2^n} за допомогою формули (5). Вертикальна вісь показує порядок розширення поля, горизонтальна – скільки виконується операцій множення в полі Q_{2^n}.

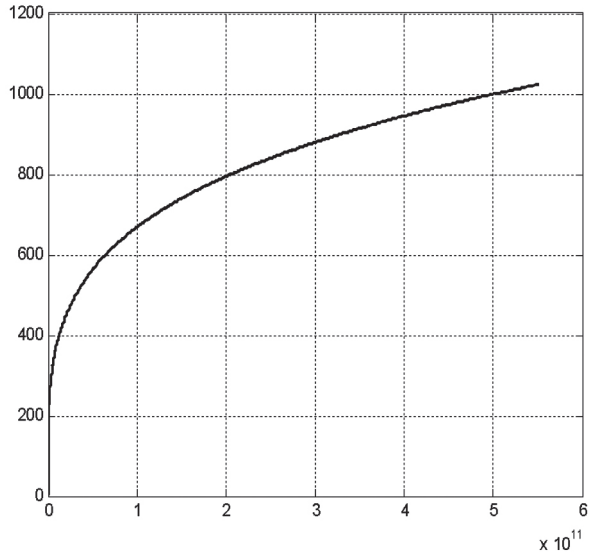

Рис. 1. Залежність кількості операцій множення від ступеня розширення поля

Позбутися інверсії при обчисленні квадратного кореня можливо, якщо використовувати поліном $g(x)=1-\beta(x)^2$. Ітераційний процес в такому випадку можна визначити за формулою:

$$x = ax + \frac{x\left(a-\beta(x)^2\right)}{2}. \qquad (6)$$

Використовуючи той факт, що $\sqrt{\beta}=\frac{\beta}{\sqrt{\beta}}$, значення квадратного кореня знаходиться за допомогою полінома $g(x)=\beta x+\frac{x\left(\beta-\beta(x)^2\right)}{2}$.

В такому випадку для обчислення квадратного кореня необхідно здійснити $4(n+1)^2$ операцій множення для еліптичних кривих, визначених на полях $GF\left(2^n\right)$. Таким чином, кількість операцій множення при застосуванні формули (6) зменшується в $\frac{n^2}{8}$ разів в порівнянні з кількістю операцій при застосуванні формули (5).

На рис. 2 зображено графік, що показує, як зростає кількість операцій множення при застосуванні формули (6) при обчисленні квадратного кореня в полі Q_{2^n}. Вертикальна вісь показує, який порядок розширення поля, горизонтальна – скільки виконується операцій множення в полі Q_{2^n}.

На рис. 3 у логарифмічному масштабі зображено графіки (1) та (2) зміни порядку виконання операцій множення при застосуванні формул (5) та (6). Графік (1) показує зміни порядку при застосуванні формули (5), графік (2) – (6).

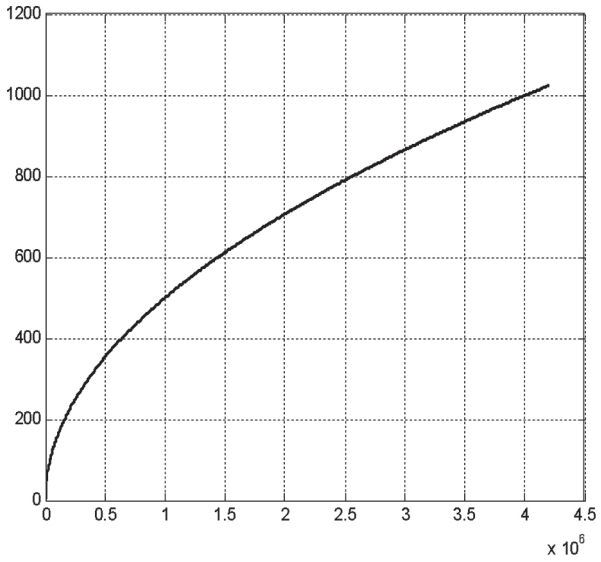

Рис. 2. Залежність кількості операцій множення від ступеня розширення поля

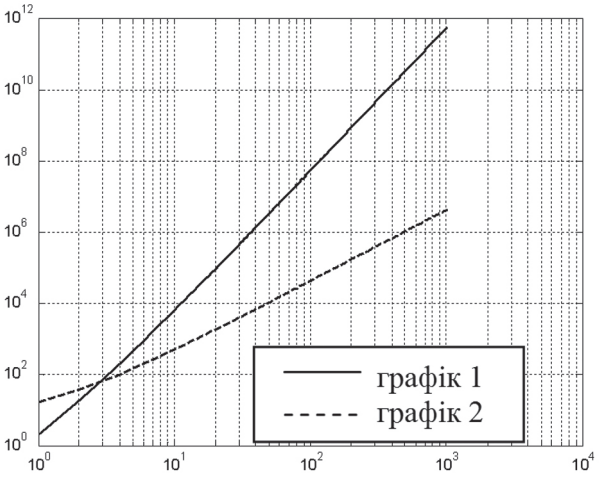

Рис. 3. Зміна порядку виконання операцій множення у логарифмічному масштабі

Побудова загальносистемних параметрів надвисокого рівня стійкості передбачає застосовувати еліптичні криві, які визначені на полях $GF\left(2^n\right)$, де $n>509$. Запропонований метод обчислення квадратного кореня в розширенні поля 2-адичних цілих за допомогою формули (6) дозволяє скорочувати час на побудову загальносистемних параметрів, але при його застосуванні слід враховувати той факт, що обчислення квадратного кореня здійснюється з подвоєнням 2-адичної точності на кожному кроці ітераційного процесу. Дане подвоєння точності має похибку, в результаті чого виникає необхідність вибору умов, які дозволять зменшити цю похибку та отримати точне значення квадратного кореня.

Для пошуку кореня даного полінома потрібно розв'язати два питання:

- для ітераційного процесу знайти початкове значення β_0, за допомогою якого буде знайдено значення кореня полінома $g(x)$;
- визначити умови, які б гарантовано давали змоги вилучити корінь із будь-якого елемента $\beta \in Q_{2^n}$;

• знайти умови, що дозволять позбутися похибки при здійсненні обчислення.

Для вирішення першого проблемного питання застосуємо той факт, що в скінченому полі $GF\left(2^n\right)$ будь-який елемент має квадратний корінь. Виходячи з цього, початкове значення β_0 можна обчислити таким чином:

• знайти елемент поля $GF\left(2^n\right)$, який задовольняє наступному порівнянню

$$\gamma \equiv \beta\left(\mathrm{mod}\left(2, f(x)\right)\right),$$

• обчислити β_0 за правилом $\frac{\gamma}{\sqrt{\gamma}}$, застосовуючи виконання операцій вилучення кореня, пошуку інверсійного елементу та операцію множення в розширенні поля характеристики 2 - $GF\left(2^n\right)$.

Умови, наведені вище, є необхідними, але не достатніми для операції вилучення квадратного кореня в полі Q_{2^n}. Для визначення достатніх умов необхідно враховувати той факт, що для будь-якого полінома $g(x)$ із розширенню кільця 2-адичних цілих та значення $\lambda \in Z_{2^n}$ існує абсолютне 2-адичне значення $\upsilon_2\left(g'(\lambda)\right)=2, \upsilon_2\left(g(\lambda)\right)=2+n.$ Застосовуючи дані абсолютні значення для елементів розширення поля 2-адичних цілих μ, та β, можна визначити наступні умови[5]:

$$1.\ \mu \equiv \lambda\left(\mathrm{mod}\left(2^n, f(x)\right)\right);$$

$$2.\ \beta \equiv \lambda - \frac{g(\lambda)}{g'(\lambda)}\left(\mathrm{mod}\left(2^i, f(x)\right)\right), i=\overline{2,2n}; \qquad (7)$$

$$3.\ \beta \equiv \mu\,\mathrm{mod}\left(2^{2n-2}, f(x)\right);$$

$$4.\ g(\beta) \equiv 0\,\mathrm{mod}\left(2^{2n}, f(x)\right);$$

$$5.\ \upsilon_2\left(g'(\beta)\right)=2.$$

Згідно з умовою (7) за допомогою лемми Гензеля ми отримаємо значення квадратного кореня з 2-адичною точністю, яка дорівнює $2n-2$, але для обчислення порядку еліптичної кривої значення квадратного кореня повинно мати 2-адичну точність $2n$. З огляду на це достатньою умовою для отримання кореня необхідної точністю буде умова, яка дозволяє здійснити апроксимацію початкового значення β_0 по модулю $\left(2^2, f(x)\right)$ для ініціалізації ітераційного процесу, який застосовується при обчисленні квадратного кореня.

Далі, використовуючи лемму Гензеля та визначені умови (7), здійснюємо ітераційний процес (6) та знаходимо корінь полінома

$$g(x)=\beta x+\frac{x\left(\beta-\beta(x)^2\right)}{2}.$$

Наведені вище умови дозволяють знаходити значення кореня для будь-якого $\beta \in Q_{2^n}$.

ВИСНОВКИ

Запропонований метод вилучення квадратного кореня та визначені початкові умови дозволять здійснити програмну реалізацію методу алгебраїчно-геометричних значень зі зменшеною в $\frac{n^2}{8}$ разів складністю для еліптичних кривих, які визначені на розширенні поля характеристики два ступеня n ($GF\left(2^n\right)$), що дозволить побудувати загальносистемні параметри для криптографічних перетворень в групах точок еліптичних кривих на полях вимірності більше, ніж 2^{509} з прийнятною часовою та просторовою складністю.

Література

[1] *Петренко О.Є.* «Умови вибору параметрів еліптичних кривих для криптографічних додатків», журнал «Прикладная радиоэектронника», Том 6 №3, 2007г.; м.Харків: ХНУРЕ- С.363-365.

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

[3] *Петренко О.Є., Фролов О.С.* «Побудова загальносистемних параметрів на полях характеристики Р для криптосистем на еліптичних кривих» Науково-технічний журнал «Радіоелектронні і комп'ютерні системи», Харків: ХАІ, випуск 5 (46) 2010 р. – С. 57-60.

[4] *Бондаренко В. Ф., Петренко О.Є., Фролов О.С.* «Розробка методу обчислення порядку еліптичної кривої для побудови параметрів надвисокого рівня стійкості», журнал «Прикладная радиоэлектроника», 2009, Том 8, №3, м. Харків: ХНУРЕ. С.296-299.

[5] *H. Cohen, C Frey* Handbook of elliptic end hyperelliptic curve cryptografy // Carman end hall / CRC – 2006, – 843 p.

[6] *Горбенко І.Д,. Гриненко Т.О.* Захист інформації в інформаційно-телекомунікаційних системах. Част. 1. Криптографічний захист інформації – Харків: ХНУРЕ, 2004. – 367 с.

Надійшла до редколегії 06.04.2011

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

Петренко Ольга Євгенівна, старший викладач ХІБС Університету банківської справи НБУ. Область наукових інтересів: генерування загальносистемних параметрів в криптосистемах, що базуються на перетвореннях в групі точок еліптичних кривих.

Фролов Олег Сергійович, аспірант кафедри БІТ ХНУРЕ. Область наукових інтересів: криптосистеми, що базуються на перетвореннях в групі точок еліптичних кривих.

УДК 681.3.06

Проблемные вопросы и математические аспекты построения параметров для криптографических преобразований / М.Ф. Бондаренко, О.Е. Петренко, О.С. Фролов // Прикладная радиоэлектроника: науч.-техн. журнал. – 2011. Том 10. № 2. – С. 159–163.

В статье приведены математическая модель вычисления квадратного корня в поле 2-адичних целых, составляющей одного из трудоемких этапов вычисления порядка эллиптической кривой, определенной на поле $GF\left(2^n\right)$ и осуществлено обоснование выбора начальных условий, необходимых для выполнения данной операции, что позволяет строить общесистемные параметры для криптографических преобразований сверхвысокого уровня устойчивости.

Ключевые слова: математическая модель, криптографическое преобразование, устойчивость, эллиптическая кривая, поле.

Іл. 3. Библиогр.: 6 назв.

UDC 681.3.06

Issues of concern and mathematical aspects of constructing parameters for cryptographic transformations / M.F. Bondarenko, O.E. Petrenko, O.S. Frolov // Applied Radio Electronics: Sci. Journ. – 2011. Vol. 10. № 2. – P. 159–163.

The paper represents a mathematical model of calculating the square root over Q_{2^n}. That is part of labour-intensive stages of computating the order of the elliptic curve over $GF\left(2^n\right)$ It denotes conditions which are necessary for fulfilling this operation. This model allows to construct general-system parameters for cryptographic transformations of superhigh stability level.

Keywords: mathematical model, cryptographic transformation, stability, elliptic curve, field.

Fig. 3. Ref.: 6 items.