УДК 519.67

АЛГОРИТМ ПОШУКУ ОБЕРНЕНОГО ЕЛЕМЕНТА ЗА МОДУЛЕМ НА ОСНОВІ ДОДАВАННЯ ЗАЛИШКУ

Рендзеняк Н.А.[1)], Мандебура Н.М.[2)], Кладій Ю.М.[3)]
Тернопільський національний економічний університет
[1,2)] *магістрант,* [3)]*студент*

I. Вступ

Модулярна арифметика є базовою при реалізації більшості криптографічних алгоритмів, зокрема алгоритмів асиметричної криптографії. Однією з найбільш обчислювально-витратних операцій модулярної арифметики є пошук мультиплікативно оберненого елемента [1] у кільці лишків за модулем *m*. Ця операція багатократно використовується при виконанні множення точки еліптичної кривої на число у афінних координатах над полем *GF*(*p*), використанні різних форм системи залишкових класів [2], у методі обміну ключам Діффі-Хелмана, криптосистемах RSA, Рабіна, Ель-Гамалята багатьох інших алгоритмах, що реалізують методи криптографії з відкритим ключем [3], тому розробка ефективних методів пошуку оберненого елемента за модулем є актуальною задачею.

II. Мета роботи

Метою даної роботи є розробка алгоритму пошуку оберненого елемента за модулем, який характеризується меншою часовою складністю в порівнянні з класичним.

III. Постановка задачі

На даний час відомі три способи пошуку оберненого елемента: перебором всіх можливих варіантів, за допомогою функції Ейлера або розширеного алгоритму Евкліда.

Однак кожен з цих способів характеризується значною обчислювальною складністю при виконанні ділень з остачею, піднесення до степеня, знаходженні функції Ейлера. Причому всі ці операції повинні виконуватися над дуже великими числами, що спричинює зменшення швидкодії та може призвести також до переповнення розрядної сітки сучасних потужних обчислювальних засобів.

IV. Алгоритм пошуку оберненого елемента за модулем на основі додавання залишку

У даній роботі запропоновано алгоритм, згідно якого для пошуку $a^{-1} \bmod b$ до числа 1 відбувається послідовне додавання залишку $c=b \bmod a$ з постійною перевіркою чи ділиться отриманий результат на число *a*. При виконанні цієї умови обернений елемент шукається за формулою $K = a^{-1} \bmod b = (i \cdot b + 1)/a$, де *i* – кількість додавань модуля.

Для експериментального дослідження часових затрат пошуку оберненого елемента за модулем з використанням розширеного алгоритму Евкліда та запропонованого методу реалізовано програмно-апаратний модуль на базі середовища розробки Aldec Active-HDL 9.1. Число *p* вибиралося простим і фіксованим, його значення становило 65537. Число *a* змінювалося від 5000 до 65000 з кроком 5000. Результати проведених досліджень показують, що тільки у двох із тринадцяти випадків при *a*=40000 та *a*=45000 запропонований метод поступається класичному, що пояснюється необхідністю виконання великої кількості операцій додавання. Середній час пошуку оберненого елемента за модулем за допомогою алгоритму Евкліда (3343600ps) в 1,47 разів більший від аналогічного параметра з використанням додавання залишків (2280619ps).

Висновки

У роботі запропоновано новий алгоритм пошуку оберненого елемента за модулем на основі послідовного додавання залишку від ділення модуля на число. Здійснено апаратну реалізацію вказаної операції на основі розширеного алгоритму Евкліда та запропонованого методу.

Список використаних джерел

1. Kasianchuk M. Conception of theoretical bases of the accomplished form of Krestensons transformation and its practical application / M. Kasianchuk // Proceedings of the 4-th International Conference ACSN–2009. – Lviv. – 2009. – PP. 299-301
2. Kasianchuk M. N. Theory and Methods of Constructing of Modules System of the Perfect Modified Form of the System of Residual Classes / M. N Kasianchuk, Ya. N. Nykolaychuk, I. Z. Yakymenko //Journal of Automation and Information Sciences. – 2016. – Vol.48, №8. – p.56-63.
3. Касянчук М.М. Теорія алгоритмів RSA та Ель-Гамаля в розмежованій системі числення Радемахера – Крестенсона / М.М. Касянчук, І.З. Якименко, О.І. Волинський, І.Р. Пітух // Вісник Хмельницького національного університету. Технічні науки. – 2011. – № 3. – С. 265–273.