4 Период последовательности

Задача. В качестве гаммы поточного шифра Алиса использует ненулевую двоичную последовательность (s_t), заданную следующим рекуррентным соотношением:

$$s_{t+128} = (s_{t+1} + 1)(s_{t+2} + 1) \dots (s_{t+127} + 1) + s_t + s_{t+1} + s_{t+2} + s_{t+7}$$

(сложение выполняется по модулю 2). Найдите период этой последовательности.

Решение. Пусть (s_t^*) — линейная рекуррентная последовательность над полем из двух элементов, заданная соотношением

$$s_t^* = s_t^* + s_{t+1}^* + s_{t+2}^* + s_{t+7}^*.$$

Характеристический многочлен этой последовательности имеет вид $f(x) = x^{128} + x^7 + x^2 + x + 1$. [1] С помощью систем компьютерной алгебры можно убедиться, что этот многочлен является неприводимым. Для этого достаточно проверить, что многочлены $x^{2^{64}} - x$ и $f(x)$ взаимно просты и что $f(x)$ делит $x^{2^{128}} - x$. [2]

Для всех простых p, которые делят

$$2^{128} - 1 = 3 \cdot 5 \cdot 17 \cdot 257 \cdot 641 \cdot 65537 \cdot 274177 \cdot 6700417 \cdot 67280421310721,$$

выполняется

$$x^{(2^{128}-1)/p} \not\equiv 1 \pmod{f(x)}$$

и, следовательно, порядок $f(x)$ равняется $2^{128} - 1$, т. е. $f(x)$ является примитивным. [3]

Примитивность $f(x)$ означает, что при ненулевых начальных значениях минимальный период последовательности (s_t^*) равняется $2^{128} - 1$. При согласовании начальных условий последовательность (s_t) получается из (s_t^*) вставкой нуля после фрагмента $100 \dots 0$ длины 128. Это значит, что минимальный период последовательности (s_t) равняется 2^{128}.

Отметим, что (s_t) — это известная в комбинаторике последовательность де Брейна. Первые 2^{128} ее фрагментов $s_1 s_2 \dots s_{128}$, $s_2 s_3 \dots s_{129}$,... различны. □

[1] Данный многочлен $f(x)$ использован в СТБ 34.101.31 для организации умножения в поле из 2^{128} элементов.

[2] См. [Rabin M. O. Probabilistic algorithms in finite fields. SIAM J. Comp. 9 (1980), 273–280]. Ср. с алгоритмом `IsIrred` из СТБ П 34.101.44-2011.

[3] См. [Лиддл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988].