Ефективний алгоритм синтезу незвідних поліномів

Ковальчук А.В., Новіков К.А., Полторацький Д.А.
Національний авіаційній університет, Київ
Науковий керівник – Білецький А.Я., д-р техн. наук, проф.

Криптографія знаходить широке застосування в різноманітних областях науки і техніки. Синтез незвідних поліномів до теперішнього часу є досить складним завданням. Криптографічні служби високорозвинених країн працюють над синтезом поліномів якомога більшого ступеня. Однак як правило свої результати вони не публікують у відкритій пресі. Відомі алгоритми синтезу незвідних поліномів мають суттєвий недолік - їх обчислювальна складність наближається до квадратичної. Тому допустима ступіть незвідного полінома обмежена потужністю обчислювальної техніки сьогодення.

Запропонований алгоритм спирається на так звані реперні сходинки(сітку), число яких, збігається зі ступенем синтезованих поліномів. На кожній сходинці здійснюються найпростіші рекурентні однотипні модулярні обчислення, по завершенні яких поліном, що тестується, однозначно класифікується або як незвідний, або як складовий.

Незвідні поліноми(НП) мають велику схожість з простими числами, які мають лише тривіальними дільниками. НП мають дві формам запису. Перша з них є так звана *поліноміальна форма*:

$$f(x) = \sum_{k=0}^{n} a_k x^k = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_k x^k + \cdots + a_1 x + a_0,$$

а в якості другої служить *векторна форма*, що є сукупністю коефіцієнтів a_k полінома, включаючи нульові коефіцієнти відсутніх мономів ряду:

$$f = a_n\, a_{n-1} \ldots a_k \ldots a_1\, a_0.$$

Поліноми характеризуються рядом основних параметрів. Одним з таких є *ступінь полінома (deg)* - це максимальний ступінь, який входить в поліном монома з ненульовим коефіцієнтом. *Порядок полінома (ord)* - це таке найменше натуральне число *m*, при якому даний поліном *f(x)* ділить без залишку двочлен $x^m - 1$. Як вже було сказано обчислювальна складність незвідного полінома є квадратичною. Кількість незвідних поліномів 32-ї ступені дорівнює 134 мільйони, а складність обчислень оцінюється ресурсами машини затраченими на його реалізацію. Зазначена проблема зумовлює в розробці нового ефективного алгоритму синтезу незвідних поліномів.

Твердження. Необхідною умовою незвідності двійкового полінома ступеня є виконання порівняння: $1\,(0)^{2^n-1} \equiv 1\ (\ mod\ f_n\ ),\ n \geq 2$. Представимо формулу $L_n \mid L_n^{\sim} = (2^n - 1)$ в такому виді: $(10)^{L_n^{\sim}} = 1\ (\ mod\ f_n)$. Ліва компонента $(10)^{L_n^{\sim}}$ порівняння являє собою координатний вектор: $CV_n = 100\ldots0\ \}\ 2^n - 1$ біт.

У свою чергу бінарний вектор, який відповідає порядку $L_n^{\sim}$ складається виключно з *n* одиниць. Назвемо цей вектор вектором одиниць (Unit Vector):

$UV_n = 11...11\ \}\ 2^n - 1$ біт

Десяткове значення вектора CV_n на одиницю більше значення вектора UV_n. Тому якщо дотримується умова, а саме $L_n \mid \tilde{L_n} = (2^n - 1)$, то тим самим підтверджується і порівняння.

Приклад. Вибравши в якості тестуємого поліному один з перевірених незвідних поліномів четверної ступені $f_4 = 10011$. Напишемо координатний вектор $CV_4 = 100...0\ \}$ 15 біт. Поділивши праву частину вектора на $f_4 = 10011$, отримаємо $ResCV_{4_{f_4}} = 1$, де позначено $Res(a)_b = a(mod\ b)$ - залишок числа a за модулем b. Отже, згідно з твердженням , $f_4 = 10011$ – незвідний поліном. До такого ж результату приходимо для варіанта $f_4 = 11111$, оскільки $ResCV_{4_{f_4}}$ дорівнює 1.

Звернемося до альтернативного варіанту, вибравши в якості тестованого полінома $f_4 = 10101$, який не являється незвідним. Для аналізованого полінома $ResCV_{4_{f_4}} = 1000 \neq 1$, з цього слідує, що поліном $f_4 = 10101$ являється звідним, тобто складовим.

Перевірим алгоритм на практиці вибравши для тестування незвідний поліном 12-го ступеня $f_{12} = 1000000001111$. Значення залишку S_r векторів CV_r по модулю f_{12} зведені в таблицю 1.

Таблиця 1

$S_1 = 10$;	$S_5 = 101010011110$;	$S_9 = 110111111100$;
$S_2 = 1000$;	$S_6 = 110101111101$;	$S_{10} = 110100000100$;
$S_3 = 10000000$;	$S_7 = 110101111110$;	$S_{11} = 11111100010$;
$S_4 = 1111000$;	$S_8 = 110101110100$;	$S_{12} = 1$

Той факт, що залишок f_{12} виявився рівним 1, є свідченням виконання необхідних умов незвідності полінома.

Розроблений алгоритм відноситься до підкласу алгоритмів лінійної складності. Суть рекурентних операцій на множені двійкових поліномів зводиться до обчислення залишків за модулем тестуємого на незвідність поліному, представленого в векторній формі, від квадрата залишку, утвореного на попередній сходинці перетворення і доповненого справа нулем.

Список використаних джерел:

1. Белецкий А.Я. Алгоритм синтезу незвідних поліномів лінійної складності. / А.Я. Белецкий, А.В. Ковальчук, К.А. Новіков, Д.А. Полторацький // «Захист інформації», Том 22, № 2 (2020). С 74-87.

2. Фомичёв, В. М. Дискретная математика и криптография. — М.: Диалог-МИФИ, (2013). — 397 с. — ISBN 978-5-86404-185-7.

3. Титов С.С. Генерация неприводимых многочленов, связанных степенной зависимостью корней. / С.С. Титов, А.В. Торгашов. // Управление, вычислительная техника и информатика. — Томск: Труды Томского Гос. ун-та, (2010). — № 2 (22). — С. 310-317.