УДК 681.32

Я. М. Николайчук, М. М. Касянчук, І. З. Якименко, С. В. Івасьєв
Тернопільський національний економічний університет,
кафедра спеціалізованих комп'ютерних систем

ЕФЕКТИВНИЙ МЕТОД МОДУЛЯРНОГО МНОЖЕННЯ В ТЕОРЕТИКО-ЧИСЛОВОМУ БАЗИСІ РАДЕМАХЕРА–КРЕСТЕНСОНА

Розроблено ефективний метод модулярного множення з використанням теоретико-числового базису Радемахера–Крестенсона, який дає змогу удвічі зменшити кількість суматорів під час виконання цієї операції та використовувати в асиметричних системах захисту інформації для зменшення складності обчислень, під час генерування ключів, шифруванні/дешифруванні.

Ключові слова: модулярне множення, теоретико-числовий базис, часова та апаратна складність, суматор.

EFFECTIVE METHOD OF MODULAR MULTIPLICATION IN THEORETIC-NUMERICAL RADEMACHER-KRESTENSON'S BASIS

An effective modular multiplication method using theoretic-numerical Rademacher-Krestenson's basis has been developed. The method allows decrease twice number of summators during this operation as well as using in information protection asymmetrical systems for simplifying calculations, during key generation, encryption/decryption.

Key words: modular multiplication, theoretic-numerical Rademacher-Krestenson's basis, temporary and instrument complication, summator.

Вступ

Операція модулярного множення багаторозрядних чисел є однією з найважливіших в асиметричних системах захисту інформації. Тому розроблені методи різної складності для розв’язання задачі. Одним з найефективнішим щодо швидкодії є метод множення, запропонований Карацубою [1], з часовою складністю $3n^{log_2 3} \approx 3n^{1,585}$. У цьому випадку часова складність зменшується з n^2 у двійковій системі числення до $3n^{1,585}$. Виконуючи модулярне множення, найменшою часовою складністю характеризується матрично-модульний метод у базисі Радемахера–Крестенсона [2].

Мета роботи

Отже, метою роботи є розроблення ефективного методу модулярного множення з використанням векторно-модульних операцій у розмежованій системі числення залишкових класів та двійкової теоретико-числового базису Радемахера–Крестенсона, який дасть змогу зменшити апаратну та часову складності опрацювання інформаційних потоків в асиметричних криптоалгоритмах. Для досягнення поставленої мети потрібно розв’язати низку взаємопов’язаних задач, а саме: проаналізувати теоретичні основи системи залишкових класів, розробити векторно-модульний метод модулярного множення та порівняти часову складність розробленого методу з відомими.

Теоретичні основи системи залишкових класів

Фундаментальною теоретичною основою системи залишкових класів є алгебра і теорія чисел [3], зокрема китайська теорема про залишки [4]. Зумовленість використання системи залишкових класів пояснюється тим, що часова складність виконання базових операцій є на порядок меншою порівняно з двійковою системою числення. Тому доцільно застосовувати цілочислові перетворення системи залишкових класів за такими аналітичними виразами:

1. Пряме перетворення:

$$N_k = (b_1 b_2 ... b_i ... b_k)_{(p_1 p_2 ... p_i ... p_k)};\ N_k = b_i (mod\ p_i),\ N_k = a_i p_i + b_i,\ P = \prod_{i=1}^{k} p_i;\ 0 \le N_k \le P. \quad (1)$$

2. Зворотне:

$$b_i = res N_k (mod\ p_i),\ N_k = res \sum_{i=1}^{k} b_i \cdot B_i (mod\ P),\ B_i = \frac{P}{p_i} \cdot m_i \equiv 1 (mod\ p_i), \quad (2)$$

де $p_1, p_2, \ldots, p_j, \ldots, p_k$ система взаємно простих модулів; $0 \le N_k \le P-1$ – код числа в базисі Радемахера; P – діапазон кодування чисел, в якому однозначно виконується пряме та зворотне перетворення базису Крестенсона; $0 \le b_i \le P_i - 1$ – найменший невід'ємний залишок числа N_k за модулем P_i; B_i – базисне число системи залишкових класів, заданої набором модулів $p_1, p_2, \ldots, p_j, \ldots, p_k$; $0 \le m_i \le P_i - 1$ – коефіцієнт досконалості СЗК; $(b_1 b_2 ... b_i ... b_k)_{(p_1 p_2 ... p_i ... p_k)}$ – код числа в базисі Крестенсона.

Теоретичні основи модульного множення в теоретико-числовому базисі Радемахера–Крестенсона

Оскільки в комп'ютерних системах всі операції здійснюють на основі використання двійкової системи числення, то виникає задача переходу із системи залишкових класів базису Крестенсона в базис Радемахера і навпаки, який можна виконати за допомогою розмежованої форми системи числення в базисах Радемахера–Крестенсона [5].

Розроблений метод векторно-модульного множення n–розрядних чисел $a = \sum_{i=0}^{n-1} a_i \cdot 2^i$ та $b = \sum_{j=0}^{n-1} b_j \cdot 2^j$, де a_i, b_j=0, 1, n–розрядність модуля p. Для знаходження результату операції модульного множення $a \cdot b\, mod\ p$ будують два вектор-рядки, перший з яких складається з елементів $c_0 = 2^0 b\, mod\ p$, $c_i = 2 \cdot c_{i-1}\, mod\ p$, другий – з a_i, що показано в табл. 1.

Таблиця 1

Представлення вектор-рядків модульного множення

c_{n-1}		c_i	…	c_1	c_0
a_{n-1}	…	a_j	…	a_1	a_0

Результат модульного множення двох n-розрядних чисел знаходять за формулою:

$$a \cdot b\, mod\ p = \left(\sum_{i=0}^{n-1} a_i \cdot c_i \right) mod\ p. \quad (1)$$

Розроблений метод характеризується меншою часовою та апаратною складністю порівняно з матрично-модульним у базисі Радемахера–Крестенсона внаслідок зменшення кількості суматорів з $2 \cdot log_2 n$ до $log_2 n$, тобто вдвічі.

Застосування розробленого алгоритму

Розглянемо приклад. Нехай потрібно знайти значення 7973·8921mod 135.

Згідно з алгоритмом подамо 8921 у двійковій системі числення, тобто: 8921_2=10001011011001. Після цього для знаходження операції модульного множення потрібно

скласти табл. 3, у першому рядку якої записуємо двійкове представлення 8921_2= 10001011011001, а в другому значення $c_0 = 2^0 \cdot 7973 \, mod \, 135$; $c_1 = 2 \cdot c_0 \, mod \, 135$; …; $c_i = 2 \cdot c_{i-1} \, mod \, 135$.

Для знаходження $c_0 = 2^0 \cdot 7973 \, mod \, 135$ доцільно скористатися методом знаходження залишку багаторозрядних чисел на основі використання теоретико-числового базису Радемахера–Крестенсона, запропонованого в [6].

Для цього потрібно записати в перший рядок табл. 2 двійкове представлення числа 7973_2=1111100100101, а в другий 2^imod135, де i=0,…,n-1, n- розрядність 7973.

Таблиця 2

Знаходження операції модуля в ТЧБ Радемахера–Крестенсона

1	*i*	7	6	5	4	3	2	1	0
2	7973	0	0	1	0	0	1	0	1
3	2^imod135	128	64	32	16	8	4	2	1

1	*i*	12	11	10	9	8
2	7973	1	1	1	1	1
3	2^imod135	46	23	79	107	121

Результатом пошуку залишку $c_0 = 2^0 \cdot 7973 \, mod \, 135$ =(1+4+32+121+107+79+23+46)mod135=8.

Отже, c_0=8, c_1=16, $c_2 = 32$, $c_3 = 64$; $c_4 = 128$; c_5=121, c_6=107, c_7=79, c_8=23, c_9=46, c_{10}=92, c_{11}=49, c_{12}=98, c_{13}=61.

Таблиця 3

Модульне множення в ТЧБ Радемахера–Крестенсона

1	*i*	6	5	4	3	2	1	0
2	8921	1	0	1	1	0	0	1
3	$2c_{i-1}$ *mod* 135	107	121	128	64	32	16	8

1	*i*	13	12	11	10	9	8	7
2	8921	1	0	0	0	1	0	1
3	$2c_{i-1}$ *mod* 135	61	98	49	92	46	23	79

Тоді значення 7973·8921mod 135=(8+64+128+107+79+46+61) mod 135=88.

Отже, розроблений метод модульного множення з використанням векторно-модульних операцій в теоретико-числовому базисі Радемахера–Крестенсона доцільно використовувати в асиметричних криптографічних алгоритмах захисту інформації [7] для зменшення складності обчислень під час генерування ключів, шифрування/дешифрування тощо.

Оцінка та порівняльний аналіз часової складності відомих та розробленого методу модульного множення

Отже, отримано новий векторно-модульний метод заміни операції множення, яка характеризується квадратичною часовою складністю $O1(n) = n^2$ – звичайний метод множення, лінійно-логарифмічною $O(n) = n \cdot log \, n \cdot log(log \, n)$ – алгоритм Шонхаге-Штрасена, або $O3(n) = n^{1,585}$, або $O4(n) = n^{1,465}$ – алгоритми Карацуби та Тома-Кука, або матрично-модульний алгоритм у ТЧБ Радемахера–Крестенсона $O2(n) = \begin{cases} 2 \, log \, n, \, якщо \; n \le 64 \\ n \, log \, n, \, в \; інших \; випадках \end{cases}$ відповідно, операцією додавання зі складністю $O5(n) = log \, n$. Результати наведено в табл. 4.

Таблиця 4

Складність відомих та запропонованого алгоритмів

Позначення	Назва	Складність
$O(n)$	Шонхаге-Штрасена	$n \cdot \log n \cdot \log(\log n)$
$O1(n)$	Стандартний	n^2
$O2(n)$	Матрично-модульний	$\begin{cases} 2\log n, \text{якщо } n \le 64 \\ n\log n, \text{інакше} \end{cases}$
$O3(n)$		$n^{1,585}$
$O4(n)$	Карацуби	$O4(n) = n^{1,465}$
$O5(n)$	Радемахера-Крестенсона	$\log n$

Графічні залежності часової складності відомих алгоритмів наведено на рис. 1, а запропонованого алгоритму – на рис. 2.

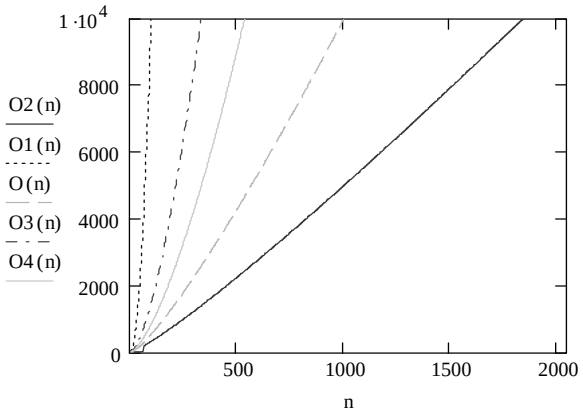

Рис. 1. Складність операції модульного множення відомих алгоритмів

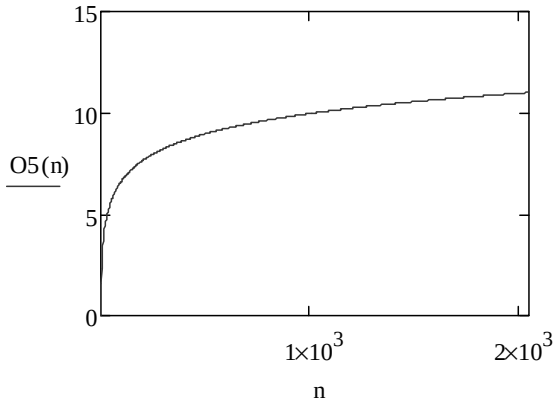

Рис. 2. Складність операції модульного множення запропонованого алгоритму

Результати досліджень показали, що основою часової складності модульного множення є складності операцій пошуку залишків за модулем та додавання. З рис. 1 та 2 видно, що використання розробленого векторно-матричного методу, який грунтується на використанні ТЧБ Крестенсона–Радемахера, дає змогу на порядок зменшити часову складність модульного множення відносно класичного методу і на 50 % порівняно з матрично-модульним алгоритмом у ТЧБ Радемахера–Крестенсона.

Висновки

Розроблено ефективний метод модульного множення на основі використання векторно-модульних операцій в теоретико-числовому базисі Радемахера–Крестенсона, який дає змогу вдвічі зменшити кількість суматорів під час виконання цієї операції та на 50 % зменшити часову складність порівняно з матрично-модульним алгоритмом.

1. Карацуба А. Умножение многозначных чисел на автоматах / А. Карацуба, Ю. Офман // Доклады Академии Наук СССР. – 1962. – Т. 145. – № 2. 2. M. Kasyanchuk, I. Yakymenko, Y. Nykolajchuk Matrix Algorithm of Processing of the Information Flow in Computer Systems Based on Theoretical and Numerical Krestenson's Based / M.Kasyanchuk, I. Yakymenko, Y.Nykolajchuk // Proceedings of the Integrational Conference TCSET'2010, february 23-27, 2010, p. – C: 241. 3. Акушский И. Я., Юдицкий Д. И. Машинная арифметика в остаточных классах. – М.: Сов. радио, 1968. – 460 с. 4. Бухштаб А. А. Теория чисел. – М.: Просвещение, 1966. – 384 с. 5. Николайчук Я. М. Теорія джерел інформації. – Тернопіль: ТзОВ "Терно-граф", 2010. – 536 с. 6. Касянчук М. М. Теорія алгоритмів пошуку найбільшого спільного дільника у базисі Крестенсона / М. Касянчук,

І. Якименко, Я. Николайчук // Вісник ТНТУ. – 2011. – Т. 16. – № 1. – С. 154–161. 7. Касянчук М. М., Якименко І. З., Волинський О. І., Пітух І.Р. Теорія алгоритмів RSA та Ель–Гамаля в розмежованій системі числення Радемахера–Крестенсона // Вісник Хмельницького національного університету "Технічні науки". – 2011. – №3.– С. 265–273.

УДК 621.382

С. П. Новосядлий, Л. В. Мельник
Прикарпатський національний
університет імені Василя Стефаника

ФІЗИКО-ТОПОЛОГІЧНІ АСПЕКТИ МОДЕЛЮВАННЯ АРСЕНІДГАЛІЄВОГО СУПЕР-БЕТА ТРАНЗИСТОРА НА ГЕТЕРОСТРУКТУРАХ ДЛЯ ШВИДКОДІЮЧИХ ВІС КОМП'ЮТЕРНИХ СИСТЕМ

Серед напівпровідників найпоширенішим у мікроелектроніці для створення цифрових мікросхем був і залишається кремній. Разом з тим сьогодні почали інтенсивно впроваджувати мікросхеми на основі арсеніду галію. Арсенідгалієві мікросхеми завдяки високій рухливості носіїв заряду в *GaAs* мають частотний діапазон функціонування, недосяжний для мікросхеми на основі кремнію (*Si*).

Ключові слова: супер-бета транзистор, гетероструктура, арсенід галію, кремній, реактори електронно-циклотронного резонансу.

PHYSICAL TOPOLOGICAL ASPECTS OF MODELING GALLIUM ARSENIDE SUPER BETA TRANSISTOR FOR SPEED LIC OFCOMPUTER SYSTEMS

Among the semiconductors in latitude use in microelectronics for digital circuits silicon has been and remains the main material. However, today began intensively implemented circuits based on gallium arsenide. Gallium arsenide circuits because of the high charge carrier mobility in *GaAs* with a frequency range of operation of reach for chips based on silicon (*Si*).

Key words: super-beta transistor, heterostructure, gallium arsenide, silicon, reactors electron-cyclotron resonance.

Вступ

Розвиток арсенідгалієвих мікросхем пов'язаний насамперед з успіхами в галузі отримання суб- і наномікронних епітаксійних плівок *GaAs*, зокрема гетероепітаксійних плівок типу *GaAs*-*AlGaAs*- *GaAs*. Високі показники було отримано тут з використанням як методу молекулярно-променевої епітаксії, так і методу НВЧ-епітаксії в реакторах електронно-циклотронного резонансу.

Постановка задачі

Задачею дослідження є розроблення швидкодіючих ВІС на основі транзисторів на гетероструктурах (супер-бета) для застосування їх у комп´ютерних системах.