УДК 681.32

О.О. Чубей[1], А.З. Шумський[2], С.В. Івасьєв[2]

[1]Галицький коледж ім. В. Чорновола

[2]Тернопільський національний економічний університет

ВИЗНАЧЕННЯ ІНТЕРВАЛЬНОГО РІШЕННЯ ЗАДАЧІ ФАКТОРИЗАЦІЇ ДЛЯ КРИПТОГРАФІЧНИХ СИСТЕМ

Вступ. Важливим напрямком розвитку досліджень у галузі методів та програмно-апаратних засобів опрацювання цифрових даних є вдосконалення алгоритмів, які використовуються в сучасних комп'ютерних системах, та розвиток математичних основ теорії чисел на базі кодових систем різних теоретико-числових базисів, до яких належать: унітарний, Хаара, Радемахера, Крестенсона, Уолша, Галуа тощо[1,2]. До таких задач відноситься задача факторизації багаторозрядних чисел, оскільки на основі її високої обчислювальної складності базуються сучасні криптосистеми RSA, Рабіна.

Метою роботи є дослідження визначення інтервального рішення задачі факторизації для криптографічних систем.

1. Метод визначення околу рішення задачі факторизації

Метод Ферма ґрунтується на розв'язанні діофантового рівняння виду:

$$F_k - P_0 = \overset{\bullet}{\Delta}^2 \qquad (1)$$

де P_0 – відоме число, яке рівне добутку двох багаторозрядних простих чисел, Fk - повний квадрат:

$$P_0=P_1\times P_2 \qquad (2)$$

Метод пошуку P_1 і P_2 є складним, оскільки потрібно здійснювати операцію ділення над БРЧ, що призводить до експоненційного зростання складності:

$$\frac{P_0}{\breve{P}_1} = P_2 \ , \ P_1<P_2 \qquad (3)$$

При розрядності 100 – 1000 біт P_0 і відповідно 50 – 500 біт P_1 та P_2 приводить до пошуку тільки одного розв'язку у цілих числах у діапазоні $2^{50} - 2^{500}$ [3].

Дослідження операції множення багаторозрядних двійкових чисел (768 біт) на основі матриць (рисунок 1) кодового

представлення $P_1 \times P_2$ показують розподіл наскрізних переносів, що, в свою чергу, вказує кількість одиниць або нулів в добутку.

Згідно методу Ферма, для факторизації числа P_0 виконуються наступні операції: обчислюється $\sqrt{P_0}$, яке округлюється до більшого цілого P_c^*. Підноситься P_c^* до квадрату $F_1 = P_c^{*2}$, після чого формується послідовність квадратів згідно співвідношень $F_1 = (P_c^*+1)^2$, $F_2 = (P_c^*+2)^2$,…, $F_k = (P_c^*+k)^2$[4].

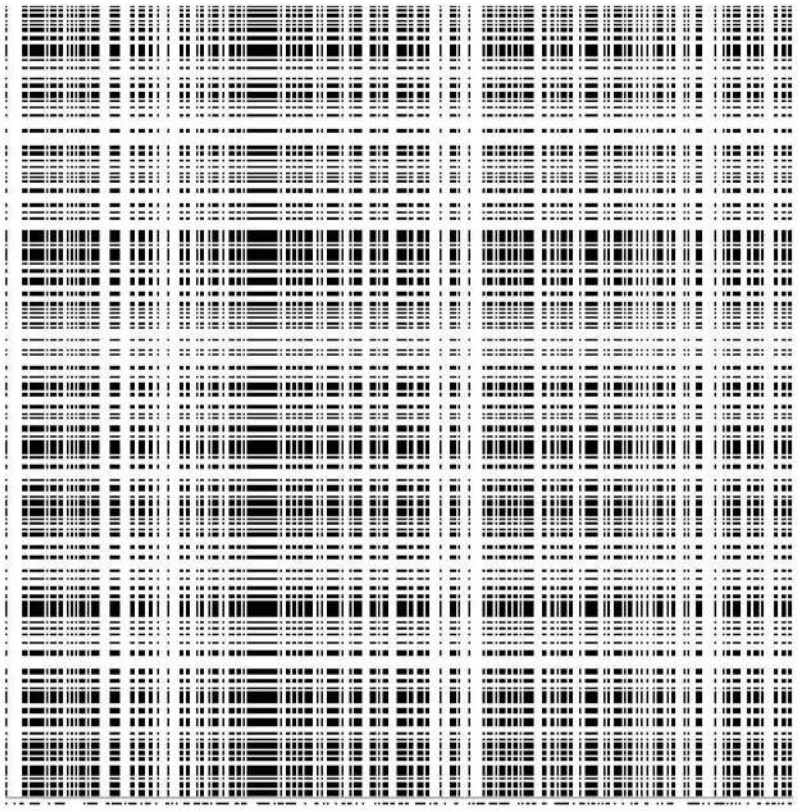

Рисунок 1 – Матриця кодового представлення множення багаторозрядних двійкових чисел (768 біт)

Перевіряється, чи добувається цілочисельний корінь з різниці $\dot{\Delta} = \sqrt{F_k - P_0}$. Якщо добувається, то числа P_1 і P_2 знаходяться згідно виразу:

$$P_1 = \dot{\Delta} - P * c + k + \dot{\Delta} = P_2 \qquad (4)$$

Обчислювальна складність методу Ферма для багаторозрядних чисел експоненційна. Із збільшенням розрядності вона відповідно зростає, оскільки число процесів k може складати 2^{300} - 2^{400} і тільки на єдино правильному кроці можливе однозначне рішення задачі факторизації[5]. Слід зазначити, що при використанні даного методу необхідно підносити до квадрату числа P_c+k з розрядністю 300-500 біт, що приводить до необхідності кожного разу знаходити різницю $F_к$-P_0 та добувати корені

квадратні з цієї різниці. Графічно модель факторизації такого методу представлено на рисунку 2.

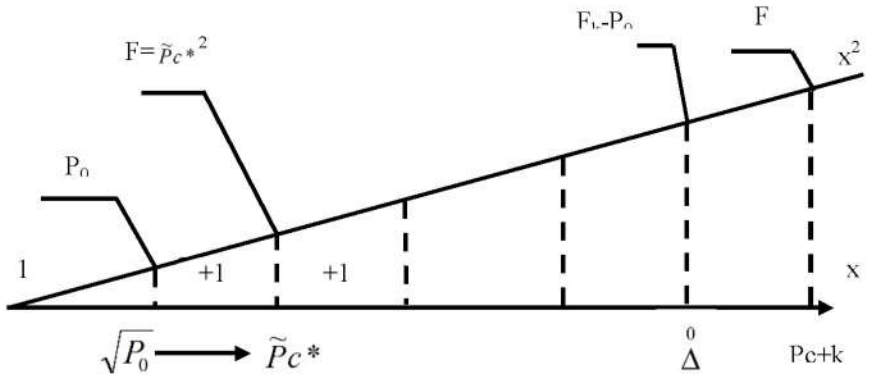

Рисунок 2 - Граф – модель спрощеного алгоритму факторизації на основі теореми Ферма

Отже, з врахуванням недоліків методу Ферма, доцільно розробити алгоритм, в основі якого лежать наступні операції: добувається $\sqrt{P_0}$ і округлюється до більшого цілого $\left|\sqrt{P_0}\right| = \widetilde{P}_c$. Піднімається $\widetilde{P}_c$ один раз до квадрату і обчислюються значення S_k згідно співвідношення:

$$S_k = k(2\widetilde{P}_c + k) + \Delta_0. \qquad (5)$$

Значення $\sqrt{S_k} = \overset{0}{\Delta}$ перевіряється на існування цілого кореня і для єдиного знайденого k з рівняння (5) визначаються шукані P_1 і P_2.

Оскільки k – багаторозрядне число, то метод, в якому відсутні операції піднесення $\widetilde{P}c + k$ до квадрату, буде мати меншу обчислювальну складність. Числа, що використовуються в методі, мають значно меншу розрядність, ніж в алгоритмі Ферма, як зображено на рисунку 3.3 граф–моделі вдосконаленого методу відображення кроків S_k.

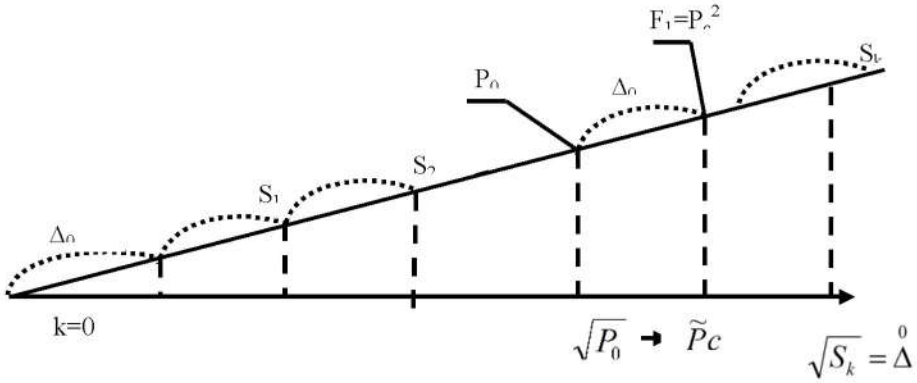

Рисунок 3 – Граф–модель спрощеного алгоритму факторизації на основі теореми Ферма

Таблиця 1 – Приклад факторизації класичним та запропонованим алгоритмом

k	n	$(\Delta_n)^2$, класичний метод	$(\Delta_n)^2$, вдосконалений метод
1	62	62^2-3811=33	62^2-3811=33
2	63	63^2-3811=158	33+125=158
3	64	64^2-3811=285	158+127=285
4	65	65^2-3811=414	285+129=414
5	66	66^2-3811=545	414+131=545
6	67	67^2-3811=678	545+133=678
7	68	68^2-3811=813	678+135=813
8	69	69^2-3811=950	813+137=950
9	70	70^2-3811=1089=33^2	950+139=1089=33^2

Таким чином, отримано розклад числа 3811 на прості множники:

$$811 = 70^2 - 33^2 = (70 + 33)(70 - 33) = 103 \cdot 37.$$

Кількість ітерацій в обох випадках буде однаковою, а найскладнішою залишається операція перевірки квадратичності лишку. Для зменшення її обчислювальної складності можна використати СЗК. Це дозволяє уникнути операцій піднесення до степеня та зменшити розрядність операндів на декілька порядків

Висновки.

В результаті досліджень видно, що у вдосконаленому методі виключається операція піднесення до квадрату. Крім того, арифметичні дії виконуються над числами, розмірність яких на декілька порядків менша, ніж у класичному методі.

Перелік джерел.

1. Buchstab, A.A. Number Theory / A.A. Buhshtab, Education, Moscow, Russia, 1966, 384 p.

2. Zadiraka, V.K. Computer technologies of cryptographic protection of information on the specific digital carriers: Textbook / V.K. Zadiraka, A.M. Kudin, V.O. Lyudvichenko, A.S. Oleksyuk, Textbooks and manuals, Kyiv - Ternopil, Ukraine, 2007, 272 p.

3. Ishmukhametov, Sh.T. Methods for factorization of integers: a tutorial / Sh.T. Ishmuhametov, Kazan University, Kazan, Russia, 2011, 190 p.

4. Zadiraka, V.K. Computer cryptology / V.K. Zadiraka, A.S. Oleksyuk, Tanha, Ternopil, Ukraine, 2002, 504 p.

5. Ya. M. Nykolaychuk, M. M. Kasianchuk, I. Z. Yakymenko. Theoretical Foundations of the Modified Perfect form of Residue Number SystemCybernetics and Systems Analysis, 52(2), pp.219-223.