УДК 681.32

С.В. ІВАСЬЄВ, Я.М. НИКОЛАЙЧУК, І.З. ЯКИМЕНКО, І.Р. КОЛІСНИК
Тернопільський національний економічний університет

ЗБІЖНІСТЬ ЕКСТРЕМУМІВ ЗАЛИШКОВОЇ ФУНКЦІЇ В ОКОЛІ РОЗВ'ЯЗКУ ЗАДАЧІ ФАКТОРИЗАЦІЇ

Проведений аналіз існуючих методів розкладу на множники та тестів простоти. Досліджено збіжність кількості екстремумів залишкової функції в околі розв'язку задачі факторизації. Представлено модель збіжності кількості екстремумів. Розглянуто ряд прикладів визначення околу розв'язку задачі фаторизації. Досліджено залишкову функцію при переборі дільників. Виявлено симетричність екстремумів залишкової функції в зоні розв'язку.

Ключові слова: факторизація, залишкова функція, перебір дільників, зона розв'язку.

S.V. IVASIEV, YA.M. NICOLAYCHUK, I.Z. YAKYMENKO, I.R. KOLISNYK
Ternopil national economical university

CONVERGENCE EXTREMES RESIDUAL FUNCTION IN THE NEIGHBOURHOOD PROBLEM SOLVING FACTORIZATION

Abstract – The analysis of existing methods Factorization tests and simplicity. The convergence of extremes quantity of residual function in the neighbourhood factorization problem solution. The model number extremes convergence. A number of examples of determination vicinity factorization problem solution. Investigated residual function when iterating divisors. Discovered symmetry extremes residual functions in the area of interpretation.

Keywords: factorization, residual function, bust dividers, seating solution.

Вступ

В задачах шифрування інформаційних потоків (ІП), як і в прикладних проблемах теорії чисел (факторизації, тестах простоти), дослідженнях стійкості асиметричних алгоритмів шифрування важливим і трудомістким процесом є розробка методів та алгоритмів виявлення діапазону розв'язку задачі факторизації [1].

Проведений аналіз існуючих методів розкладу на множники та тестів простоти говорить про те, що розв'язання даної задачі далеке від досконалості. З розвитком інформаційних технологій зростають розмірності вхідних параметрів криптосистем, що в свою чергу призводить до збільшення обчислювальної складності при генерації та опрацюванні багато розрядних простих чисел. Тому розробка ефективного методу пошуку простих чисел та методів знаходження околу розв'язків факторизації є актуальною задачею, що дозволить зменшити часову складність RSA подібних асиметричних алгоритмів шифрування.

1. Аналіз складностей алгоритмів факторизації

Найбільш поширеним алгоритмом факторизації чисел є повний перебір можливих дільників. В даному випадку обчислювальна складність дорівнює $O(N^{1/2})$ [2].

Досить розповсюдженими є Ферма–подібні алгоритми зі складністю[2] $O(\exp(N))$.

В праці [2] приведений ρ-алгоритм Поларда, який характеризується меншою обчислювальною складністю, а саме $O(N^{1/4})$.

Джон Діксон запропонував декілька методів [2]:

1) метод безперервних дробів складність якого ;

2) метод квадратичного решета зі складністю [2] $O(\exp[c\ln(N)^{1/3}\ln(\ln(N))^{2/3}])$;

3) метод на основі еліптичних кривих, який має обчислювальну складність $O(\exp[c\ln(N)\ln(\ln(N))])^{1/3}$ [2].

У результаті дослідження слід виділити, що найефективнішим щодо швидкодії є метод квадратичного решета числового поля.

Питання про існування алгоритму факторизації з поліноміальною складністю на класичному комп'ютері є однією з важливих відкритих задач сучасної теорії чисел. В той же час, для спорідненої задачі про розпізнавання простоти числа існує поліноміальне рішення — AKS тест простоти [3].

Рішення задачі факторизації з поліноміальною складністю можливо на квантовому комп'ютері за допомогою алгоритму Шора.

2. Дослідження залишкової функції при переборі дільників

В результаті дослідження процесу факторизації прямим перебором було отримано наступні результати. Нехай задане число P_0, яке потрібно факторизувати. Знайдемо:

$$P^* = \left|\sqrt{P_0}\right| \quad \text{– непарне число;}$$

Тоді обчислюємо значення згідно співвідношення $P_1 = P_0 \bmod P^*$, $P_n = P_0 \bmod P^* + 2_n$, $n \in Z$.

Наступним кроком буде побудова послідовності

$$P_2 = P_1 + Q_1, P_3 = P_2 + Q_2, \ldots, P_n = P_{n-1} + Q_{n-1}$$

де $Qi = 2i, i = 1, \ldots, n-1$

Аналогічним чином знаходимо значення $P_{1*} = P_0 \bmod(P*-2i), i = 1, \ldots, n-1.$

$$P_1* = P_0 \bmod P* = P_1$$
$$P_2* = P_0 \bmod(P*-2)$$
$$P_3* = P_0 \bmod(P*-4)$$

де P_i* назвемо залишковою функцією.

Слід відмітити, що в результаті таких перетворень значення залишків постійно зростає і різко падає, після чого залишки знову починають зростати. Таку залежність можна представити за допомогою залишкоподібної (пилкоподібної) функції, представленої на рис. 1.

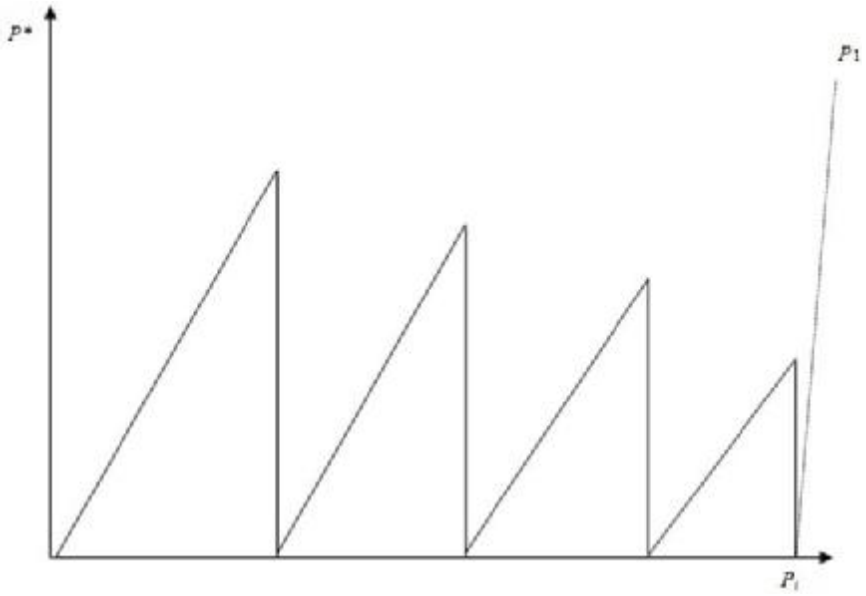

Рис. 1. Пилкоподібна функція

З рис. 1 видно, що кількість зростань залишків стабільно наближається до зони розв'язку і це, в свою чергу, дозволить її локалізувати. Даний підхід зменшує діапазон та обчислювальну складність пошуку розв'язання задачі факторизації багаторозрядних чисел.

В результаті проведених досліджень отримаємо таблицю значень кількості змін залишкової функції $P*_n$ на початку перебору при вхідних даних:

P_0 445023604703_{10} $1100111100111010111100101001111110111111_2$

$P*$ 667101_{10} 10100010110111011101_2

P_1 10010101001111100001_2

P_2 10110001101110111111_2

Віднімаємо 2 від $P*$

Таблиця 1

Кількості змін залишкової функції на початку перебору

1	186	261	157	123	105	93	85	77	73	68	64	61	58	56	54	52	51	48	48
46	44	44	43	41	41	40	39	38	38	36	37	35	35	35	34	33	33	32	32
32	31	31	30	30	30	29	29	29	28	28	28	27	27	27	27	26	26	26	26
25	25	25	25	25	24	24	24	24	23	24	23	23	23	23	22	22	23	22	22
21	22	21	22	21	21	21	21	21	20	20	21	20	20	20	20	20	19	20	19
19	20	19	19	19	18	19	19	18	19	18	18	18	19	18	17	18	18	18	17
18	17	17	18	17	17	17	17	17	17	16	17	17	16	17	16	17	16	16	16
16	16	16	16	16	16	15	16	16	15	16	15	16	15	15	15	16	15	15	15
15	15	15	14	15	15	14	15	15	14	15	14	14	15	14	14	15	14	14	14
14	14	14	14	14	13	14	14	14	13	14	13	14	13	14	13	14	13	13	14
13	13	13	13	14	13	13	13	13	12	13	13	13	13	13	12	13	13	12	13
12	13	12	13	12	13	12	12	13	12	12	12	13	12	12	12	12	12	12	12
12	12	12	12	12	12	11	12	12	12	11	12	12	11	12	12	11	12	11	12

Продовження табл. 1

11	11	12	11	12	11	11	11	12	11	11	11	11	12	11	11	11	11	11	11
11	11	11	11	11	11	10	11	11	11	11	10	11	11	10	11	11	10	11	11
10	11	10	11	10	11	10	11	10	10	11	10	10	11	10	10	11	10	10	10
10	11	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
10	9	10	10	10	10	9	10	10	10	9	10	10	9	10	9	10	10	9	10
9	10	9	10	9	10	9	10	9	9	10	9	9	10	9	9	10	9	9	10
9	9	9	9	10	9	9	9	9	9	10	9	9	9	9	9	9	9	9	9
9	9	9	9	9	9	9	8	9	9	9	9	9	8	9	9	9	9	8	9
9	9	8	9	9	8	9	9	8	9	9	8	9	8	9	8	9	8	9	9
8	9	8	8	9	8	9	8	9	8	8	9	8	9	8	8	9	8	8	8
9	8	8	9	8	8	8	8	9	8	8	8	8	9	8	8	8	8	8	8
8	8	9	8	8	8	8	8	8	8	8	8	8	8	8	7	8	8	8	8
8	8	8	8	8	7	8	8	8	8	8	7	8	8	8	7	8	8	8	7
8	8	8	7	8	8	7	8	8	7	8	7	8	8	7	8	7	8	8	7
8	7	8	7	8	7	8	7	8	7	8	7	8	7	8	7	7	8	7	8
7	7	8	7	7	8	7	8	7	7	7	8	7	7	8	7	7	7	8	7
7	7	8	7	7	7	8	7	7	7	7	7	8	7	7	7	7	7	7	7
8	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7
7	7	7	7	7	7	7	7	7	6	7	7	7	7	7	7	7	6	7	7
7	7	7	6	7	7	7	7	6	7	7	7	6	7	7	7	6	7	7	7

Даний процес продовжуємо, на основі аналітичних співвідношень доти, поки не локалізуємо зону розв'язку, тобто:

$$P^*_n = P_0 \bmod(P^* - 2n), n \in Z$$

$$P_2^* = P_1^* + Q_1^*, P_3^* = P_2^* + Q_2^*, \ldots, P_n^* = P_{n-1}^* + Q_{n-1}^*$$

$$Q_1 = |P_2 - P|, Q_2^* = |P_3 - P_2|, \ldots, \; Q_{n-1} = |P_n - P_{n-1}|$$

$$Q_1^* = |P_2^* - P_1^*|, Q_2^* = |P_3^* - P_2^*|, \ldots, \; Q_{n-1}^* = |P_n^* - P_n^* - 1|$$

$$Q_1 = |P_0 \bmod(P^* + 2) - P_0 \bmod P^*|$$

$$Q_2 = |P_0 \bmod(P^* + 4) - P_0 \bmod(P^* + 2)|$$

$$Q_{n-1} = |P_0 \bmod(P^* + 2_n) - P_0 \bmod(P^* + 2_n - 2)|$$

$$Q_1^* = |P_0 \bmod(P^* - 2) - P_0 \bmod P^*|$$

$$Q_2^* = |P_0 \bmod(P^* - 4) - P_0 \bmod(P^* - 2)|$$

…

$$Q_{n-1}^* = |P_0 \bmod(P^* - 2_n) - P_0 \bmod P^* - 2_n + 2|$$

Для того, щоб знайти значення P_1 і P_2, $(P_0 = P_1 P_2)$, потрібно, щоб послідовності Q_{n-1}^* збігались до 0. Результати дослідження можна відобразити у вигляді діаграми, представленої на рис. 2.

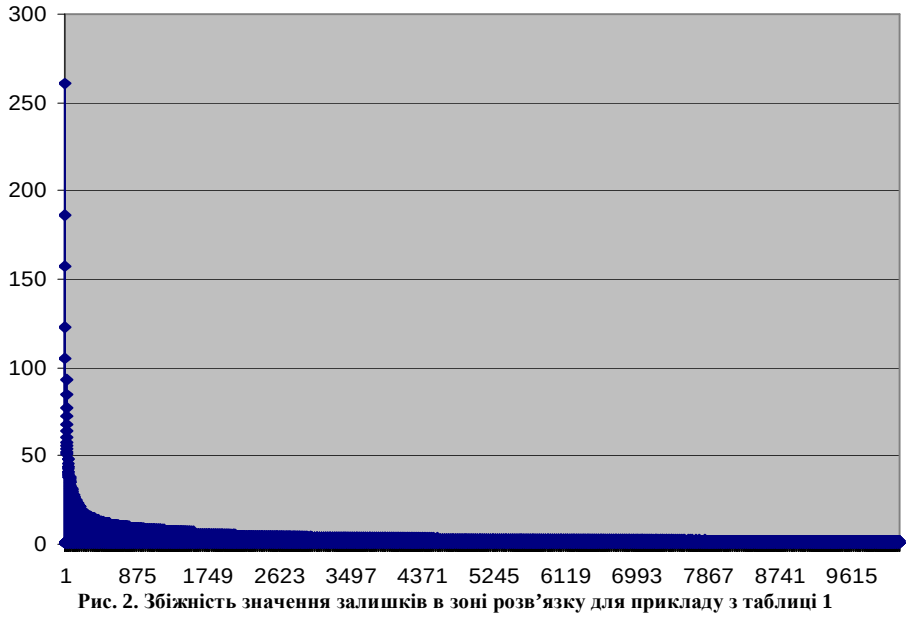

Рис. 2. Збіжність значення залишків в зоні розв'язку для прикладу з таблиці 1

В загальному випадку крок, при якому послідовності будуть збігатися, можна змінювати, тобто додавати і віднімати не тільки 2, а й інші значення. Тоді дані послідовності можна переписати наступним чином:

$$Q_{1k} = \left|P_0 - (P^* + k) - P_0 \bmod P^*\right|$$

$$Q_{2k} = \left|P_0 - (P^* + 2k) - P_0 \bmod P^* + k\right|$$

…

$$Q_{(n-1)k} = \left|P_0 - (P^* + kn) - P_0 \bmod (P^* + kn - k)\right|$$

Відповідно

$$Q_{1k}{}^* = \left|P_0 - (P^* + k) - P_0 \bmod P^*\right|$$

$$Q_{2k}{}^* = \left|P_0 - (P^* + 2k) - P_0 \bmod P^* - k\right|$$

…

$$Q_{(n-1)k}{}^* = \left|P_0 - (P^* + kn) - P_0 \bmod (P^* + kn + k)\right|$$

Даний перебір здійснюється до тих пір, поки $P^* \to 0$, $n \to Q_i$, де Q_i – значення при якому $P^* - Q_i = P_1$. P_1 – розв'язок задачі факторизації. В таблиці 2 представлено значення змін залишкової функції $P^*{}_n$ в зоні розв'язку.

Таблиця 2

Кількості змін залишкової функції в зоні розв'язку

1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	2	2	2	2
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	2	2
2	2	2	2	2	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2
2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2
2	1	2	2	2	2	2	2	2	2	2	2	2	2	1	2	2	2	2	2
2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	1	2	2
2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	1	2
2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	1	2
2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	1	2	2	2
2	2	2	2	2	1	2	2	2	2	2	2	2	2	1	2	2	2	2	2
2	2	1	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	1	2
2	2	2	2	2	2	1	2	2	2	2	2	2	1	2	2	2	2	2	2
2	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1	2	2	2	2
2	2	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1	2	2	2
2	2	2	1	2	2	2	2	2	1	2	2	2	2	2	2	1	2	2	2
2	2	1	2	2	2	2	2	2	1	2	2	2	2	2	1	2	2	2	2
2	1	2	2	2	2	2	1	2	2	2	2	2	1	2	2	2	2	2	1
2	2	2	2	2	1	2	2	2	2	2	1	2	2	2	2	1	2	2	2
2	2	1	2	2	2	2	1	2	2	2	2	2	1	2	2	2	2	1	2
2	2	2	2	1	2	2	2	2	1	2	2	2	2	2	1	2	2	2	2
1	2	2	2	2	1	2	2	2	2	1	2	2	2	2	1	2	2	2	2
1	2	2	2	2	1	2	2	2	2	1	2	2	2	2	1	2	2	2	2
1	2	2	2	2	1	2	2	2	2	1	2	2	2	2	1	2	2	2	1
2	2	2	2	1	2	2	2	2	1	2	2	2	1	2	2	2	2	1	2
2	2	2	1	2	2	2	1	2	2	2	2	1	2	2	2	1	2	2	2
2	1	2	2	2	1	2	2	2	2	1	2	2	2	1	2	2	2	1	2
2	2	2	1	2	2	2	1	2	2	2	1	2	2	2	1	2	2	2	2
1	2	2	2	1	2	2	2	1	2	2	2	1	2	2	2	1	2	2	2
1	2	2	2	1	2	2	2	2	1	2	2	2	1	2	2	2	1	2	2
2	1	2	2	2	1	2	2	2	1	2	2	1	2	2	2	1	2	2	2
1	2	2	2	1	2	2	2	1	2	2	2	1	2	2	2	1	2	2	2
1	2	2	1	2	2	2	1	2	2	2	1	2	2	2	1	2	2	1	2
2	2	1	2	2	2	1	2	2	1	2	2	2	1	2	2	2	1	2	2
1	2	2	2	1	2	2	2	1	2	2	1	2	2	2	1	2	2	1	2
2	2	1	2	2	1	2	2	2	1	2	2	1	2	2	2	1	2	2	1
2	2	2	1	2	2	1	2	2	2	1	2	2	1	2	2	2	1	2	2
1	2	2	1	2	2	2	1	2	2	1	2	2	1	2	2	2	1	2	2
1	2	2	1	2	2	2	1	2	2	1	2	2	1	2	2	2	1	2	2
1	2	2	1	2	2	1	2	2	2	1	2	2	1	2	2	1	2	2	1
2	2	1	2	2	2	1	2	2	1	2	2	1	2	2	1	2	2	1	2

В результаті таких обчислень отримаємо відображення значень залишків функції P^*_n в околі розв'язку, які проілюстровані на рис. 2.

В зоні розв'язку графік буде мати вигляд, показаний на рис. 3.

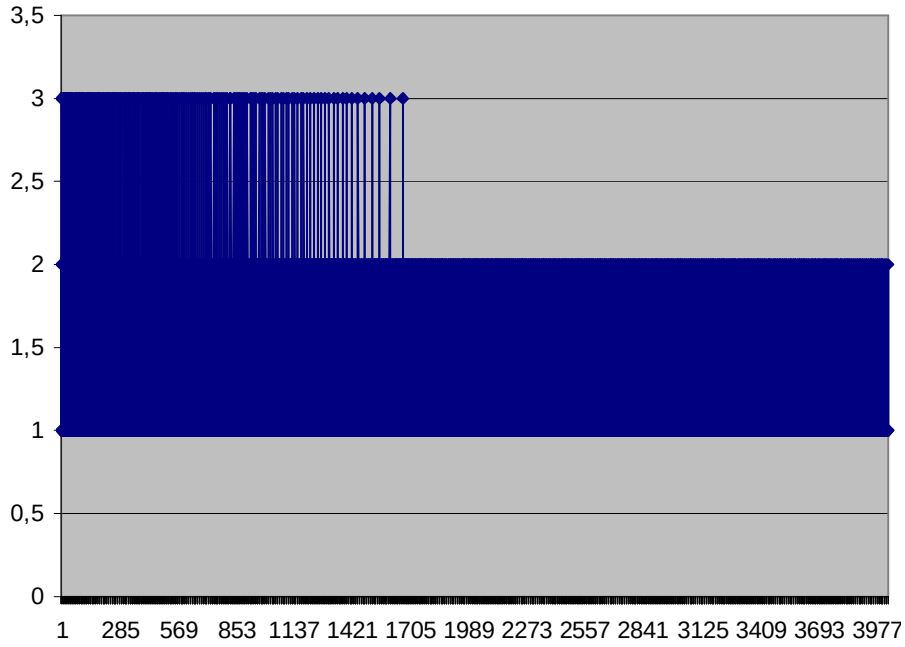

Рис. 3. Збіжність значення залишків в зоні розв'язку, деталізовано

Інші дослідження показують аналогічну збіжність в зоні розв'язку. Це дозволяє значно спростити процес факторизації прямим перебором.

При досягненні розв'язку, тобто $P^*_n = 0$, продовжуємо процес отримання залишків для $P^*_{n+1}, \ldots, P^*_{n+k}$. В результаті проведених чисельних експериментів, слід зазначити, що спостерігається симетричність екстремумів залишкової функції P^*_n відносно розв'язку задачі факторизації (рис. 4).

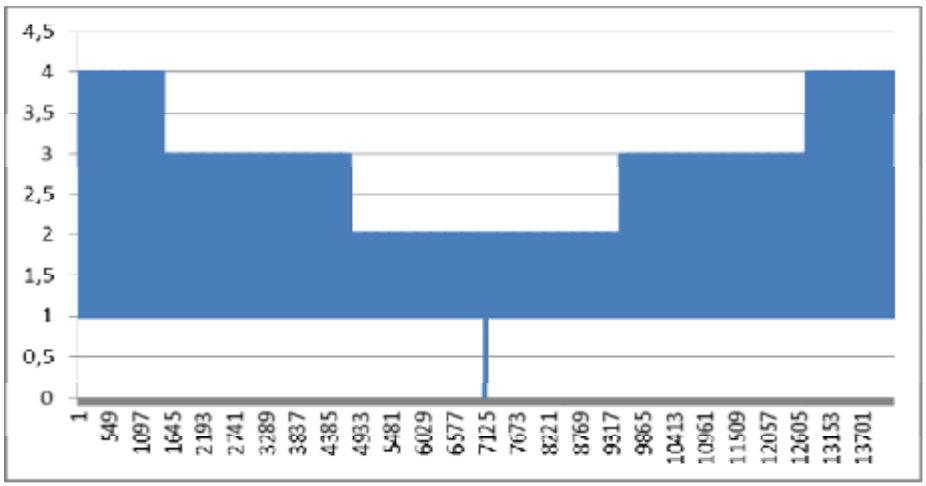

Рис. 4. Симетричність екстремумів залишкової функції в зоні розв'язку для заданого прикладу

В результаті реалізації запропонованого методу факторизації багаторозрядних чисел на основі використання ТЧБ Крестенсона нижче показано збіжність в зоні розв'язку для чисел RSA 100.

Результати чисельного експерименту свідчать про те, що кількість екстремумів до розв'язку симетрична кількості екстремумів після розв'язку. Побудуємо графічну модель, що буде відображати цю властивість (рис. 5).

Згідно з результатами досліджень можна розпочати пошук вірогідного відрізка з розв'язком, тим самим зменшити вибірку перебору на декілька порядків.

Отже, якщо ми знайдемо два симетричних відрізки на однаковій відстані від розв'язку, то вони вкажуть на сам розв'язок.

Таблиця 3

Симетричність кількості змін залишкової функції в зоні розв’язку

Кількість екстремумів до розв'язку	Кількість екстремумів після розв'язку												
1	1	8	8	1	1	8	8	1	1	8	8	1	1
8	8	1	1	8	8	1	1	8	8	1	1	8	8
1	1	8	8	1	1	8	8	1	1	8	8	1	1
8	8	1	1	8	8	1	1	8	8	1	1	8	8
1	1	8	8	1	1	8	8	1	1	8	8	1	1
8	8	1	1	8	8	1	1	8	8	1	1	8	8
1	1	8	8	1	1	8	8	1	1	8	8	1	1
8	8	1	1	8	8	1	1	8	8	1	1	8	8
1	1	8	8	1	1	8	8	1	1	8	8	1	1
8	8	1	1	8	8	1	1	8	8	1	1	8	8
1	1	8	8	1	1	8	8	1	1	8	8	1	1
8	8	1	1	8	8	1	1	8	8	1	1	7	7
1	1	8	8	1	1	8	8	1	1	8	8	1	1
8	8	1	1	8	8	1	1	8	8	1	1	8	8
1	1	7	7	1	1	8	8	1	1	8	8	1	1
8	8	1	1	8	8	1	1	8	8	1	1	8	8
1	1	8	8	1	1	8	8	1	1	8	8	1	1
8	8	1	1	8	8	1	1	8	8	1	1	8	8
1	1	8	8	1	1	8	8	1	1	8	8	1	1
8	8	1	1	8	8	1	1	8	8	1	1	8	8
1	1	8	8	1	1	7	7	1	1	8	8	1	1
8	8	1	1	8	8	1	1	8	8	1	1	8	8
1	1	8	8	1	1	8	8	1	1	8	8	1	1
8	8	1	1	8	8	1	1	8	8	1	1	8	8
1	1	8	8	1	1	7	7	1	1	8	8	1	1
8	8	1	1	8	8	1	1	8	8	1	1	8	8
1	1	8	8	1	1	8	8	1	1	8	8	1	1
8	8	1	1	8	8	1	1	8	8	1	1	8	8
1	1	8	8	1	1	7	7	1	1	8	8	1	1

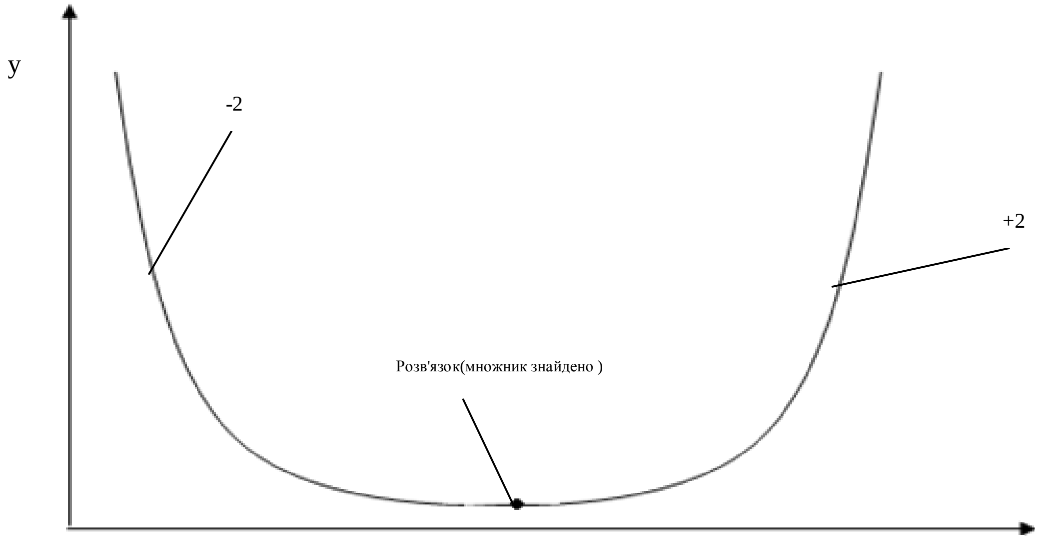

Рис. 5. Модель симетричності кількості екстремумів в зоні рішення RSA 100

Розглянемо ще декілька прикладів з багаторозрядними числами.

P_0 111000000100000011101110001010101010011100110111001000010101011001000111111011

$P*$ 101010010110110010000110000111100011011

P_1 110011100010101011110010100110111100101

P_2 100010110011101010001010100110101011111

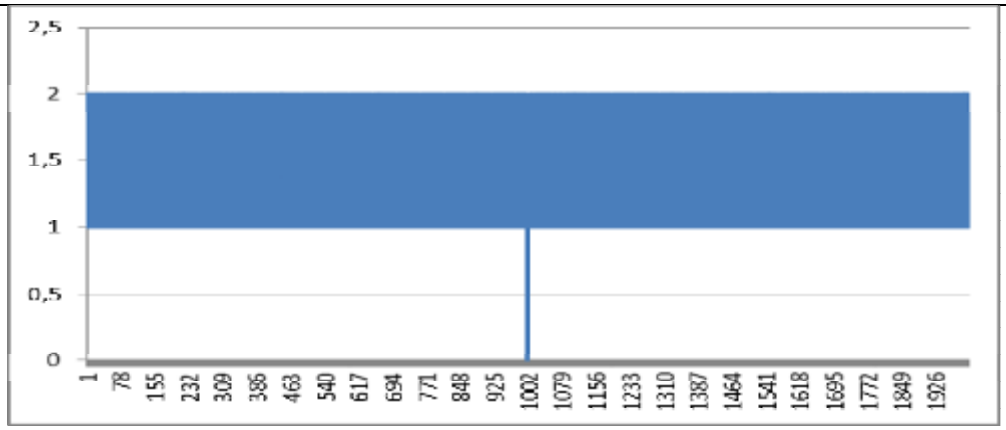

Рис. 6. Збіжність екстремумів залишкової функції для прикладу 1

P_0 11100001000001110010110101101000011100110010110011010011010100110101010000010110110011111110000011

P^* 10101001101101110101100011101001010001010001010000

P_1 11001110011100010101011110010100110111100101010001

P_2 10001011100001011111110000001111010001111000010011

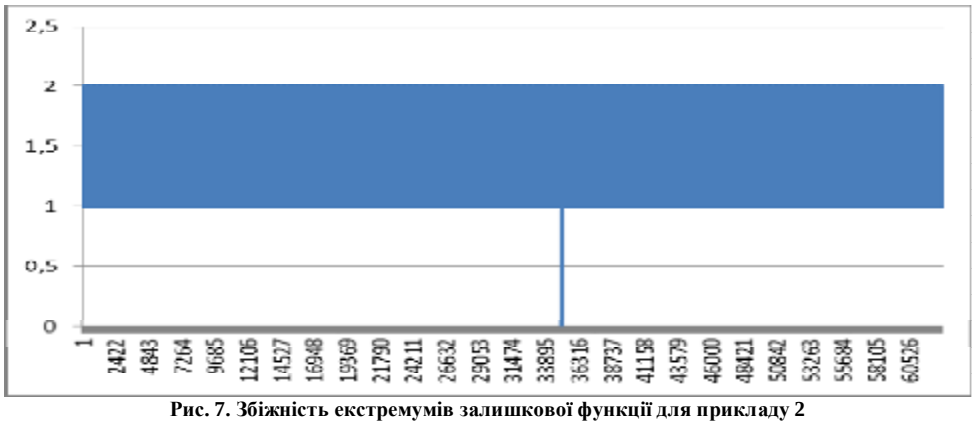

Рис. 7. Збіжність екстремумів залишкової функції для прикладу 2

Для багаторозрядних чисел подібні дослідження провести досить складно, тому доцільно досліджувати залишкову функцію з багаторозрядним кроком. Наприклад проведемо дослідження для RSA 100, результати подібного дослідження зображені на рис. 8.

Рис. 8. Результати дослідження екстремумів залишкової функції для RSA 100 з використанням багаторозрядного кроку

Аналіз чисельного експерименту (рис. 4, рис. 6, рис. 7) свідчить, що розв'язок задачі факторизації запропонованим методом.

$$P_0 \bmod P^* = X_1 \quad (1)$$
$$P_0 \bmod P^* - 2 = X_2$$
$$P_0 \bmod P^* - 2 = X_n$$

Шукаємо доти, поки $X_n \le X_{n+1}$ (2), тоді переходимо на наступний етап, на якому початкове значення лічильника $i = 0$, продовжуємо дані дії (1).

Такий ітераційний процес показує збіжність даної послідовності до розв'язку поставленої задачі факторизації, відображає симетричність залишкової функції $f(Q^*)$.

Висновки

Розроблений метод дозволяє виявити та локалізувати зону розв'язку задачі факторизації для багаторозрядних чисел за рахунок симетричності екстремумів залишкової функції, що в свою чергу забезпечить значне зменшення експоненційної складової процесу факторизації на декілька порядків.

Література

1. Теорія джерел інформації : монографія / Я.М. Николайчук. – Тернопіль : ТНЕУ, Економічна думка. – 2008 – 536 с.

2. Касянчук М.М. Теорія алгоритмів RSA та Ель–Гамаля в розмежованій системі числення Рademахера–Крестенсона / М.М. Касянчук, І.З. Якименко, О.І. Волинський, І.Р. Пітух // Вісник Хмельницького національного університету. Технічні науки – 2011. – № 3.– С. 265–273.

3. Задірака В.К. Комп'ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях / В.К. Задірака, А.М. Кудін, В.О. Людвиченко, О.С. Олексюк. – К. ; Т. : Підруч. і посіб., 2007. – 272 с.

References

1. Y.M. Nykolaichuk, Teoriia dzherel informatsii: monohrafiia. Ternopil: TNEU, Ekonomichna dumka, 2008, 536 p.

2. M.M. Kasianchuk, I.Z. Yakymenko, O.I. Volynskyi, I.R. Pitukh, "Teoriia alhorytmiv RSA ta El–Hamalia v rozmezhovanii systemi chyslennia Rademakhera–Krestensona", Herald of Khmelnytsky National University, Technical sciences, 2011, Issue 3, p. 265–273.

3. V.K. Zadiraka, A.M. Kudin, V.O. Liudvychenko, O.S. Oleksiuk. Kompiuterni tekhnolohii kryptohrafichnoho zakhystu informatsii na spetsialnykh tsyfrovykh nosiiakh. Kyiv-Ternopil, Pidruch. i posib., 2007, 272 p.

Рецензія/Peer review : 7.7.2015 р. Надрукована/Printed : 30.8.2015 р.
Рецензент: д.т.н., проф. М.П. Дивак