Якименко І. Ефективні методи паралельної реалізації алгоритму Шуфа / Якименко І., Кінах Я., Трембач Р. // Вісник ТНТУ. — 2011. — Том 16. — № 1. — С.180-185. — (приладобудування та інформаційно-вимірювальні технології).

УДК 681.3

І. Якименко; Я. Кінах, канд. техн. наук;
Р. Трембач, канд. техн. наук

Тернопільський національний економічний університет

ЕФЕКТИВНІ МЕТОДИ ПАРАЛЕЛЬНОЇ РЕАЛІЗАЦІЇ АЛГОРИТМУ ШУФА

Резюме. *На основі аналізу захисту інформаційних потоків на еліптичних кривих та досліджень їх стійкості з використанням алгоритму Шуфа доведено, що даний алгоритм є трудомістким. Водночас він дозволяє знаходити точні розв'язки задачі пошуку порядку ЕК. Тому для ефективного розв'язання даної задачі запропоновано розпаралелення алгоритму Шуфа на мережі типу NGN, високопродуктивній обчислювальній техніці та телекомунікаційній мережі для зменшення часового ресурсу.*

Ключові слова: *алгоритм Шуфа, захист інформаційних потоків, алгоритми розподіленого опрацювання даних, ефективність.*

I. Iakymenko, I. Kinakh, R. Trembash

EFFECTIVE METHODS OF PARALLEL ALGORITHM SCHOOF

The summary. *On the basis of protection of information flows on elliptic curves, and study their stability using the algorithm Schoof, showed that this algorithm is time consuming, but at the same time, it allows you to find exact solutions of the problem of finding EC. Therefore, to effectively address this problem, a new parallelization algorithm Schoof type of network NGN, High Performance Computing Technology and telecommunications network to reduce the time resources.*

Key words: *algorithm Schoof, protection of information flows, algorithms, distributed computing efficiency.*

Вступ. Комп'ютерні мережі є високопродуктивними з великим обсягом обчислювальних ресурсів, тому доцільно їх використовувати для захисту інформації на основі використання ЕК. Одним з найбільш перспективних напрямків є розробка нових алгоритмів розподіленої обробки даних, що дозволяють ефективно визначати інформаційну стійкість алгоритмів на еліптичної кривої (ЕК). Розглянемо практично важливі питання захисту інформаційних потоків з використанням математичного апарату еліптичних кривих. Однією з важливих задач є пошук порядку ЕК для встановлення стійкості алгоритму шифрування.

Огляд публікацій та відомих рішень. Питанням захисту інформації та використанню мережевих технологій у шифруванні інформаційних потоків присвячений ряд наукових робіт і публікацій. У працях О.Н. Василенко, А.Ростовцев і Е. Маховенко подано теоретичні основи захисту інформаційних потоків із використанням математичного апарату ЕК, але не розглянуто сучасні методи розв'язку важливої задачі пошуку порядку ЕК, а саме, паралельні та розподілені алгоритми та алгоритми з використанням теоретико-числових базисів, розмежованої системи числення [1, 5]. Однією з найтрудомісткіших операцій алгоритму Шуфа є операція модулярного експоненціювання. Прискорення даної операції запрононовано методом паралельних обчислень у роботі [2]. Великий вклад у розвиток теорії, методів та алгоритмів задач захисту інформаційних потоків із використанням математичного апарату еліптичних кривих внесли зарубіжні вчені L. C. Washington і Rong_Jaye Chen, а саме, практичне застосування теорії чисел у криптографії ЕК та ефективні методи розв'язання задачі пошуку порядку з використанням алгоритму Шуфа [3,4].

Мета роботи. Для підвищення стійкості систем захисту інформаційних потоків із використанням математичного апарату ЕК необхідно, щоб порядок ЕК, а саме, число кількості точок, був максимальним та містив великий простий дільник. Розв'язання цієї задачі можливе з використанням таких алгоритмів: «крок гіганта–крок малюка», Шуфа, Еткіна та Еліза. Найбільш ефективним серед даних алгоритмів є алгоритм Шуфа, який дозволяє знайти значення точної кількості точок ЕК. На практиці розв'язання задачі обчислення кількості точок є досить трудомістким.

Таким чином, для підвищення високого і необхідного в перспективі рівня захисту інформаційних потоків у КМ необхідне розроблення двох важливих напрямків – методів та засобів захисту інформаційних потоків стійких до різного виду атак на основі мережевих, а також високопродуктивних програмно-апаратних засобів. Метою даної роботи є дослідження ефективного використання мережі типу NGN, високопродуктивної обчислювальної техніки та телекомунікаційної мережі для розв'язання задачі пошуку порядку з використанням паралельних обчислень алгоритму Шуфа.

Постановка задачі. Розв'яжемо задачу пошуку порядку еліптичної кривої паралельними методами на рівні комп'ютерної мережі, що допускає використання швидких прямих методів розв'язання мережевих задач для криптографії ЕК та їх паралельних реалізацій.

В якості системи для реалізації обчислювальних алгоритмів обрано кластер розподілених обчислень з топологією телекомунікаційної мережі (ТМ). Кожна робоча станція характеризується продуктивністю 3ГГц, об'ємом оперативної пам'яті 1Гб, що працює під керуванням операційної системи Ubuntu на ядрі 2.6.16. Запропоновано використовувати методи розпаралелення, засновані на платформі типу domain decomposition.

Ефективність паралельної реалізації алгоритму Шуфа. Для визначення часу виконання паралельного алгоритму необхідно побудувати модель виконання алгоритму у вигляді орієнтованого графа, вершинами якого є окремі арифметичні операції або блоки операцій, які виконуються безперервно на одному процесорі, а дуги являють собою зв'язки між обчислювальними блоками. Далі визначається максимальна довжина шляху обчислювального алгоритму з урахуванням блокувань процесорів при виповнені обміну даними. На виділеному шляху максимальної довжини обчислюється кількість узагальнених арифметичних операцій, операцій обміну даними та обсяги переданих даних. Для розглянутої обчислювальної системи визначається співвідношення швидкості обміну даними та часу виповнення узагальненої арифметичної операції. На основі отриманих даних розраховуються теоретичні значення прискорення та ефективності алгоритму.

Кожен паралельний алгоритм оцінюється за двома параметрами – прискорення S_p та ефективності E_p, які визначають за формулами

$$S_n = \frac{t_1}{t_n}\ ,\ E_n = \frac{S_n}{n} * \nu_N\,, \qquad (1)$$

де t_1 – час розв'язання вихідної задачі на одному процесорі, t_n – час розв'язання вихідної задачі за паралельним алгоритмом на n процесорах. Так як у системі з розподіленою пам'яттю присутні комунікації, то час виконання комунікацій входить у загальний час виконання паралельного алгоритму, тому оцінки прискорення та ефективності необхідно скоригувати на величину, що є середньозваженим коефіцієнтом швидкодії вузлів ν_N=(0..1). Введемо ряд коефіцієнтів, що характеризують швидкодію обчислювачів і комунікацій конкретної системи і позбавляє нас від необхідності знати протоколи обміну даними.

Коефіцієнт ефективності передавання k_E дорівнює відношенню швидкості передавання корисної інформації, що обчислюємо як

$$S = \frac{p}{t}, \tag{2}$$

де t – час передавання повідомлення розміром p байтів до швидкості передавання даних між вузлами S_c. З його допомогою можна отримати час передавання, знаючи довжину цього передавання в бітах або кількість арифметичних операцій, які виконуються за передавання. Час передавання визначаємо як

$$T_{пер} = \frac{\delta}{k_e * S_c}, \tag{3}$$

кількість арифметичних операцій виконуваних за передавання

$$Q_A = \frac{\delta * \theta}{k_e}, \tag{4}$$

де δ – підзадачі паралельного алгоритму Шуфа;

θ – коефіцієнт, що характеризує число узагальнених арифметичних операцій пошуку порядку ЕК, які виконуються за час передавання 1 біта між вузлами кластера.

Значення коефіцієнта ефективності передавання k_E можна апроксимувати функціональною залежністю

$$k_E = V/\left(V + V \cdot c_1 + c_2\right), \tag{5}$$

де V – довжина повідомлення в бітах;

$V \cdot c_1$ – обсяг службової інформації в пакеті;

c_2 – коефіцієнт, що відображає час на підготовку посилання.

Тоді прискорення у ефективність алгоритму можна записати

$$S_n = \frac{t_a * Q_{AS}}{t_a * Q_{AP} + t_{пд1}}, \qquad E_n = \frac{t_a * Q_{AS}}{N(t_a * Q_{AP} + t_{пд1})}, \tag{6}$$

де Q_{AS} – кількість арифметичних операцій послідовного алгоритму Шуфа;

Q_{AP} – кількість арифметичних операцій паралельного алгоритму Шуфа;

t_a – час виконання однієї узагальненої арифметичної операції;

N – кількість використовуваних вузлів. Тоді площу мережі P_m обчислюємо за формулою

$$P_m = \sum_{i=1}^{N}(V_i * \frac{\delta}{k_e(V_i)}) * t_a. \tag{7}$$

Паралельні алгоритми методу Шуфа та обчислення найбільшого спільного дільника в полях Галуа призначені для розв'язання криптографічних задач на кластерних системах з розподіленою пам'яттю. Отримано оцінки ефективності алгоритмів на основі аналізу числа виконуваних операцій.

Практична реалізація розроблених алгоритмів на кластері розподілених обчислень і отримані експериментальні оцінки дозволяють зробити висновок про ефективність і доцільність використання алгоритмів на БОС з розподіленою пам'яттю, де $N = 2^q$ – кількість вузлів (рис. 1).

Дослідження показали, що площа мережі значно зростає зі збільшенням кількості вузлів і досягає свого максимуму при 256 вузлах. При подальшому збільшенні кількості вузлів ефективність зменшується, оскільки значна частина інформаційних

ресурсів мережі опрацьовує службову інформацію, а не спрямована на розв'язання задачі пошуку порядку ЕК.

Таблиця 1. Ефективність алгоритму Шуфа залежно від кількості вузлів і типу мережі

Кількість вузлів, N	E8	E4	E2
0	0	0	0,2
1	0,0001	0,0001	0,3
2	0,0002	0,0002	0,56
3	0,01	0,015	0,78
4	0,02	0,027	0,8
5	0,01	0,05	0,91
6	0,02	0,52	0,93
7	0,03	0,54	0,95
8	0,04	0,51	0,87
9	0,05	0,47	0,88
10	0,09	0,5	0,97
11	0,35	0,45	0,91
12	0,38	0,45	0,97
13	0,39	0,45	0,92
14	0,39	0,45	0,97
15	0,38	0,45	0,9

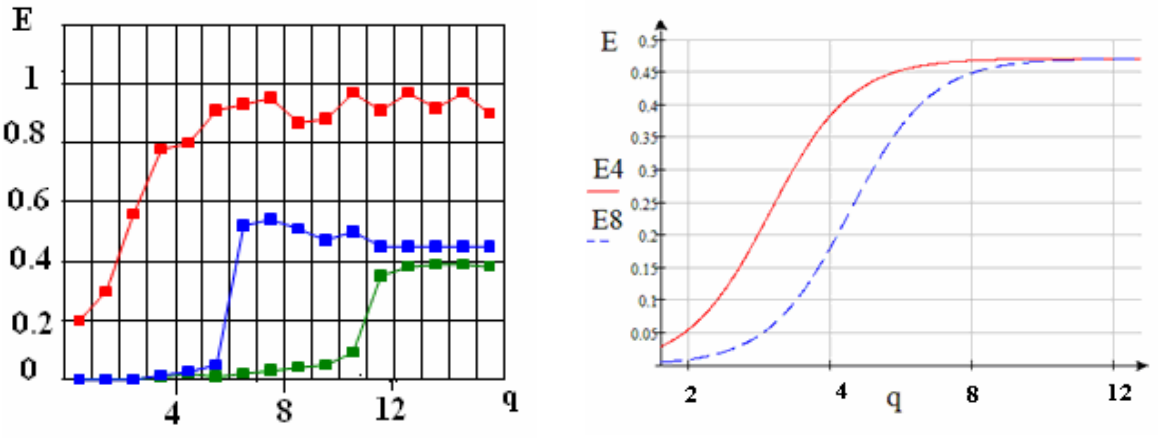

Рисунок 1. Ефективність паралельного алгоритму методу Шуфа

Тому на практиці для розв'язання поставленої задачі доцільно скористатися телекомунікаційною мережею, що містить 256 вузлів, на котрих задіяно по 256 робочих станцій.

Дослідження незвідності поліномів з алгоритму Шуфа показали, що теоретичні викладки і практична реалізація має деякі відмінності, оскільки на практиці використовують обчислювальні машини різних типів і поколінь.

Для значень параметра q від 1 до 4 вузлів доцільно використовувати високопродуктивну обчислювальну техніку (лінія E4), рис. 2, або мережу типу NGN (лінія E5). У діапазоні значень 4–7 вузлів найефективнішою є мережа типу NGN, вона досягає свого максимуму 0,84 відносних одиниць.

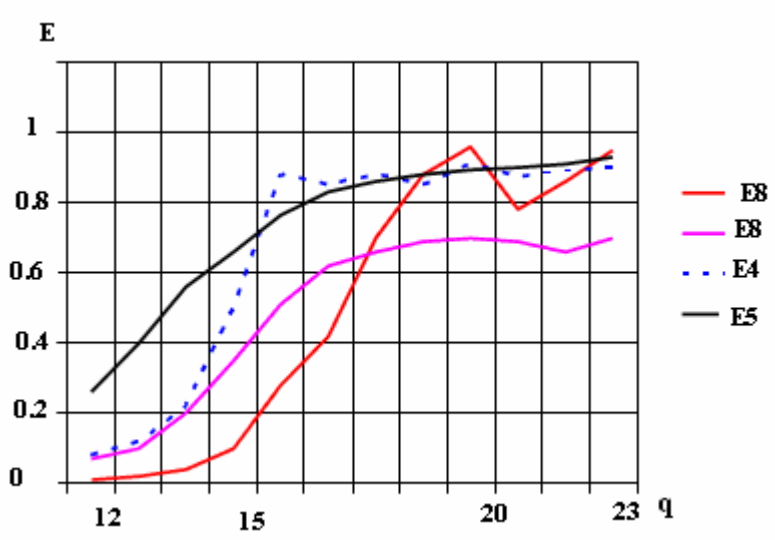

Рисунок 2. Ефективність паралельного обчислення незвідності поліномів

Від 7 до 9 вузлів доцільно використовувати телекомунікаційну мережу, оскільки вона досягає максимуму 0,89 відносних одиниць. Тому для ефективного розв'язання задачі пошуку порядку ЕК на основі використання алгоритму Шуфа слід скористатися телекомунікаційною мережею.

Розроблено паралельні алгоритми методів обчислення на еліптичних кривих. Отримано теоретичні та експериментальні оцінки ефективності алгоритмів з урахуванням витрат часу на обміни та отримані області ефективності алгоритму Шуфа. Показано, що максимальна ефективність паралельної реалізації комбінованого алгоритму неповної редукції може бути досягнута шляхом вибору кількості кроків редукції, що передують розкладанню по базису і наведено відповідні залежності.

При паралельній реалізації обчислення порядку еліптичних кривих вхідну інформацію потрібно розбити на підзадачі, які розподіляються по вузлам кластеру і обчислення проводиться на окремих процесорах. Обчислення на черговому рівні редукції починаються з передавання даних між процесорами кластеру.

Результати реалізованого паралельного обчислення наведено на рисунку 3.

Якщо використовувати обчислювальну техніку одного типу, тоді з рисунка 3 можна побачити, що мережі працюють стабільно і при збільшенні кількості вузлів збільшується ефективність роботи паралельного алгоритму Шуфа. Але з результатів досліджень випливає, що доцільно використовувати телекомунікаційну мережу (лінія E2).

Паралельний алгоритм складається з двох основних етапів: обчислення найбільшого спільного дільника двох поліномів та методу Шуфа.

Розроблені алгоритми реалізовані у вигляді структурованої бібліотеки програм, основна мета якої – максимально ефективно розв'язати поставлену задачу, знаючи її розмірність і параметри кластера розподілених обчислень. Для вибору оптимального алгоритму на основі вхідних даних було розроблено оболонку, яка виробляє визначення характеристик використовуваної обчислювальної системи для обчислення коефіцієнта і подальший аналіз з вибору оптимального алгоритму розв'язання задачі.

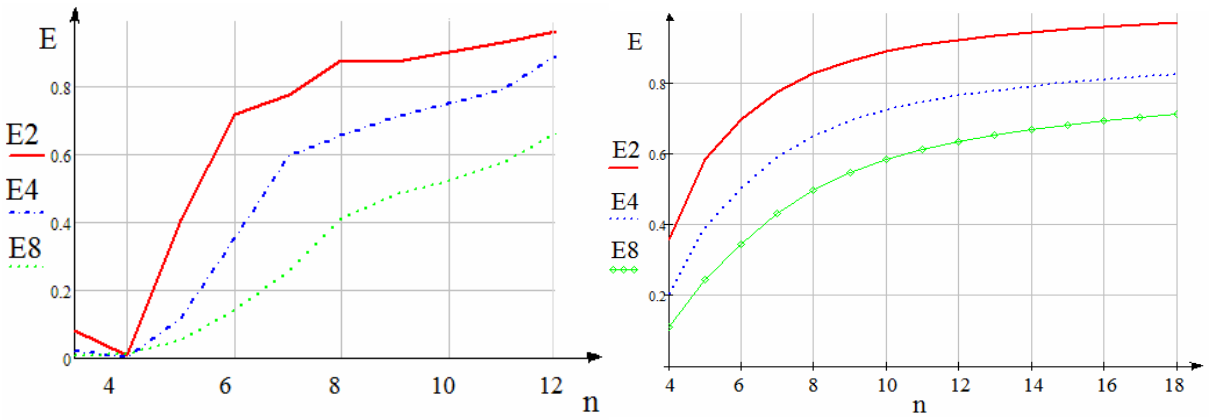

Рисунок 3. Ефективність роботи паралельного алгоритму Шуфа

Виконано порівняльний аналіз розроблених алгоритмів та визначено області ефективного застосування кожного алгоритму залежно від характеристик швидкодії обчислювальної системи. На рис. 1–3 наведено графіки відносної ефективності паралельних алгоритмів. У якості базового розглянуто алгоритм Шуфа для того, щоб можна було провести порівняльний аналіз паралельних алгоритмів і визначити, який з них має оптимальний час розв'язання задачі, для параметрів ЕК розмірності 512 біт на 256 вузлах телекомунікаційної мережі.

Висновки. Виконано практичну реалізацію розпаралелення алгоритму Шуфа. Дослідження паказали, що лише в часткових випадках доцільно використовувати високопродуктивну обчислювальну техніку. В загальному випадку доцільно скористатися мережею типу NGN, вона досягає свого максимуму 0,84 відносних одиниць. Зі збільшенням параметрів ЕК найефективнішою є телекомунікаційна мережа, оскільки вона досягає максимуму 0,89 відносних одиниць. Тому для ефективного розв'язання задачі пошуку порядку ЕК на основі використання алгоритму Шуфа слід скористатися телекомунікаційною мережею. Наступні вдосконалення паралельної реалізації доцільно проводити на основі використання теоретико-числових базисів та розмежованої системи числення залишкових класів, які дозволяють виконувати глибоке розпаралелення алгоритму Шуфа.

Література

1. Ростовцев А. Теоретичекая криптография / А. Ростовцев, Е. Маховенко / СПб.: АНО НПО «Профессионал», 2005. – С.139–141, 294–305.
2. Прискорення алгоритму Шуфа методом паралельних обчислень // І. Якименко, А. Хомінчук / Матеріали дванадцятої наукової конференції Тернопільського державного технічного університету імені Івана Пулюя, 14–15 травня 2008 р. – Тернопіль, ТДТУ, 2008. – С.116.
3. L. C. Washington: Elliptic Curves: Number Theory and Cryptography. Chapman & Hall/CRC, New York, 2003.
4. Rong_Jaye Chen. Schoof's Algorithm/// Pepartment of Computer Science / National Chiao Tung University. ECC-2008.
5. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М.: МЦНМО, 2003. – 328 с.

Отримано 18.01.2011