УДК 681.3.06

О.Є. Петренко

Харківський інститут банківської справи Університету банківської справи Національного банку України, Харків

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ОБЧИСЛЕННЯ ПОРЯДКУ ЕЛІПТИЧНИХ КРИВИХ ЗА ДОПОМОГОЮ ПІДНЯТТЯ, ЩО ВИЗНАЧЕНІ НАД ПОЛЕМ F(2^n)

Розглянуто методи обчислення порядку еліптичної кривої за допомогою підняття та здійснено аналіз обчислювальної складності цих методів. Запропоновано метод обчислення порядку кривої зі зменшеною складністю.

Ключові слова: *еліптична крива, порядок еліптичної кривої, базова точка.*

Вступ

Сучасні криптографічні перетворення неможливо уявити без застосування еліптичних кривих. Еліптичні криві займають значне місце завдяки можливості забезпечити достатній рівень стійкості використовуючи ключові данні невеликої довжини та завдяки швидкодії алгоритмів, які базуються на перетвореннях в групі точок цих кривих. Для побудови криптосистем на еліптичних кривих потрібно знайти еліптичні криві з майже простим порядком над визначеним заздалегідь полем простої характеристики або над його розширенням. З моменту запропонування еліптичних кривих, у 1985 році, постійно триває робота по вдосконаленню методів обчислення порядку еліптичної кривої, що визначені над простими полями та їх розширенням. Особлива увага приділялася еліптичним кривим, що визначені над розширенням поля характеристики два ступеня вище ніж 2^{512}. На цей час кривих, що визначені над полями вказаної вимірності та представлених в стандартизованому вигляді, немає. Діючий в Україні стандарт ДСТУ 4145-2002 пропонує застосовувати еліптичні криві над полями найвища вимірність яких 2^{431}, міжнародні стандарти [1, 2] пропонують застосовувати еліптичні криві над полями вимірності до 2^{512}.

Для побудови комбінованих криптосистем, які застосовують симетричні та асиметричні перетворення для забезпечення стійкості необхідно застосовувати еліптичні криві, що визначені над полями вимірності до 2^{1024}. З огляду на це, проблемним питанням є питання отримання придатних до застосування в криптографічних перетвореннях еліптичних кривих, що визначені над розширеними полями вимірності від 2^{512} до 2^{1024}. Складність вирішення даного питання полягає в тому, що існуючі методи комплексного множення, SEA [3, 4] не спроможні вирішити дану задачу для полів визначеної вимірності з прийнятною складністю та швидкодією. Метод Сато [5] та його вдосконалення [6] дозволяють обчислювати порядки еліптичних кривих над визначеними полями. Вказаний метод, використовуючи криву над полем характеристики два, здійснює її підняття до розширення кільця 2-адичних цілих степеня m характеристики нуль. Дане підняття дозволяє обчислити порядок кривої над полем характеристики нуль та визначити порядок кривої над полем характеристики два.

Метод Сато, на відміну від детермінованих методів комплексного множення та SEA є ймовірнісним, який дозволяє обчислювати порядок випадкової кривої над обраним полем з заздалегідь невідомими властивостями. З огляду на це, невідомо скільки необхідно розглянути кривих над обраним полем та обчислити їх порядки, щоб знайти криву придатну для використання в криптосистемах. Придатність використання в криптосистемах обумовлена майже простим порядком еліптичної кривої В результаті для пошуку необхідної кривої, що визна-

чена над полем $F\left(2^n\right)$, може виникнути потреба в обчисленні порядків кривих, кількість яких становить до 2^{n+1}. Дане обчислення збільшує час на отримання потрібної кривої. Виникає проблемне питання, яке полягає в тому, що методи, які дозволяють будувати криві з обраними властивостями та порядком, неможливі для застосування для еліптичних кривих над полями вимірності більше ніж 2^{512}, а метод Сато спроможний обчислювати порядки кривих з прийнятною швидкодією але з невідомими заздалегідь властивостями. З огляду на це, збільшується час на пошук кривої придатної до застосування в криптографічних перетвореннях з необхідними властивостями.

Метою даної роботи є пошук методів та способів обчислення порядків кривих над полем $F(2^n)$ зі зменшеною, в порівнянні з методом Сато, кількістю операцій множення, які відповідають умовам застосування в криптографічних перетвореннях та можуть бути включені в державні стандарти.

Метод обчислення порядку еліптичної кривої за допомогою підняття

В роботі [7] представлена математична основа ще одного методу обчислення порядку кривої за допомогою підняття, загальна теорема Хассе-Вейля.

Теорема: нехай E – еліптична крива над полем $F\left(p^m\right)$ та N - порядок її групи. Тоді для порядку $N(n)$ групи еліптичної кривої $E\left(F\left(p^r\right)\right)$ над полем $F\left(p^m\right)$ виконується наступна формула $N(n)=p^m+1-\alpha^m-\beta^m$, де α,β є коренями квадратного рівняння (характеристичного рівняння ендоморфізма Фробеніуса) $x^2-tx+p=0$, де t - значення сліду ендоморфізма Фробеніуса, яке обчислюють за формулою $t=p+1-N$.

Зауваження: завжди виконується за умови теореми наступна нерівність: $t^2<4p$, тому α,β є комплексно спряженими коренями.

Алгоритм побудування еліптичних кривих передбачає виконання наступних кроків.

1. Обчислення порядку еліптичної кривої N над простим полем малого порядку $E\left(F(2)\right)$.

2. Визначення у бітах мінімального та максимального значення порядку еліптичної кривої над полем $F\left(2^m\right)$.

3. За допомогою рівняння $t=p+1-N$ здійснення вибору значень α,β таким чином, щоб $t=\alpha+\beta,\ p=\alpha\beta$.

4. Обчислення цілого значення $N_m=p^m+1-\alpha^m-\beta^m$ та перевірку умови $N>N_{max}$.

5. Отримання значення N - порядку еліптичної кривої $E\left(F\left(2^m\right)\right)$.

6. Знаходження базової точки еліптичної кривої порядку n.

7. Отримання рівняння еліптичної кривої.

8. Перевірку належності базової точки даної кривої.

В пункті 3 методу α,β обирають з характеристичного рівняння ендоморфізму Фробеніуса:

$$x^2-tx+2=0,$$

де t - значення сліду ендоморфізма Фробеніуса.

Знаходження $\alpha^m+\beta^m$ здійснено за допомогою рекурентних співвідношень. Дані співвідношення наведені в роботі [8] в наступній лемі.

Лема: Нехай $S_m=\alpha^m+\beta^m$. Тоді $S_0=2$, $S_1=t$, де t - значення сліду ендоморфізму Фробеніуса, $S_{n+1}=tS_n+qS_{n-1}$, де q – характеристика поля $F(q)$.

Застосування даної леми дозволяє на основі значення порядку еліптичної кривої, яка визначена на простому полі малої характеристики, знайти значення сліду відображення ендоморфізму Фробеніуса. Далі, застосовуючи вказане значення сліду відображення ендоморфізму Фробеніуса та характеристику поля, обчислити значення S_m. На виході отримати порядок еліптичної кривої, що визначена над розширенням поля малої характеристики.

Алгоритм, що створений за допомогою леми, яка наведена вище, дозволяє за допомогою рекурентних співвідношень швидко знаходити порядки кривих над розширеннями поля малої характеристики (особливо характеристики два) та перевіряти отримане значення порядку на простоту. Слід зазначити, що при застосуванні даного алгоритму ми знаємо порядок кривої, але потрібно знайти коефіцієнти рівняння еліптичної кривої. На основі значення порядку кривої можливо визначити порядок базової точки. Обираючи випадкові точки з поля, на якому визначена еліптична крива, є можливим знайти точку, для якої скалярне множення її на порядок базової точки дасть нам нескінченно віддалену точку. Для визначення чи є дана точка базовою необхідно, щоб її координати задовольняли рівнянню еліптичної кривої. Представлений вище алгоритм обчислення порядку еліптичної кривої на основі підняття кривої, що визначена над полем $F(2)$, до кривої, що визначена над розширенням цього поля степені m, дозволяє швидко знаходити порядок кривої, але

потім потрібно отримати рівняння цієї кривої. Рівняння кривої дозволяє перевірити належить цій кривій знайдена базова точка чи ні.

Побудувати рівняння еліптичної кривої за умови того, що відомий її порядок, можливо за допомогою поліномів Гільберта [3]. На першому кроці знаходимо цілі значення D, V, де D - вільно від квадратів. Вказані значення задовольняють наступному співвідношенню:

$$8-\left(1+2^m-N\right)^2=DV^2,$$

де N - порядок кривої. Далі знаходять значення $t=2^m+1-N$, де N - порядок кривої $E\left(F(p)\right)$, p - вимірність поля, на якому визначена крива.

Число D - це фундаментальний дискримінант, на основі його і будують поліноми Гільберта $P_D(x)$. Розв'язок порівняння $P_D(x)=0 \bmod 2^m$, що належить полю $F\left(2^m\right)$, є j-м інваріантом еліптичної кривої $E\left(F\left(2^m\right)\right)$. Квадратична форма фундаментального дискримінанта визначається трійкою цілих значень $a, b, c: b^2-4ac=-D$. Між квадратичною формою та її коренями τ існує відповідність, що визначається виразом $\tau=\dfrac{-b+\sqrt{-D}}{2a}$. Кількість квадратичних форм з даною властивістю створює скінчену множину $H(-D)$. Порядок $H(-D)$ і є найвищий ступень полінома Гільберта. Введення операції над квадратичними формами дозволить створити Абелеву групу. Корені квадратичних форм з цієї множини τ_k визначають поліном Гільберта [3] за наступною формулою:

$$H_D(x)=\prod_{k=1}^{h}\left(x-j(\tau_k)\right);$$

$$j(\tau)=\frac{\left(256\theta(\tau)+1\right)^3}{\theta(\tau)};$$

$$\theta(\tau)=\frac{\Delta(2\tau)}{\Delta(\tau)}.$$

Складові даної формули обчислюють, застосовуючи теорію комплексних чисел, наступним чином:

$$\Delta(\tau)=$$

$$=e^{2\pi\tau i}\left(1+\sum_{n=1}(-1)^n\left(e^{\frac{2\pi\tau in(3n-1)}{2}}+e^{\frac{2\pi\tau in(3n+1)}{2}}\right)\right)^{24}=$$

$$=e^{2\pi\tau i}\left(1+\sum_{n=1}(-1)^n\left(e^{\pi\tau in(3n-1)}+e^{\pi\tau in(3n+1)}\right)\right)^{24}.$$

Використовуючи поліном Гільберта, розв'язують порівняння $P_D(x)=0 \bmod p$. Його розв'язок, який належить полю $F\left(2^m\right)$, є j-м інваріантом еліптичної кривої $E\left(F(p)\right)$.

Використовуючи отримане значення j-го інваріанта ($j\neq 0$, $j\neq 1728$), є можливість отримати рівняння еліптичної кривої за допомогою формули, що наведена в роботі [8]:

$$y^2+xy=x^3+\frac{36}{1728-j}x+\frac{1}{1728-j}.$$

Пошук коефіцієнтів рівняння еліптичної кривої потрібен для застосування еліптичної кривої в криптосистемах. Для цього застосування необхідно виконання наступних умов:

– скалярне множення точки поля, на якої визначена крива, на порядок цієї точки повинен дорівнювати нескінченно віддаленої точки;

– координати точки повинні задовольняти рівнянню еліптичної кривої.

Аналіз існуючих методів обчислення порядку еліптичних кривих за допомогою підняття

Метод Сато, згідно з роботами [5, 6], є методом, який має найменшу обчислювальну складність в порівнянні з методами Скуфа та комплексного множення. При обчисленні порядку еліптичної кривої за допомогою підняття здійснено підняття еліптичної кривої, яка визначена над розширенням поля характеристики два до кривої, яка визначена над розширенням поля 2-адичних цілих характеристики нуль. Для обчислення порядку еліптичної кривої, що визначена над розширенням поля характеристики два, необхідно виконати згідно з роботою [7] $D_1(m)=\dfrac{17m^2}{2}+10m$ операцій множення в полі $GF\left(2^m\right)$.

Як зазначалось вище, під час пошуку кривої, придатної до застосування, може виникнути потреба в обчисленні порядків усіх кривих, що визначені над полем $GF\left(2^m\right)$. Тоді складність пошуку необхідної кривої збільшиться в залежності від того, яка по рахунку крива виявиться придатною для застосування. Тоді даний метод втрачає свою перевагу та стає непривабливим при побудові кривих, визначених над розширенням поля характеристики два степеня більше ніж 2^{512}.

Запропонований в статті метод передбачає підняття еліптичної кривої, яка визначена над простим полем характеристики два, до розширення поля характеристики два ступеня m. З огляду на це, обчи-

слювальна складність методу, на відміну від методу Сато, зменшується завдяки тому, що представлення елементів поля $F\left(2^m\right)$ та правила виконання дій простіші ніж представлення елементів поля 2-адичних цілих та правила виконання дій в ньому. В результаті складність методу, що розглянутий в статті, передбачає виконання меншого числа операцій множення. В даному методі для обчислення поліному Гільберта необхідно виконання 2-х операцій інвертування в полі $F\left(2^m\right)$. Одна операція інвертування, згідно з оцінкою методів виконання інверсії в полі, вимагає здійснити близько вісімдесяти операцій множення [9]. Крім того, при побудові поліному Гільберта необхідно виконати таку кількість операцій множення, яка виражена деякою константою, яка залежить від фундаментального дискримінанту та не залежить від ступеня розширення поля. Для обчислення порядку кривої необхідно виконати $2m$ операцій множення. В результаті кількість операцій множення при обчисленні порядку кривої запропонованим методом має лінійну залежність та може бути виражена формулою $D_2(m) = 2m + c$, де $c = \text{const}$.

Висновки

Запропонований в статті метод побудування еліптичної кривої виконує усі операції над полем $F\left(2^m\right)$ на відміну від метода Сато, при застосуванні якого усі операції здійснюють над розширенням поля 2-адичних цілих характеристики нуль. В результаті виконання операцій в полі $F\left(2^m\right)$ зменшується обчислювальна складність даного методу. Крім того, кількість операцій множення, яку необхідно виконати для обчислення порядку кривої запропонованим методом, має лінійну залежність від ступеня розширення поля, а в методі Сато – квадратичну.

З огляду на це, запропонований метод на відміну від метод Сато, дозволяє швидко знайти порядок кривої, а після перевірки умови простоти порядку здійснювати найскладніший етап, а саме побудову кривої.

З огляду на це, запропонований метод дозволяє побудувати еліптичні криві з зменшеною складністю.

Список літератури

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

2. American National Standard X9.62-1999. Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm, 1999.

3. Lersier R. Counting the number of points on an elliptic curve over finite fields: strategies and performense / R. Lersier // Proc. Eurocrypt. – 1995. – P. 101-116.

4. Elkies E. Elliptic and modular curves over finite fields and related computational issues / E. Elkies // Computational perspectives in number theory. – 1998. – P. 21-27.

5. Satoh T. Canonical lifting of elliptic curves and p – adic point counting. (theoretical background) / T. Satoh // Department of Mathematics, Faculty of Science, Saitame University. – 2001. – P. 1-21.

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

7. Washington L.C. Elliptic Curves-Number Theory and Cryptography / L.C. Washington. – Chapman &Hall/CRC, edition, 2008.

8. Silverman J.H. The arifmetic of Elliptic Curve / J.H. Silverman. – GTM 106, Springer-Verlag, New-York, 1986. – 868 p.

9. X9.62 Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). ANSI, – 1998.

Надійшла до редколегії 10.05.2012

Рецензент: д-р техн. наук, проф. О.І. Сухаревський, Харківський університет Повітряних Сил Сил ім. І. Кожедуба, Харків.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ВЫЧИСЛЕНИЯ ПОРЯДКА ЭЛЛИПТИЧЕСКИХ КРИВЫХ С ПОМОЩЬЮ ПОДНЯТИЯ, ОПРЕДЕЛЕННЫХ НАД ПОЛЕМ F(2^n)

О.Е. Петренко

Рассмотрены методы вычисления порядка эллиптической кривой с помощью поднятия и осуществлен анализ их вычислительной сложности. Предложен метод вычисления порядка кривой с уменьшенной сложностью.

Ключевые слова: *эллиптическая кривая, порядок эллиптической кривой, базовая точка.*

THE COMPARATIVE ANALYSES OF METHODS OF CALCULATION THE ORDER ELLIPTIC CURVES OF LIFTING OVER F(2^n)

O.E. Petrenko

The methods of calculation the order elliptic curves with help of lifting were considered. The analyses these methods Computational complexity of elliptic curve order was made. The method of calculation the order elliptic curves reduced complexity is proposed.

Keywords: *elliptic curve, order of elliptic curve, base point.*