Касянчук М. Теорія алгоритмів пошуку найбільшого спільного дільника у базисі Крестенсона / Касянчук М., Якименко І., Николайчук Я. // Вісник ТНТУ. — 2011. — Том 16. — № 1. — С.154-161. — (приладобудування та інформаційно-вимірювальні технології).

УДК 681.3

М. Касянчук, канд. фіз.-мат. наук; І. Якименко;
Я. Николайчук, докт. техн. наук

Тернопільський національний економічний університет

ТЕОРІЯ АЛГОРИТМІВ ПОШУКУ НАЙБІЛЬШОГО СПІЛЬНОГО ДІЛЬНИКА У БАЗИСІ КРЕСТЕНСОНА

Резюме. *Викладено теоретичні основи алгоритмів пошуку найбільшого спільного дільника при застосуванні теоретико-числових базисів Радемахера та Крестенсона. Отримано нові аналітичні вирази обчислювальної складності нових високопродуктивних алгоритмів із використанням розмежованої системи числення залишкових класів.*

Ключові слова: *найбільший спільний дільник, базиси Радемахера та Крестенсона, алгоритм, алгоритм Евкліда, розмежована система числення.*

M. Kasyanchuk, I. Iakymenko, Y. Nykolaychuk

THEORY OF ALGORITHMS SEARCH OF THE GREATEST COMMON DIVISOR IN THE BASIS OF KRESTENSON'S

The summary. *This article presents the theoretical background of algorithms for finding the greatest common divisor in case the application of theoretical and numerical bases of Rademacher's and Krestenson's. The new analytical expressions of computational complexity of high–performance algorithms using delimited numeration system of residual classes were obtained.*

Key words: *greatest common divisor, bases of Rademacher's and Krestenson's, algorithm, Euclidean algorithm, delimited numeration system.*

Актуальність дослідження. Знаходження найбільшого спільного дільника (НСД) є важливою фундаментальною задачею теорії чисел, успішне вирішення якої дозволяє вдосконалити алгоритми широкого класу прикладних задач, особливо задач захисту інформаційних потоків у комп'ютерних системах із використанням асиметричної криптографії (алгоритмів RSA, Рабіна, Ель–Гамаля, електронного цифрового підпису [1]–[3], дослідження порядку еліптичної кривої за допомогою алгоритму Шуфа) [4]. Це зумовлено необхідністю використання, як правило, взаємно простих чисел, НСД яких дорівнює 1.

У зв'язку з цим актуальною проблемою досліджень є розроблення теоретичних основ пошуку НСД із використанням теоретико-числових базисів Радемахера та Крестенсона [5], застосування яких дозволяє зменшити обчислювальну складність.

Аналіз досліджень та огляд літературних джерел. Найбільш розповсюдженим методом знаходження НСД є один із найдавніших математичних алгоритмів – алгоритм Евкліда, згідно з яким для знаходження НСД двох чисел необхідно кілька разів від більшого числа відняти менше, поки різниця не стане меншою від'ємника. Тоді цю ж саму процедуру потрібно виконати з від'ємником та різницею. Процес віднімання буде тривати до тих пір, поки від'ємник та різниця не стануть однакові. Оскільки числа, над якими виконуються операції, на кожному кроці зменшуються, то такий процес не може тривати нескінченно, а закінчиться через деяке число кроків.

Сучасний математичний запис алгоритму Евкліда має такий вигляд [6]: для будь-якого $a>b=r_0$, де a і b –цілі числа, виконується система рівнянь

$$\begin{aligned} & a = r_0 \cdot q_1 + r_1,\ 0 \le r_1 < r_0; \\ & r_0 = r_1 \cdot q_2 + r_2,\ 0 \le r_2 < r_1; \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ & r_{n-2} = r_{n-1} \cdot q_n + r_n,\ 0 \le r_n < r_{n-1}; \\ & r_{n-1} = r_n \cdot q_{n+1} + 0. \end{aligned} \qquad (1)$$

НСД ($a,\ b$) дорівнюватиме r_n, тобто останньому ненульовому членові послідовності r_i. Оскільки $r_0>r_1>r_2>\ldots>r_n>0$, то даний процес закінчиться щонайменше через b кроків, тобто потрібно виконати b ділень з остачею. Однак дана оцінка є незадовільною, оскільки для знаходження НСД двох чисел (або перевірки їх на простоту), які використовуються в сучасних асиметричних криптосистемах, затрачається дуже великий обсяг часу. В [7] показано, що для знаходження НСД за допомогою алгоритму Евкліда потрібно виконати не більше, ніж $5k$ операцій ділення з остачею, де k – кількість цифр у десятковому записі числа a. В [8] показано, що кількість кроків не перевищує $2\cdot\log_2 b+1$. Інша оцінка випливає з теореми Ламе [9], згідно з якою кількість кроків алгоритму Евкліда не перевищує $\left\lfloor \log_{\Phi}\left(\sqrt{5}a\right)\right\rfloor - 2$, де $[\alpha]$– верхнє ціле α; $\Phi = \left(1+\sqrt{5}\right)/2$ – більший корінь характеристичного рівняння послідовності Фіббоначчі.

Незважаючи на вказані оцінки та простоту програмної реалізації алгоритму Евкліда, його обчислювальна складність залишається великою, оскільки операція ділення є досить трудомісткою. Розрахунки показують, що пошук НСД із використанням алгоритму Евкліда в базисі Радемахера характеризується обчислювальною складністю щонайменше $17{,}5\cdot n(n+1)^2$, де n – розрядність числа a у двійковому коді.

Іншим недоліком алгоритму Евкліда є послідовне виконання операції ділення одна за одною, тобто неможливість його розпаралелення.

Перспективним напрямком удосконалення досліджуваних алгоритмів є розроблення теорії їх реалізації на основі розмежованої системи числення залишкових класів [10] – [11].

Мета роботи. Розробити нові високопродуктивні алгоритми знаходження НСД за допомогою розмежованої системи числення та базису Крестенсона, які характеризуються значно меншою обчислювальною складністю, ніж стандартний алгоритм Евкліда.

Алгоритм Евкліда в розмежованій системі числення. Нехай потрібно знайти НСД чисел a і b:

$$a=a_{n-1}2^{n-1}+\ldots+a_i2^i+\ldots+a_12+a_0; \qquad (2)$$

$$b=b_{n-1}2^{n-1}+\ldots+b_i2^i+\ldots+b_12+b_0, \qquad (3)$$

причому $a>b=r_0$; $a,b=0,1$.

Виходячи з (1), $r_1 = a \bmod b = (a_{n-1}2^{n-1}+\ldots+a_i2^i+\ldots+a_12+a_0) \bmod b =$ $= \left(\sum_{i=0}^{n-1}\left(a_i 2^i \bmod b\right)\right) \bmod b = \left(\sum_{i=0}^{n-1}\left(a_i r_{1i}\right)\right) \bmod b$, де $r_{1i} = 2^i \bmod b$. Це означає, що шуканий залишок дорівнюватиме сумі тих степенів двійки, для яких відповідно $a_i=1$. Слід зазначити також, що два послідовні значення r_{1i} та $r_{1\ i+1}$ пов'язані рекурентним співвідношенням $r_{1\ i+1}=(2\cdot r_{1i}) \bmod b$. Для знаходження залишку за модулем b не обов'язково виконувати ділення з остачею, а можна обмежитися відніманням: якщо $r_{1\ i+1}<b$, то воно залишається незмінним, в іншому випадку $r_{1\ i+1}= r_{1\ i+1}-b$. Найпростіше

реалізувати описаний крок алгоритму Евкліда в розмежованій системі числення за допомогою таблиці 1.

Таблиця 1. Знаходження залишку a mod b.

a_{n-1}	a_{n-2}	…	a_i	…	a_2	a_1	a_0
r_{1n-1}	r_{1n-2}	…	$r_{1\,i}$	…	r_{12}	r_{11}	r_{10}

Згідно з таблицею 1, r_1 шукаємо як суму r_{1i} за модулем b, над якими у верхньому рядку розміщено 1, тобто $r_1 = \left(\sum_{i=0}^{n-1} r_{1i}\right) \bmod b$ при умові a_i=1.

Аналогічно будуємо таблицю 2.

Таблиця 2. Знаходження залишку b mod r_1.

$b_{n-1}=r_{0\,n-1}$	$b_{n-2}=r_{0\,n-2}$	…	$b_i=r_{0\,i}$	…	$b_2=r_{0\,2}$	$b_1==r_{0\,1}$	$b_0=r_{0\,0}$
r_{2n-1}	r_{2n-2}	…	$r_{2\,i}$	…	r_{22}	r_{21}	r_{20}

Відповідно $r_2 = \left(\sum_{i=0}^{n-1} r_{2i}\right) \bmod r_1$ при умові b_i=1.

Узагальнюючи отримані результати, запишемо вираз для знаходження будь-якого залишку: $r_j = \left(\sum_{i=1}^{n-1} r_{j-2i} r_{ji}\right) \bmod r_{j-1}$, де $r_{j-2\,i}$=0,1; $r_{ji}=2^i \bmod r_{i-1}$.

Відзначимо, що кількість кроків стандартного алгоритму Евкліда та алгоритму Евкліда в розмежованій системі числення однакові. Однак обчислювальна складність виконання кожного кроку істотно зменшується і становить $\log_2 n/2$. Загальна обчислювальна складність алгоритму Евкліда в розмежованій системі числення оцінюється виразом $O(17{,}5n(\log_2 n/2))$. Крім того, він виключає можливість розпаралелювання.

Алгоритм пошуку НСД за допомогою базису Крестенсона. Запропонований алгоритм знаходження НСД грунтується на пошуку залишків від ділення чисел a і b (a > b) в розмежованій системі числення (2), (3) на всі прості числа до $\sqrt{b}$.

Спільним дільником чисел a та b буде модуль p_j^k, який знаходимо з умови

$$\left(\sum_{i=0}^{n-1} a_{ij}\right) \bmod p_j^k = \left(\sum_{i=0}^{n-1} b_{ij}\right) \bmod p_j^k = 0, \qquad (4)$$

де $a_{ij} = a_i \cdot 2^i \bmod p_j^k$, $b_{ij} = b_i \cdot 2^i \bmod p_j^k$, p_j – просте число, менше $\sqrt{b}$, k =1,2,3, ... – степінь p_j.

Слід зазначити, що при k=1 і виконанні (4) перевіряється та ж умова при k=2 і т.д. Таким чином, враховується спільний дільник, який є степенем простого числа. Шуканий найбільший спільний дільник знаходимо як добуток отриманих за допомогою (4) спільних дільників.

Запропонований алгоритм характеризується логарифмічною обчислювальною складністю $O(m \cdot \log_2 n)$, де $m = \int_2^{\sqrt{b}} \frac{dt}{\ln t}$ – кількість простих чисел у діапазоні від 2 до $\sqrt{b}$. Крім того, він дозволяє розпаралелити виконання всіх операцій за кожним модулем і виконати факторизацію чисел a та b.

Удосконалений алгоритм пошуку НСД за допомогою базису Крестенсона. Запропонований вище алгоритм можна суттєво удосконалити шляхом скорочення

кількості модулів (тобто кількості кроків), за якими потрібно шукати залишки. Нехай маємо систему модулів, яка складається з простих чисел p_1, p_2, p_3, ..., менших $\sqrt{b}$, і для деякого p_j^k виконується умова (4). Наступний крок полягає у послідовній перевірці умови (4) для модуля $\left(p_j^k p_{j+1}^{k_1}\right)$, k_1=1,2,3,…; i=1,2,….

Таким чином, при послідовному множенні модулів отримуємо, що $НСД(a,b)=\prod_{j=1}^{s} p_j^k$, для яких виконується умова (4).

У порівнянні з попереднім, даний алгоритм використовує меншу кількість кроків, однак він не піддається розпаралелювання і не розв'язує задачу факторизації чисел.

Приклади застосування алгоритмів пошуку НСД. Нехай потрібно обчислити НСД(3843, 1449).

1. Стандартний алгоритм Евкліда:

3843=1449·1+945

1449=945·1+504

945=504·1+441

504=441·1+63

441=63·7+0

Отже, НСД(3843, 1449)=63.

2. Алгоритм Евкліда в розмежованій системі числення зручно представити у вигляді таблиці 3.

Таблиця 3. Алгоритм Евкліда в розмежованій системі числення

1	3843	1	1	1	1	0	0	0	0	0	0	1	1
2	2^imod1449	599	1024	512	256	128	64	32	16	8	4	2	1
3	1449		1	0	1	1	0	1	0	1	0	0	1
4	2^imod945		79	512	256	128	64	32	16	8	4	2	1
5	945			1	1	1	0	1	1	0	0	0	1
6	2^imod504			8	256	128	64	32	16	8	4	2	1
7	504				1	1	1	1	1	1	0	0	0
8	2^imod441				256	128	64	32	16	8	4	2	1
9	441				1	1	0	1	1	1	0	0	1
10	2^imod63				4	2	1	32	16	8	4	2	1

З рядка 2 бачимо, що (599+1024+512+256+2+1)mod 1449=945.

З рядка 4 – (79+256+128+32+8+1)mod 945=504.

З рядка 6 – (8+256+128+32+16+1)mod 504=441.

З рядка 8 – (256+128+64+32+16+8)mod 441=63.

З рядка 10 – (4+2+32+16+8+1)mod 63=0.

Таким чином можна отримати НСД, уникнувши громіздкої операції ділення.

3. Пошук НСД у базисі Крестенсона.

Дану задачу також зручно представити у вигляді таблиці 4, врахувавши, що $\sqrt{1449}\approx 38$.

Таблиця 4. Знаходження залишків за простими модулями

1		2048	1024	512	256	128	64	32	16	8	4	2	1
2	3843	1	1	1	1	0	0	0	0	0	0	1	1
3	1449		1	0	1	1	0	1	0	1	0	0	1
4	2^lmod2	0	0	0	0	0	0	0	0	0	0	0	1
5	2^lmod3	2	1	2	1	2	1	2	1	2	1	2	1
6	2^lmod5	3	4	2	1	3	4	2	1	3	4	2	1
7	2^lmod7	4	2	1	4	2	1	4	2	1	4	2	1
8	2^lmod11	2	1	6	3	7	9	10	5	8	4	2	1
9	2^lmod13	7	10	5	9	11	12	6	3	8	4	2	1
10	2^lmod17	8	4	2	1	9	13	15	16	8	4	2	1
11	2^lmod19	15	17	18	9	14	7	13	16	8	4	2	1
12	2^lmod23	1	12	6	3	13	18	9	16	8	4	2	1
13	2^lmod29	18	9	19	24	12	6	3	16	8	4	2	1
14	2^lmod31	2	1	16	8	4	2	1	16	8	4	2	1
15	2^lmod37	13	25	31	34	17	27	32	16	8	4	2	1
16	2^lmod9	5	7	8	4	2	1	5	7	8	4	2	1
17	2^lmod27	23	25	26	13	20	10	5	16	8	4	2	1

З таблиці 4 шукаємо залишки за простими модулями.

Рядок 4: 3843 mod 2=1; 1449 mod 2=1.

Рядок 5: 3843 mod 3=(2+1+2+1+2+1) mod 3=0; 1449 mod 3=(1+1+2+2+2+1) mod 3=0.

Рядок 6: 3843 mod 5=(3+4+2+1+2+1) mod 5=3; 1449 mod 3=(4+1+3+2+3+1) mod 5=4.

Рядок 7: 3843 mod 7=(4+2+1+4+2+1) mod 7=0; 1449 mod 7=(2+4+2+4+1+1) mod 7=0.

Рядок 8: 3843 mod 11=(2+1+6+3+2+1) mod 11=4; 1449 mod 11=(1+3+7+10+8+1) mod 3=8.

Рядок 9: 3843 mod 13=(7+10+5+9+2+1) mod 13=8; 1449 mod 3=(10+9+11+6+8+1) mod 13=6.

Рядок 10: 3843 mod 17=(8+4+2+1+2+1) mod 17=1; 1449 mod 17=(4+1+9+15+8+1) mod 17=4.

Рядок 11: 3843 mod 19=(15+17+18+9+2+1) mod 19=5; 1449 mod 19=(17+9+14+13+8+1) mod 19=5.

Рядок 12: 3843 mod 23=(1+12+6+3+2+1) mod 23=2; 1449 mod 23=(12+3+13+9+8+1) mod 23=0.

Рядок 13: 3843 mod 29=(18+9+19+24+2+1) mod 29=15; 1449 mod 29=(9+24+12+3+8+1) mod 29=28.

Рядок 14: 3843 mod 31=(2+1+16+8+2+1) mod 31=30; 1449 mod 31=(1+8+4+1+8+1) mod 31=23.

Рядок 15: 3843 mod 37=(13+25+31+34+2+1) mod 37=32; 1449 mod 37=(25+34+17+32+8+1) mod 37=6.

Дані розрахунки показують, що спільними простими дільниками є числа 3 та 7. Для знаходження НСД потрібно перевірити їх степені:

Рядок 16: 3843 mod 3^2=(5+7+8+4+2+1) mod 3^2=0; 1449 mod 3^2 =(7+4+2+5+8+1) mod 3^2=0.

Рядок 17: 3843 mod 3^3=(23+25+26+13+2+1) mod 3^3=9; 1449 mod 3^3 =(25+13+20+5+8+1) mod 3^3=18.

Число 7^2=49>38 і його можна не перевіряти. Отже, НСД(3843, 1449)= $3^2 \cdot 7$=63. Даний метод дозволяє провести факторизацію чисел, наприклад $1449=3^2 \cdot 7 \cdot 23$. Крім того, обчислення можна виконувати паралельно за різними модулями.

4. Удосконалений алгоритм пошуку НСД у базисі Крестенсона.

Будуємо таблицю 5.

Таблиця 5. Знаходження залишків в удосконаленому алгоритмі

1		2048	1024	512	256	128	64	32	16	8	4	2	1
2	3843	1	1	1	1	0	0	0	0	0	0	1	1
3	1449		1	0	1	1	0	1	0	1	0	0	1
4	2^imod2	0	0	0	0	0	0	0	0	0	0	0	1
5	2^imod3	2	1	2	1	2	1	2	1	2	1	2	1
6	2^imod9	5	7	8	4	2	1	5	7	8	4	2	1
7	2^imod27	23	25	26	13	20	10	5	16	8	4	2	1
8	2^imod45	23	34	17	31	38	19	32	16	8	4	2	1
9	2^imod63	32	16	8	4	2	1	32	16	8	4	2	1
10	2^imod441	284	142	71	256	128	64	32	16	8	4	2	1
11	2^imod693	662	331	512	256	128	64	32	16	8	4	2	1

Аналізуємо таблицю 5.

Рядок 4: 3843 mod 2=1; 1449 mod 2=1.

Рядок 5: 3843 mod 3=(2+1+2+1+2+1) mod 3=0; 1449 mod 3=(1+1+2+2+2+1) mod 3=0.

Рядок 6: 3843 mod 9=(5+7+8+4+2+1) mod 9=0; 1449 mod 9 =(7+4+2+5+8+1) mod 9=0.

Рядок 7: 3843 mod 27=(23+25+26+13+2+1) mod 27=9; 1449 mod 27 =(25+13+20+5+8+1) mod 27=18.

Рядок 8: 3843 mod 45=(23+34+17+31+2+1) mod 45=18; 1449 mod 45=(34+31+38+32+8+1) mod 3=8.

Рядок 9: 3843 mod 63=(32+16+8+4+2+1) mod 63=0; 1449 mod 63=(16+4+2+32+8+1) mod 63=0.

Рядок 10: 3843 mod 441=(284+142+71+256+2+1) mod 441=315; 1449 mod 441=(142+256+128+32+8+1) mod 441=126.

Рядок 11: 3843 mod 693=(662+331+512+256+2+1) mod 693=378; 1449 mod 693=(331+256+128+32+8+1) mod 693=63.

Із розрахунків також випливає, що НСД(3843, 1449)=63.

Крім того, зазначимо, що в двох останніх алгоритмах не обов'язково шукати залишки від обох чисел a та b. Досить знайти залишки від меншого числа і тільки при їх рівності 0 перевіряти друге число.

Оцінка обчислювальної складності відомого та запропонованих алгоритмів пошуку НСД. Складність запропонованих алгоритмів визначається обчислювальною складністю таких операцій:

1) знаходження залишків a_j, b_j чисел X, Y за простими модулями $p_j^{m_j}$, для яких виконується умова $a_j = b_j = 0$;

2) обчислення добутку модулів $Z = НСД(X, Y) = \prod_{j=1}^{k} p_j^{m_j}$.

У таблиці 6 наведено оцінки обчислювальної складності основних операцій алгоритму пошуку НСД у базисі Крестенсона, що дозволяє зробити порівняльний аналіз із вищенаведеними алгоритмами пошуку найбільшого спільного дільника.

Таблиця 6. Обчислювальна складність основних операцій алгоритму пошуку НСД у базисі Крестенсона та його удосконалення

№	Основні операції	Обчислювальна складність
1	$p_j^{m_j}$	$O\left(\log_2 n \cdot \left(\log_2 n + \frac{n}{2}\right)\right)$
2	$a_j^{(m)} = res\left(\sum_{i=1}^{n-1} a_{ij} (\mathrm{mod}\, p_j^m)\right)$ $b_j^{(m)} = res\left(\sum_{i=1}^{n-1} b_{ij} (\mathrm{mod}\, p_j^m)\right)$	$O\left(\log_2 n/2\right)$
3	$Z = \prod_{j=1}^{k} p_j^{m_j}$	$O(k \cdot \log_2 n)$

k – кількість модулів, для яких виконується умова $a_j = b_j = 0$.

З урахуванням даних табл. 6 загальна обчислювальна складність запропонованого алгоритму пошуку НСД у базисі Крестенсона та його удосконалення буде визначатися сумою складностей основних операцій, а саме: $O\left(\log_2 n \cdot \left(\log_2 n + \frac{n}{2} + k \cdot \log_2 n\right) + n \cdot \log_2 n/2\right)$ і $O3\left(\log_2 n\left(\log_2 n + k \cdot \log_2 n + \frac{n}{2}\right) + \frac{n}{2} \cdot \log_2 \frac{n}{2}\right)$ відповідно. На рис. 1 зображено графіки, які характеризують складності існуючого та запропонованих алгоритмів залежно від розрядності компонентів Z .

Чисельний експеримент оцінки складностей запропонованих алгоритмів пошуку НСД показує, що в діапазоні двійкових розрядів від 0 до 42 бітів слід використовувати удосконалення реалізації алгоритму Евкліда з використанням розмежованої системи числення Радемахера – Крестенсона, а при збільшенні розрядності чисел – алгоритм пошуку НСД в базисі Крестенсона та його удосконалення.

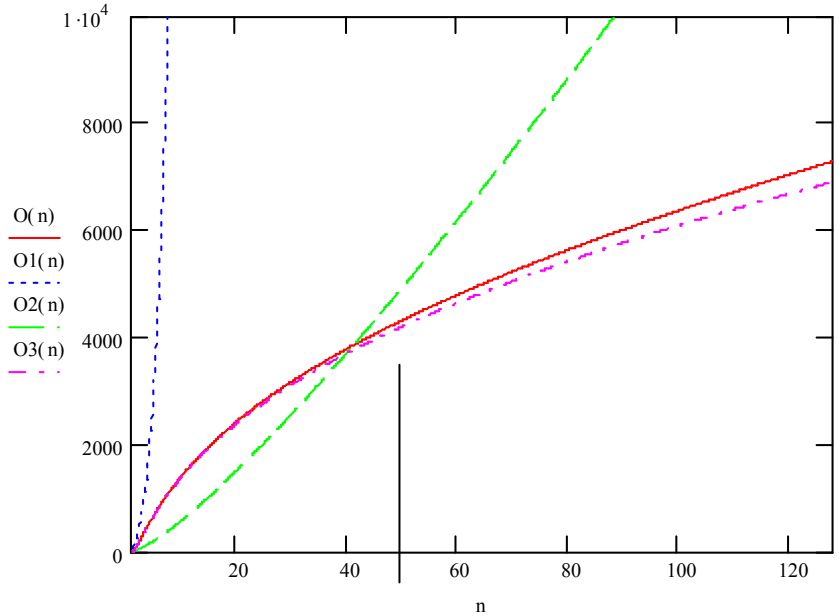

Рисунок 1. Складності алгоритмів пошуку НСД(X, Y), $O(n)$ – у базисі Крестенсона, $O1(n)$ – алгоритму Евкліда, $O2(n)$ – удосконалення реалізації алгоритму Евкліда з використанням розмежованої системи числення, $O3(n)$ – удосконалений алгоритм пошуку НСД у базисі Крестенсона

Висновки. Запропоновані теоретичні основи пошуку НСД із застосуванням теоретико-числового базису Крестенсона та розмежованої системи числення залишкових класів дозволяють зменшити обчислювальну складність на 1–2 порядки, проводити обчислення з використанням паралельної технології та ефективно використовувати для реалізації високопродуктивних алгоритмів опрацювання і захисту інформаційних потоків на основі асиметричних алгоритмів шифрування.

Література

1. Задірака В. Комп'ютерна криптологія: підручник / В. Задірака, О. Олексюк. – К., 2002. – 504 с.
2. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.П. Шаньгин; под ред. В.Ф.Шаньгина. – М.: Радио и связь, 1999. – 328с.
3. Фергюсон Н. Практическая криптография: пер. с англ. / Н. Фергюсон, Б. Шнайер. – М.: Вильямс, 2005. – 424 с.
4. Якименко І.З. Прискорення алгоритму Шуфа методом паралельних обчислень / І.З. Якименко, А.А.Хомінчук: матеріали дванадцятої наукової конференції Тернопільського державного технічного університету імені Івана Пулюя (Тернопіль, 14–15 травня 2008 р.). – 116 с.
5. Николайчук Я.М. Теоретичні основи базисних перетворень СЗК / Я.М. Николайчук, Ю.С.Федорович // Матеріали наукової конференції «Автоматика 2000». – Львів, 2000. – С. 120.
6. Бородін О.І. Теорія чисел / О.І. Бородін. – К.: Вища школа, 1970. – 275 с.
7. Варновский Н.П. Криптография и теория сложности / Н.П. Варновский // Математическое просвещение. – 1998. – №2. – С. 71–86.
8. Вербіцький О.В. Вступ до криптології. / О.В. Вербіцький. – Львів:ВНТЛ, 1998. – 248 с.
9. Бухштаб А.А. Теория чисел / А.А. Бухштаб. – М.: Просвещение, 1966. – 384 с.
10. Волинський О.І. Методи порівняння та сумування в розмежованій системі числення / О.І.Волинський // Поступ в науку. Збірник праць Бучацького інституту менеджменту і аудиту. – 2009. – Т1, №4. – С. 91–94.
11. Якименко І.З. Розмежована система числення залишкових класів та спецпроцеси на її основі / І.З.Якименко, О.І. Волинський // Поступ в науку. Збірник праць Бучацького інституту менеджменту і аудиту. – 2009. – Т1, №4. – С. – 94–98.

Отримано 10.01.2011