УДК 621.391

К.т.н., доцент Сулема Є.С., студент Заворотній А.М.

Національний технічний університет України
«Київський політехнічний інститут»

МОДИФІКОВАНИЙ МЕТОД ВИКОНАННЯ ПЕРЕТВОРЕННЯ ФЕРМА

Abstract

Yevgeniya S. Sulema, assoc. prof., PhD; Andrii Zavorotnii, student

Modified Method of Fermat's Transformation Fulfillment

This paper is devoted to the enhancement of Fermat's transformation algorithm in order to achieve less operative complexity. This modification consists in decimation in time and frequency. The proposed modification doesn't lead to recursive form of algorithm and allows to decrease the operative complexity in 3-4 times.

Вступ

Перетворення Ферма та Мерсена є найпоширенішими серед теоретико-числових перетворень, що у свою чергу широко використовуються для виконання згорток в цілочисельних полях. Не існує єдиного швидкого алгоритму теоретико-числових перетворень, тому в загальному випадку використовується рекурсивний алгоритм Кулі-Тьюкі, що зводить перетворення до серій перетворень менших розмірів.

Перетворення Мерсена та Ферма використовуються завдяки своїй операційній простоті. Особливістю цих перетворень є фіксований розмір послідовності, над якою виконується перетворення, в кожному конкретному полі. В даній статті пропонується алгоритмічна модифікація перетворення Ферма, що зменшує операційну складність даного теоретико-числового перетворення.

Постановка задачі

Задача полягає в модифікації перетворення Ферма для 32 елементів таким чином, щоб його реалізація мала меншу операційну складність, ніж його канонічна форма.

Термінологія

Теоретико-числове перетворення – дискретне перетворення Фур'є над полем Галуа.

Перетворення Ферма – теоретико-числове перетворення в полі з модулем, що є простим числом Ферма $F_P = 2^{2^P} + 1$ та діє над послідовністю розміру $2^{(P+1)}$.

Операційна складність алгоритму – мінімальна кількість атомарних операцій, що містяться в алгоритмі та не можуть бути замінені на більш прості. Може бути визначена як набір абсолютних або відносних значень.

Опис методу

Теоретико-числові перетворення мають такий самий вигляд і таке саме призначення, що і дискретне перетворення Фур'є в комплексному полі [1]:

$$F_k = \sum_{n=0}^{N-1} x_n \, g^{-nk} \ mod \, M,$$

де *M* – модуль поля Галуа, для якого записане перетворення,

N – довжина послідовності, над якою здійснюється перетворення,

g – примітивний корінь одиниці ступеня N, що за означенням – це елемент **GF**(*M*), для якого виконується $g^k = 1 \, mod \, M$ для $k = N$ і не виконується для всіх $0 < k < N$.

Особливістю перетворень Ферма є те, що в них примітивним коренем є двійка, що дозволяє виконувати перетворення без операцій множення. В полі Галуа **GF**(F_4) ми отримаємо перетворення Ферма вигляду [2]:

$$F_k = \sum_{n=0}^{31} 2^{nk} x_n \ mod \ (2^{16} + 1)$$

Дане перетворення називається канонічним і характеризується високою швидкодією через відсутність операцій множення. Операційна складність даного перетворення визначається кількістю операцій зсувів, цілочисельних додавань та операцій повернення в поле (*mod*). Для канонічного рівняння кількість нетривіальних зсувів: 31*31 = 961, кількість додавань: 32*31 = 992,

кількість повернень в поле залежить від розрядності використаних комірок пам’яті.

З означення поля **GF**(F_4) випливає наступна рівність [2]:

$$2^{16} = -1 \ mod \ (2^{16} + 1)$$

Після розбиття елементів на дві групи, зможемо виділити спільний множник:

$$F_k = \sum_{n=0}^{31} 2^{nk} x_n = \sum_{n=0}^{15} 2^{nk} x_n + 2^{(n+16)k} x_{n+16} \; mod \; (2^{16} + 1)$$

$$= \sum_{n=0}^{15} 2^{nk} x_n + (-1)^k 2^{nk} \, x_{n+16} = \sum_{n=0}^{15} 2^{nk} (x_n + (-1)^k x_{n+16}) \; mod \; (2_{16} + 1)$$

Розбиття вихідної послідовності на парні та непарні елементи робить піднесення до степеня значення (-1) тривіальним:

$$F_{2k} = \sum_{n=0}^{15} 2^{2nk} (x_n + (-1)^{2k} x_{n+16}) = \sum_{n=0}^{15} 2^{2nk} (x_n + x_{n+16}) \; mod \; (2^{16} + 1)$$

$$F_{2k+1} = \sum_{n=0}^{15} 2^{2nk} \, (x_n - x_{n+16}) 2^n \; mod \; (2^{16} + 1)$$

Операційна складність в такому випадку буде наступною: кількість нетривіальних зсувів: 31*15+15 = 480, кількість додавань, якщо вважати, що додавання в дужках виконуються лише один раз: 16 + 16 + 32*15 = 512.

Таким чином, при виконанні початкових перетворень над вхідними елементами та розбитті перетворення для парних та непарних елементів, операційна складність зменшується майже в 2 рази.

Якщо розбити вхідну послідовність на 4 групи, а вихідні елементи за кратністю 4, будуть отримані наступні перетворення:

$$F_k = \sum_{n=0}^{31} 2^{nk} x_n$$

$$= \sum_{n=0}^{7} 2^{nk} x_n + 2^{(n+8)k} x_{n+8} + 2^{(n+16)k} x_{n+16} + 2^{(n+16+8)k} x_{n+24}$$

$$F_{4k} = \sum_{n=0}^{7} 2^{4nk} (x_n + x_{n+8} + x_{n+16} + x_{n+24}) \; mod \; (2^{16} + 1)$$

$$F_{4k+1} = \sum_{n=0}^{7} 2^{4nk} (x_n + 2^8 x_{n+8} - x_{n+16} - 2^8 x_{n+24}) 2^n \; mod \; (2^{16} + 1)$$

$$F_{4k+2} = \sum_{n=0}^{7} 2^{4nk} (x_n - x_{n+8} + x_{n+16} - x_{n+24}) 2^{2n} \; mod \; (2^{16} + 1)$$

$$F_{4k+3} = \sum_{n=0}^{7} 2^{4nk}(x_n - 2^8 x_{n+8} - x_{n+16} + 2^8 x_{n+24})2^{3n} \ mod\ (2^{16}+1)$$

Операційна складність в такому випадку буде наступною: кількість нетривіальних зсувів: 7*8+31*7 = 273, кількість додавань: 12*8+ 32*7 = 320.

Таким чином, прискорений метод складається з двох етапів – обчислення проміжних (робочих) елементів та основних рівнянь перетворення.

На першому етапі, обчислюються значення:

$$t_n^0 = x_n + x_{n+8} + x_{n+16} + x_{n+24}\ mod\ (2^{16}+1)$$
$$t_n^1 = (x_n + 2^8 x_{n+8} - x_{n+16} - 2^8 x_{n+24})2^n\ mod\ (2^{16}+1)$$
$$t_n^2 = (x_n - x_{n+8} + x_{n+16} - x_{n+24})2^{2n}\ mod\ (2^{16}+1)$$
$$t_n^3 = (x_n - 2^8 x_{n+8} - x_{n+16} + 2^8 x_{n+24})2^{3n}\ mod\ (2^{16}+1),$$

де $n \in [0;7]$.

На другому етапі обчислюються результуючі значення перетворення:

$$F_{4k+q} = \sum_{n=0}^{7} 2^{4nk} t_n^q\ mod\ (2^{16}+1),$$

де $q \in [0;3]$.

Розбиття на групи більших розмірів (8, 16, 32) не дасть меншої операційної складності, так як при зменшенні елементів сумування основного перетворення, збільшується кількість кроків виконання попередніх обчислень.

Кількість повернень в поле може бути обчислена наступним чином. Початкові дані знаходяться в полі Галуа **GF**(2^{16}+1) і займають до 17 двійкових розрядів. Після першого етапу значення t_n^q будуть займати до 49 розрядів.

Таким чином, при використанні 32-розрядних регістрів, на першому етапі необхідно максимум 2 повернення в поле на елемент (для елементів t_n^0 повернення в поле може навіть не знадобитися).

На другому етапі найбільша ступінь двійки, на яку відбувається множення – 15. Таким чином, при використанні 32 розрядних регістрів, знадобиться максимум 3 повернення в поле на елемент.

При використанні 64-розрядних регістрів, знадобиться 2 повернення в поле в гіршому випадку (21 зсув на першому етапі та 15 на другому).

Висновки

При порівнянні запропонованого алгоритму із канонічним алгоритмом отримуємо підвищення швидкості виконання. Отриманий

метод має операційну складність в 3-4 рази меншу, ніж канонічне перетворення. Крім того, для даного методу визначено максимальну кількість повернень в поле, що забезпечить відсутність переповнень розрядної сітки.

Хоча розглянутий метод працює лише для 32 елементів, його прискорення є ключовим моментом для всіх швидких теоретико-числових перетворень більшої кількості елементів. Це пов'язано з тим, що вони засновані на використанні алгоритму Кулі-Тьюкі – дані представляються у вигляді матриці, для якої спочатку виконується перетворення стовпчиків, потім результат помножається на розраховані коефіцієнти, після чого виконуються перетворення рядків. Таким чином, швидке виконання перетворення для 1024 елементів виконується розкладанням на низку перетворень по 32 елементи.

Література

1. *Крендалл, Р.* Простые числа: Криптографические и вычислительные аспекты [Текст] / Р. Крендалл, К. Померанс ; пер. с англ. – М. : Книжный дом «ЛИБРОКОМ», 2011. – 664 с.

2. *Блейхут, Р.* Быстрые алгоритмы цифровой обработки сигналов [Текст] / Р. Блейхут ; пер. с англ. – М. : Мир, 1989. – 448 с.