ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ НЕЗВІДНОСТІ ТА ПРИМІТИВНОСТІ ПОЛІНОМІВ

Назарук Р.Р.
Науковий керівник – к.т.н., доцент, Мельникова О.А.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. Безпеки інформаційних технологій, тел. (057) 702-14-25)
e-mail: 97roman@gmail.com, факс (050) 346-05-96

Irreducible and primitive polynomials in $Z_2[x]$ are widely used in modern cryptography. For example many stream and block ciphers use such polynomials with big degrees of the form 2^k. Reduction with modulus of this type can be performed faster if smaller non-zero coefficients are placed in one computer word, mostly the lowest one. Algorithms for generating polynomials with such properties are considered in this paper. As a result, it was found 596 primitive pentanoms of power 128, 271 primitive pentanoms of power 256, and 145 primitive pentanoms of power 512 whose smaller non-zero coefficients are less than 64.

В ряді криптографічних алгоритмів і стандартів, у тому числі потокових та блокових шифрах (наприклад, ДСТУ 7624:2014 [1]), використовуються незвідні та примітивні поліноми.

У даному досліджені був проведений пошук примітивних та незвідних поліномів у кільці $Z_2[x]$. Для цього використовувався адаптований алгоритм перевірки властивостей поліному з [2]:

1. $g(x) = x$;
2. *for* ($i = 0; i < l/2; ++i$)
   2.1 $g(x) = g(x)^2 \bmod f(x)$;
   2.2 $d(x) = GCD(f(x), g(x)+x)$;
   2.3 *if* ($d(x) \neq 1$)
      ret "поліном не незвідний (і не примітивний)";
3. $T = 2^l - 1 = q_1 \times q_2 \times \ldots \times q_k$;
4. *for* ($i = 1; i \leq k; ++i$)
   4.1 $d(x) = x^{T/qi} \bmod f(x)$;
   4.3 *if* ($d(x) == 1$)
      ret "поліном не примітивний (але незвідний)";

ret "поліном примітивний (та незвідний)";

В цьому алгоритмі: l — степінь поліному $f(x)$, який тестується, *GCD* — найбільший спільний дільник, q_i — прості множники числа T.

На 3 кроці алгоритму використовується факторизація великого числа T. Факторизація є складною розрахунковою задачею, однак у криптографічних алгоритмах потокових та блочних шифрів [1] використовуються поліноми, степені яких являються степенями числа 2

(наприклад, 128, 256, 512). Такі числа можна розкласти на множники за різницею квадратів ($a^2 – b^2 = (a + b) \times (a - b)$).

Наприклад, для поліному степеню $l = 128$ маємо:

$$T = 2^{128} – 1 = (2^{64})^2 – 1^2 = (2^{64} + 1) \times (2^{64} – 1) = F_6 \times (2^{64} – 1);$$

де F_6 — 6-те число Ферма (F_6 = 0x42f01 × 0x3d30f19cd101), а $(2^{64} – 1)$ далі розкладується за різницею квадратів:

$(2^{64} – 1) = (2^{32})^2 – 1^2 = (2^{32} + 1) \times (2^{32} – 1) = F_5 \times (2^{32} – 1);$

F_5 = 0x281 × 0x663d81;

$(2^{32} – 1) = (2^{16})^2 – 1^2 = (2^{16} + 1) \times (2^{16} – 1) = F_4 \times (2^{16} – 1);$

F_4 = 0x10001;

$(2^{16} – 1) = (2^{8})^2 – 1^2 = (2^{8} + 1) \times (2^{8} – 1) = F_3 \times (2^{8} – 1);$

F_3 = 0x101;

$(2^{8} – 1) = (2^{4})^2 – 1^2 = (2^{4} + 1) \times (2^{4} – 1) = F_2 \times (2^{4} – 1);$

F_2 = 0x11;

$(2^4 – 1) = 15$ = 0x5 × 0x3;

Дані про числа Ферма та результати їх факторизації/доказу простоти чисел взяті з [3].

В результаті маємо 9 співмножників у факторизації значення $T = 2^{128} – 1$ = 0x42f01 × 0x3d30f19cd101 × 0x281 × 0x663d81 × 0x10001 × 0x101 × 0x11 × 0x5 × 0x3.

Операції приведення за модулем $f(x)$ виконуються значно швидше, коли його менші ненульові коефіцієнти розташовані у молодшому слові, тобто на бітових позиціях менших 32 або 64, в залежності від розрядності обчислювальної техніки. Алгоритми одночасної редукції особливо ефективні, якщо степінь поліному $f(x)$ вирівняна по границі слова, тобто є степеню числа 2. У роботі сформовані варіанти пентаномів та триномів з бітовими позиціями ненульових коефіцієнтів менших 64.

За результатами дослідження було виявлено 596 примітивних пентаномів степеню 128, 271 примітивних пентаномів степеню 256, та 145 примітивних пентаномів степеню 512.

Список джерел:

1. ДСТУ 7624: 2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. — Перше видання; Введ. 01.07.2015. — К.: Мінекономрозвитку України, 2015 р. — 238 с.

2. ДСТУ 4145 – 2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. — Перше видання; Введ. 1.07.2003. — К.: Державний комітет України з питань технічного регулювання та споживчої політики, 2003 р. — 36 с.

3. Fermat factoring status [Електронний ресурс]: Режим доступу: http://www.prothsearch.com/fermat.html (24.01.2019).