УДК 004.382

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 2, pp. 165-172

ВИКОРИСТАННЯ СИМВОЛІВ ЯКОБІ ДЛЯ ГЕНЕРУВАННЯ ПАРАМЕТРІВ ЕЛІПТИЧНОЇ КРИВОЇ В КРИПТОСИСТЕМАХ

І.З. Якименко[1], Л.М. Тимошенко[2], В.А.Мокріцький[2]

[1] Тернопільський національний економічний університет,
вул. Львівська, 1, м.Тернопіль, 46020, Україна;
[2] Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна, e-mail: lint0902@gmail.ru

Запропоновано підхід до генерування параметрів еліптичної кривої в криптосистемах на основі генетичного алгоритму та з використанням символів Якобі, розроблено новий алгоритм генерування параметрів та базової точки еліптичної кривої, що дозволив підвищити стійкість алгоритмів шифрування інформації на еліптичних кривих та ефективність захисту інформації в комп'ютерних системах.

Ключові слова: криптосистема, еліптична крива, параметри еліптичної кривої, символ Якобі

Вступ

Інформаційні ресурси в сучасних умовах є одним із найважливіших результатів діяльності людського суспільства, саме тому особлива увага приділяється задачі їх захисту. Чільне місце у вирішенні цієї складної задачі посідає криптографічний захист інформації - вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо (ст. 1 Закону України «Про державну таємницю»).

Всі криптографічні алгоритми з відкритим ключем для розподілу ключів, шифрування інформації спираються на один з наступних типів незворотних перетворень [1]: розклад великих чисел на прості множники, або задача факторизації; проблема дискретного логарифмування; обчислення коренів алгебраїчних рівнянь.

Для надійного захисту інформації в криптосистемі RSA використовуються ключі розрядністю не менше 1024 біт. Захищеність більшості інших алгоритмів з відкритим ключем – Ель-Гамаля, DSA тощо ґрунтується на задачі дискретного логарифмування. При оцінці складності операції факторизації чисел і розв'язанні задачі дискретного логарифма показано, що вони вимагають приблизно однакового обсягу роботи [2]. Отже, ключі RSA, Ель-Гамаля, DSA однакової довжини будуть мати приблизно однакову стійкість.

Якщо не враховувати вже відомі криптографічно слабкі криві, стійкість алгоритмів шифрування на еліптичних кривих оцінюється як експоненційна [3, 4, 5, 6] . Складність атаки на ключ у цьому випадку експоненційно пов'язана з довжиною ключа, тобто наростає дуже швидко й для деякої довжини ключа атака стає практично нереалізованою. Стійкість же систем шифрування RSA й Ель-Гамаля субекспоненційна. Практично це означає, що алгоритми шифрування на еліптичних кривих за однакової стійкості мають розмір ключа на порядок менший, ніж у названих системах. Відомо [7], що еліптична крива із розміром ключа 160 біт забезпечує ту ж

стійкість, що й традиційні системи захисту розмірності ключа 1024 біт. Тому на даний час, по суті, немає альтернативи алгоритмам шифрування на еліптичних кривих.

На сьогодні еліптичні криві застосовують для реалізації різноманітних класів систем захисту інформації, зокрема для побудови симетричних, асиметричних криптосистем та систем електронного цифрового підпису. Незважаючи на вагомі переваги застосування еліптичної кривої (ЕК), існують проблеми, що зумовлюють такі класи задач [2,3]: генерування параметрів еліптичної кривої; обчислення порядку еліптичної кривої; дискретне логарифмування.

Постановка задачі дослідження і мета статті

Задачею генерування параметрів еліптичної кривої вигляду [2]

$$y^2 \equiv x^3 + ax + b(\mathrm{mod}\, p), \quad pF \in F_p,$$
$$\Delta = -(4a^3 + 27b^2) \neq 0,\ a, b \in F_p, \tag{1}$$

де $(x, y) \in E(F_p) \cup O$, O - нескінченно віддалена точка, є знаходження таких параметрів:

1. Просте число p – модуль перетворення груп точок ЕК, що повинно задовольняти нерівність $p > 2^{255}$. Верхня границя числа визначається конкретною реалізацією криптосистеми. Для створення цифрового підпису довжиною 512 біт, як це було для стандарту ГОСТ 34.310-95, число p повинно задовольняти нерівність $p < 2^{256}$. В подальшому вважаємо, що число p лежить в межах $2^{255} < p < 2^{256}$;
2. Просте число q, яке визначає порядок циклічної підгрупи групи точок еліптичної кривої E [2].

Для генерування простого числа можна використовувати такі процедури:

- генерування числа q в стандарті ГОСТ 34.310-95;
- генерування випадкового простого числа довжиною 256 біт;
- генерування сильного простого числа;
- генерування коефіцієнтів, де $a, b \in GF(p)$, що задають еліптичну криву E.

У [8] запропоновано метод генерування параметрів ЕК, що базується на генетичному підході, який полягає в одержанні за оптимальний час максимально наближеного значення цільової функції [9]. Для його реалізації взято за основу алгоритм А.12.4 стандарту IEEE P1363 [10] і розроблено алгоритм генерування параметрів ЕК з використанням генетичного підходу.

Використано такий критерій на базі наведеного в стандарті співвідношення оцінки гладкості кривої, отриманої на основі виразу

$$f = c \cdot b^2(\mathrm{mod}\, p) - a^3(\mathrm{mod}\, p), \tag{2}$$

де $a, b \in GF(p)$.

Врахування напряму зміни коефіцієнтів a, b дозволило суттєво підвищити ефективність роботи алгоритму – швидкодія зросла в 1.5-2 рази в залежності від розмірності параметрів a і b відносно алгоритму простого перебору. Зазначимо, що даний алгоритм має функціональні обмеження - простий перебір параметрів (a, b), хоча і з врахуванням операторів мутації та напрямків зміни коефіцієнтів a, b.

Отже, для підвищення ефективності захисту інформації в комп'ютерних системах та стійкості алгоритмів шифрування інформаційних потоків на еліптичних кривих

потрібен пошук нових підходів, які дозволять пришвидшити алгоритм генерування параметрів ЕК, що і є *метою* даної статті.

Основна частина

Для підвищення швидкодії генерування параметрів ЕК пропонується новий підхід з використанням символів Якобі [11]. Дослідження показали, що це дасть змогу зменшити часовий ресурс і збільшити загальну кількість пар параметрів (a,b), що генеруються. Символи Якобі дають можливість визначити, чи існує таке h, яке задовольняє рівність, отриману шляхом перетворення виразу (2):

$$h = (c^{-1}(\mathrm{mod}\, p)a^3) \bmod p. \qquad (3)$$

Згідно властивості символів Якобі [11], якщо $(a/p) = -1$, то $x_2 = a \bmod p$ не має рішення. Завдяки цьому можна відсіювати значення h, для яких символ Якобі дорівнює –1. Якщо ж символ Якобі дорівнює 1, то одержуємо

$$b^2 \equiv h(\mathrm{mod}\, p) \qquad (4)$$

Запропонований алгоритм збільшить швидкодію в порівнянні з генетичним алгоритмом пошуку параметрів ЕК за рахунок відсіювання параметрів (a,b), для яких символ Якобі не дорівнює 1.

З врахуванням вище сказаного загальний алгоритм генерування параметрів ЕК запишеться наступним чином.

1. Генерування числа c.
2. Генерування випадкового числа a.
3. Обчислення значення h.
4. Знаходження символу Якобі $j = J(h, p)$.
5. Якщо $j = -1$, то перейти до кроку 2.
6. Знаходження числа b.
7. Перехід на крок 1.

Слід зазначити, що при кожному генеруванні нового числа c для кожної пари параметрів ЕК значно зменшується швидкодія алгоритму. Блок-схема алгоритму подана на рис. 1.

З використанням наведеного алгоритму розроблено програмний продукт генерування параметрів ЕК для заданого модуля p в середовищі візуального програмування C++ Builder 6.0. Для визначення швидкодії запропонованого алгоритму було згенеровано 10 тисяч пар параметрів ЕК. Загальний час генерування становить 2 хв. 26.58 сек., тобто приблизний час генерування однієї пари дорівнює 14 мс. Варто зазначити, що при визначенні швидкодії число a було 256-бітним, а алгоритм допускає зменшення його розрядності. Тоді швидкодія алгоритму буде ще вищою. Програма, розроблена для реалізації поданого алгоритму, була доповнена реалізацією алгоритму генерування базової точки на ЕК. Модуль кривої p було взято з стандарту X9-62 [12]:

$$p = 115792089210356248762697446949407573530086143415290314195533631308867097853951$$

Після доповнення програми генерування параметрів генеруванням точки швидкість виконання алгоритму незначно зменшилася.

В таблиці 1 подано приклад згенерованих параметрів і координат базових точок еліптичної кривої.

Кількість пар, які генеруються, визначає паузу між циклами генерування. Під час генерування параметрів доступу до елементів керування вікном немає, тому після генерування кількості пар, яка задана в вищезазначеному полі, робиться пауза на 100 мс. При заданні дуже малих значень швидкодія програми суттєво зменшиться через велику кількість пауз, під час яких параметри не генеруватимуться. При заданні великих значень швидкодія висока, проте майже не буде доступу до вікна. Оптимальний вибір – 500-1000 пар. Ім'я поля редагування, в якому встановлюється кількість генерованих пар, EFreq. По замовчуванні в цьому полі встановлюється число 500.

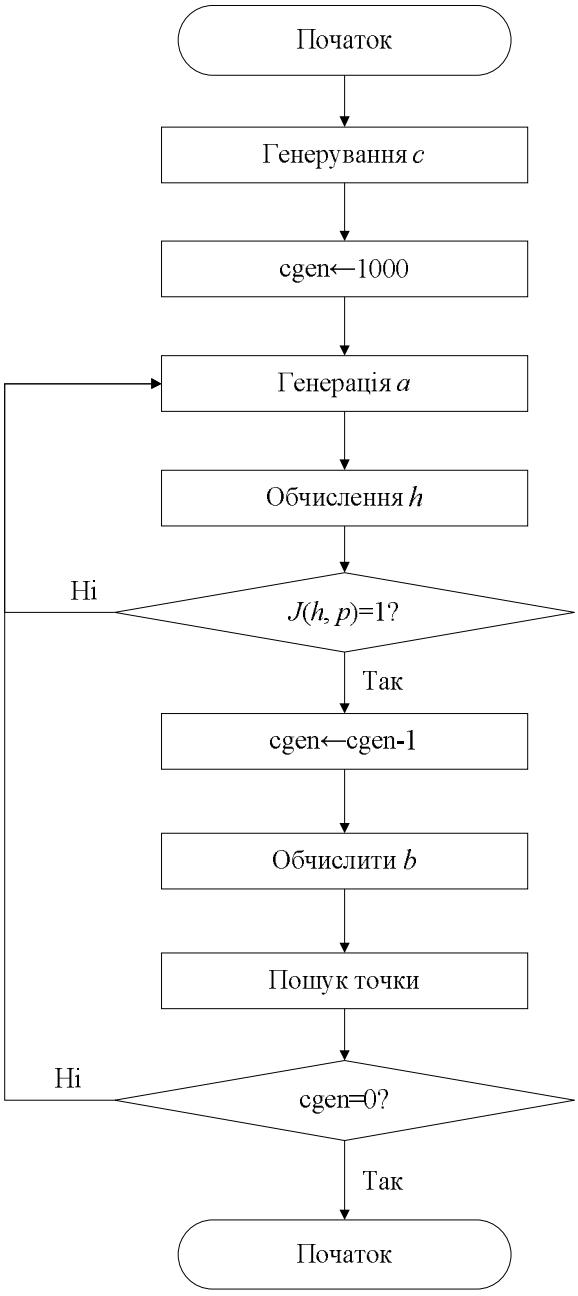

Рис.1. Алгоритм генерування параметрів ЕК з використанням символів Якобі

Проте не завжди потрібно генерувати саме 256-бітне число a. Його розрядність можна змінити, переключившись на змінну розрядність і вказати межі бітності числа a. Якщо потрібне число строгої розрядності (наприклад, 200 біт), то необхідно

встановити однакові значення для максимальної та мінімальної розрядності. Якщо розрядність встановити неправильно, то подається повідомлення, представлене на рис. 2.

Таблиця 1.

Приклад згенерованих параметрів та координат базових точок на ЕК

Число *c*	Параметри ЕК	Координати точки
c=4622141082350 761958088502957 771218460401318 074586653131924 490106838143083 4019	*a*=114696062184921291074865670680543091979803725285584054352011807055156770377329 *b*=84102322246235314974559211656505809896498381488370328980244492251701089994880	*x*=56342186822196110081703964857654083632130498187698608236967225088647602140708 *y*=45436596592511931629569885564096535284318424274910022081214046273849647278168
c=4495282155949 033906019773293 755442107970996 262433769553132 698783128445532 2679	*a*=62448504371778093752333915466416825250203415860656193403073976324655346540088 *b*=48776027794922097701268592125885615099753604479151430418547735948440420840414	*x*=93273292646220438052492376663941162818585306673620807190438274113700039002007 *y*=-556843238082099176 5342879723984285106 45865178119693397205711468572 54294477132
c=4631150059097 348210440033480 198418634575360 382240344739275 695741690967414 4562	*a*=69455553926359998935956975207837961345215187825158850426367316454247044183376 *b*=101921245183226147244012099904435024056556830696894318207652305979079392107026	*x*=9611699472638136808238570167400549939411556554261581779586275296230817584968 *y*=-785024814107883208 6782998900642022692058 58180045641255973366754666003 73083457
c=2587762300678 935703451124709 265240616294772 707383432045542 153686871273158 7895	*a*=73587567126760483677585357860726059097012187533517473774145023184880783157813 *b*=33206349606275448453205867854697432988301728737300381901236754438097544091177	*x*=72752367552177405495835515961374751940024200546485626335681266135036309097122 *y*=72616182050857165831081044177317019061041565413455809618410794248932607278083
c=2181212195678 094818479708491 098824025372465 709197803661588 154957091039001 9686	*a*=85999743901732190041149488884242181294898484866902415434124761386757328167530 *b*=103615535785767612720472812075114761432543620696917041411990013038205060297460	*x*=6779257572574225023 *y*=-8462646205002030098020 14132751659349153 50944360430106725242471082843207917740

До вихідних даних програми відносяться згенеровані параметри, число c, координати точки на ЕК із знайденими параметрами, кількість запусків процедури генерації параметрів, символ Якобі для конкретного числа a, кількість знайдених параметрів та час пошуку параметрів.

Числа a, b, c виводяться в поля редагування з іменами ANum, BNum, CNum відповідно. В цих полях властивість ReadOnly встановлена в true, тобто змінювати в них текст користувач не може, але може скопіювати його в буфер обміну ОС Windows.

Всі інші вихідні дані виводяться за допомогою міток (тип TLabel). Їх імена для значень кількості запусків процедури генерації символу Якобі, кількості знайдених пар (a,b), мітки, яка містить кількість згенерованих пар (для часової характеристики значення кількості пар кратні 500) та мітки, яка містить загальний час генерації, мають значення відповідно CStep, Jac, Couples, LFound, Found.

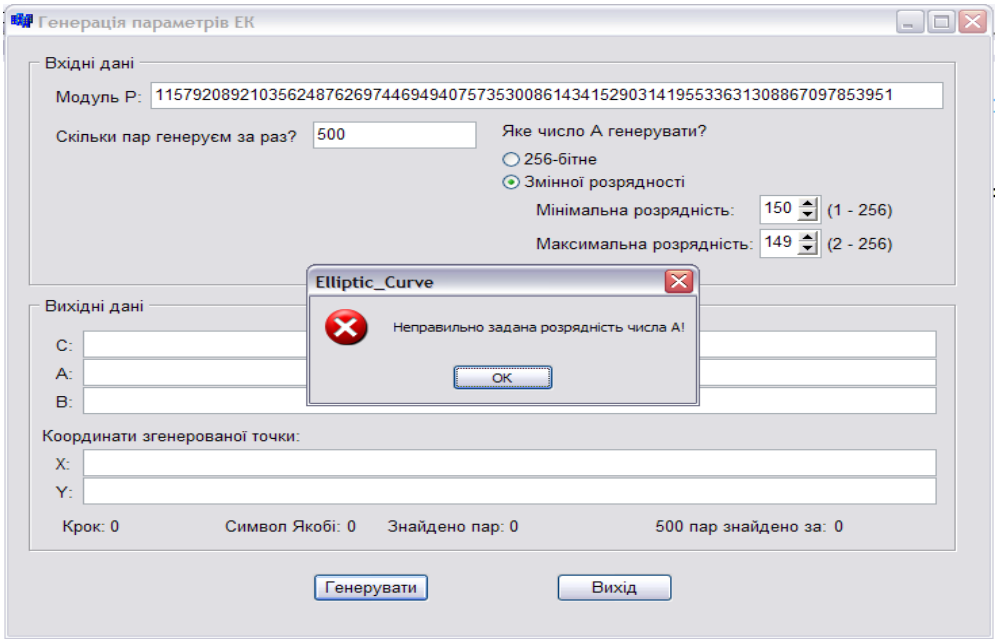

Рис.2. Процес генерування параметра ЕК

Приклад роботи програми для генерації 1200 пар з бітовим коридором для a 120-200 біт подано на рисунку 3.

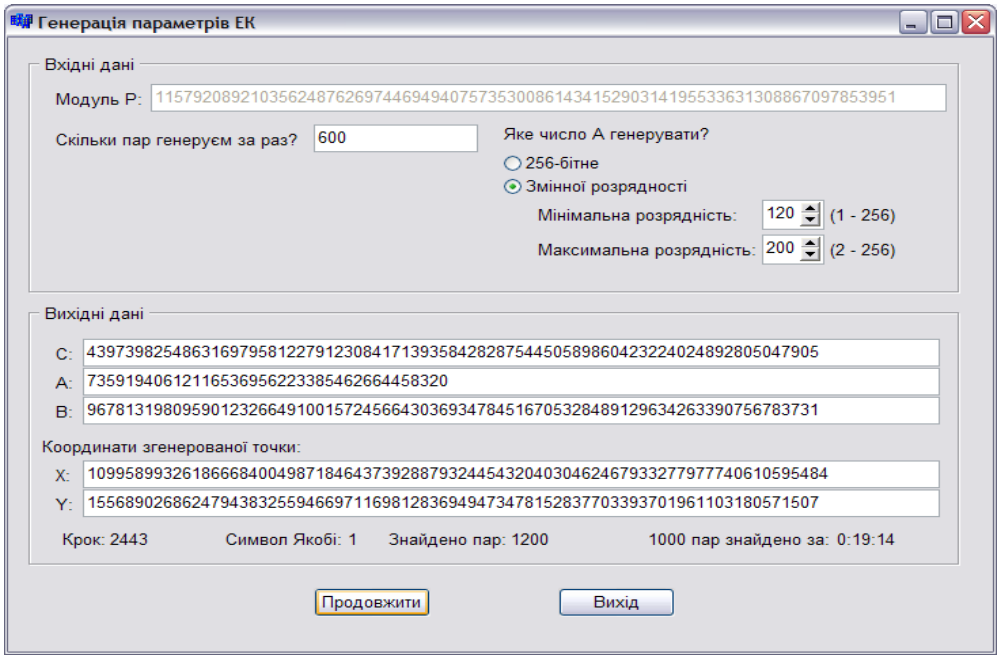

Рис.3. Інтерфейс генерування параметрів та базової точки ЕК

Також вихідні дані виводяться в два файли – Numbers.txt та Time.txt. В перший файл виводяться згенеровані параметри та координати точки. Він програмою ніколи не знищується. В файл Time.txt виводиться часова характеристика. При кожному запуску програми цей файл очищується. Програма використовує зовнішні бібліотеки lip.c та BigInt.cpp. В першій містяться функції для реалізації алгоритмів, які використовує IEEE P1363 A.12.4 та IEEE P1363 A.11.1. Друга містить функції, які використано для реалізації процедури виконання операцій над числами великої розрядності.

Результати чисельного експерименту генерування параметрів - залежності кількості пар параметрів ЕК від часу генерування наведено в табл. 2.

Аналіз результатів моделювання показав, що підхід з використанням символів Якобі дозволяє пришвидшити час роботи алгоритму в 9.91736*103 разів по відношенню до генетичного алгоритму, отже, генерувати параметри еліптичної кривої для побудови систем захисту інформаційних потоків з використанням математичного апарату ЕК майже на чотири порядки швидше, та до шести порядків відносно алгоритму простого перебору.

Таблиця 2.

Часові характеристики роботи програми

Кількість пар (a,b)	Час, c алгоритм з використанням символів Якобі	Час, 10^{-3} с Генетичний алгоритм
500	10.89	108.001
1000	21.19	209.1467
1500	31.77	315.0749
2000	42.69	423.2771
2500	53.25	528.0979
3000	63.66	631.3396
3500	74.25	736.3912
4000	84.80	840.9612
4500	95.52	947.1576
5000	106.05	1051.7643

Висновки

Запропонований алгоритм генерування параметрів ЕК на основі використання символів Якобі, розроблений на базі генетичного алгоритму, характеризується суттєвими перевагами швидкодії - приблизно чотири порядки по відношенню до генетичного алгоритму, та до шести порядків відносно алгоритму простого перебору, що є важливою перевагою його застосування для побудови стійких систем захисту інформаційних ресурсів з використанням математичного апарату ЕК.

Список літератури

1. Болотов, А.А. Алгоритмические основы эллиптической криптографии./ А.А. Болотов, С.Б. Гашков, А.Б. Фролов, А.А. Часовских./ – Москва: МЭИ.– 2000. – 100 с.
2. Бессалов, А.В. Криптосистемы на эллиптических кривых: Учеб. пособие.// А.В. Бессалов, А.Б. Телиженко / – К.: ІВЦ «Видавництво «Політехніка»».– 2004. – 224 С.
3. Карпінський, М.П. Еліптична крива для асиметричної криптографічної системи. // М.П. Карпінський, І.З. Якименко, І. Дуда / Вісник Тернопільського державного технічного університету імені Ів. Пулюя, - Том 6, - №3 – 2001. – С:91–95.

4. Карпінський, М.П. Оцінка продуктивності та стійкості до часового аналізу алгоритмів експоненціювання точки еліптичної кривої.// М.П. Карпінський, І.З. Якименко, М. Гіжицкі / Вісник Хмельницького національного університету. – 2006. – № 5. – С. 23-30.
5. Дубчак, Л.О. Оцінка часової реалізації алгоритму Монтгомері // Л.О.Дубчак, Л.М. Тимошенко, Ю.М. Чайківська / Зб.праць міжн. наук.-пр. конф. «Інформаційні технології в економіці, менеджменті і бізнесі. Проблеми науки, практики і освіти» К.: ЄУ,2007.-С.77-78.
6. Дубчак, Л.О. Спосіб вибору методу модулярного експоненціювання для побудови оптимальної системи захисту конфіденційної інформації // Л.О.Дубчак, Л.М. Тимошенко, Т.О. Яремчук / Інформаційна безпека. – Луганськ:, ЛНУ. - 2011. №1(5). - С.112-117.
7. Карпінський, М.П. Оцінка продуктивності та стійкості до часового аналізу алгоритмів експоненціювання точки еліптичної кривої.// М.П. Карпінський, І.З. Якименко, М. Гіжицкі / Вісник Хмельницького національного університету. Х:, ТУП. – 2006. – № 5. – С. 23-30.
8. Карпінський, М. Метод генерування параметрів еліптичних кривих. // М. Карпінський, І. Васильцов, І. Якименко, Я. Кінах / Правове, нормативне, та метрологічне забезпечення системи захисту інформації в Україні. К. –2003– № 6.– С.74.
9. Исаев, С. Генетические алгоритмы – эволюционные методы поиска. [Электронный ресурс] // С. Исаев. Режим доступа: http://ai-online.fromru.com/documents-genetic_algorithms.html.
10. IEEE P1363-2000 / D8(Draft Version 8). Standard Specifications for Public Key Cryptography.
11. Айерлэнд, К. Классическое введение в современную теорию чисел.// К. Айерлэнд, М. Роузен/ — М.: Мир.– 1987- 416 с.
12. X9.62-1998. Public Key Cryptography For The Financial Services Industry. Public Key Cryptography For The Financial Services Industry.

ИСПОЛЬЗОВАНИЕ СИМВОЛОВ ЯКОБИ ДЛЯ ГЕРИРОВАНИЯ ПАРАМЕТРОВ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ В КРИПТОСИСТЕМАХ

И. З. Якименко[1], Л. Н. Тимошенко[2], В.А. Мокрицкий[2]

[1] Тернопольский национальный экономический университет,
ул. Львовская, 1, г.Тернополь, 46020, Украина;
[2] Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: lint0902@gmail.ru

Предложено подход генерирования параметров эллиптической кривой в криптосистемах на основе генетического алгоритма и с использованием символов Якоби, разработано новый алгоритм генерирования параметров и базовой точки эллиптической кривой, который позволил повысить стойкость алгоритмов шифрования информации на эллиптических кривых и эффективность защиты информации в компьютерных системах.
Ключевые слова: Криптосистема, эллиптическая кривая, параметры эллиптической кривой, символ Якоби.

USE OF JACOBI SYMBOLS TO GENERATE THE ELLIPTIC CURVE PARAMETERS IN CRYPTOSYSTEMS

I.Z. Yakimenko[1], L.N. Timoshenko[2], V.A. Mokritskyi[2]

[1] Ternopil national economical university
1, Lvivska Str., Ternopil, 46020, Ukraine;
[2] Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: lint0902@gmail.ru

A Jacobi symbols-utilizing approach to generation of elliptic curve parameters in cryptosystems was proposed based on genetic algorithm. A new algorithm to generate the elliptic curve parameters and reference point was developed thereby providing for improvement in both robustness of data coding algorithm based on elliptic curves and efficiency of data protection in computer systems.
Keywords: cryptosystem, elliptic curve, elliptic curve parameters, Jacobi symbol.