Секция 2

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.7

МНОГОЧЛЕНЫ НАД ПРИМАРНЫМИ КОЛЬЦАМИ ВЫЧЕТОВ С МАЛЫМ РАССТОЯНИЕМ ЕДИНСТВЕННОСТИ

А. В. Аборнев, Д. Н. Былков

Пусть $F(x)$ — унитарный многочлен степени m над кольцом $R = \mathbb{Z}_{2^n}$. Через $L_R(F)$ будем обозначать множество всех линейных рекуррентных последовательностей над R с характеристическим многочленом $F(x)$ [1]. Каждой последовательности u из $L_R(F)$ сопоставим последовательности $u_0, \ldots, u_{n-1}$, получающиеся из двоичного разложения

$$u(i) = u_0(i) + 2u_1(i) + \ldots + 2^{n-1}u_{n-1}, u_s(i) \in \{0,1\}, s = 0, \ldots, n-1;\ i \geqslant 0. \qquad (1)$$

При правильном выборе многочлена $F(x)$ последовательности u_s обладают рядом важных для криптографии свойств: большим периодом, высоким рангом, хорошими частотными характеристиками. Одним из наименее изученных параметров является *расстояние единственности*.

Определение 1. Назовем расстоянием единственности многочлена $F(x)$ и обозначим через $\mathrm{Ud}(F)$ минимум натуральных чисел l, таких, что для любых двух рекуррент $u, v \in L_R(F), u \neq v$, верно соотношение

$$u_{n-1}[\overline{0, l-1}] \neq v_{n-1}[\overline{0, l-1}];$$

если же таких натуральных l не существует, то будем писать $\mathrm{Ud}(F) = \infty$.

А. А. Нечаевым выдвинута

Гипотеза 1. Параметр $\mathrm{Ud}(F)$ зависит линейно от величины mn.

В настоящее время эта гипотеза не доказана, но и не опровергнута. Первым шагом в продвижении этой гипотезы стал результат А. А. Варфоломеева о расстоянии единственности многочлена $x^2 - x - 1 \in \mathbb{Z}_{2^n}[x]$ (устные сообщения). В дальнейшем второму из авторов удалось частично подтвердить гипотезу 1 в случае, когда многочлен $F(x) \in \mathbb{Z}_4$ является трехчленом [2]. В частности, справедлива

Теорема 1. Пусть $F(x) = x^m - x - 1$, тогда $\mathrm{Ud}(F) = 3m$.

Далее $n = 2, R = \mathbb{Z}_4$. Конечность параметра $\mathrm{Ud}(F)$ означает, что начальный вектор $u[\overline{0, m-1}]$ последовательности $u \in L_R(F)$ однозначно определяется по отрезку $u_1[\overline{0, \mathrm{Ud}(F)-1}]$. Обширные вычислительные эксперименты на ЭВМ показали существование многочленов $F(x) \in R[x]$ со свойством $\mathrm{Ud}(F) = 2m$.

Для таких многочленов А. А. Нечаевым предложен способ построения подстановки ψ_F, действующей на множестве $T = \mathbb{Z}_2^m$. В этом случае отрезок $u[\overline{0, m-1}]$ однозначно задается отрезком $u_1[\overline{0, 2m-1}]$. Для каждого $t \in T$ зададим последовательность $u \in L_R(F)$ по правилу $u_0[\overline{0, m-1}] = t,\ u_1[\overline{0, m-1}] = \overline{0}$. В соответствии со сказанным выше отрезок $u_1[\overline{0, 2m-1}]$ однозначно определяет начальный вектор

$u[\overline{0,m-1}]$, а значит, и элемент t. Так как $u_1[\overline{0,m-1}] = \overline{0}$, то $t = u_0[\overline{0,m-1}]$ однозначно определяется отрезком $u_1[\overline{m,2m-1}]$. Зададим подстановку ψ_F равенством $\psi_F(t) = u_1[\overline{m,2m-1}]$.

Достоинством таких подстановок является возможность их эффективной реализации на современных микропроцессорах. Отметим, что некоторые координатные функции ψ_F имеют степень нелинейнсти 2. Рассмотрим узел блочного шифра с r раундами и набором раундовых ключей $k = (k_1, \ldots, k_r) \in T^r$, построенный на основе подстановки ψ_F. Исходное сообщение $x \in T$ преобразуется согласно равенству

$$y = S_k(x) = \psi_F(\ldots \psi_F(\psi_F(x + k_1) + k_2) \ldots + k_r).$$

Зададим группу подстановок $G = \{g_t : g_t(x) = x \oplus t,\ x, t \in T\}$. Тогда $S_k \in (\psi_F G)^r$. В ходе экспериментов установлено, что в ряде случаев множество подстановок $\psi_F G$ порождает знакопеременную группу подстановок. Построены примеры, когда уже при $k = m$ данный узел является стойким к методу дифференциального анализа.

Тривиальными примерами многочленов с расстоянием единственности $2m$ являются многочлены $F(x)$, такие, что $F(x) \equiv x^m + 1 \pmod 2$. Однако пока не обосновано существование нетривиальных многочленов со свойством $\mathrm{Ud}(F) = 2m$ произвольной степени m. Важным шагом в этом направлении является

Теорема 2. Пусть $m = 2^k + s$, $k \in \mathbb{N}$, s нечетно, $F(x) = F_0(x) + 2F_1(x)$ — двоичное разложение многочлена $F(x)$, $F_0(x) \equiv (x+1)^m \pmod 2$ и $(F_1(x) + x^s, x + 1) = 1$. Тогда $\mathrm{Ud}(F) \in \{2m, \infty\}$.

Пусть $R = \mathbb{Z}_{p^2}$, $p > 2$ — простое число, $\Gamma(R) = \{a \in R : a^p = a\}$ — p-адическое координатное множество. Известно [1], что каждый элемент $a \in R$ однозначно представляется в виде $a = a_0 + pa_1, a_0, a_1 \in \Gamma(R)$. Аналогично (1) каждую линейную рекуррентную последовательность $u \in L_R(F)$ можно представить в виде

$$u(i) = u_0(i) + pu_1(i), \quad u_0(i), u_1(i) \in \Gamma(R), \quad i \geqslant 0.$$

Параметр $\mathrm{Ud}(F)$ определяется так же, как и в двоичном случае. Серия экспериментов на ЭВМ показала, что результат теоремы 1 справедлив для $p = 3$, $m \in \overline{2,9}$; $p = 5$, $m \in \overline{2,5}$. Экспериментально показано существование многочленов с расстоянием единственности $2m$. Такие многочлены также позволяют задавать подстановки на множестве $\mathbb{Z}_p^m$. Степень нелинейности координатных функций соответствующих подстановок равна p.

ЛИТЕРАТУРА

1. *Kurakin V. L., Kuzmin A. S., Mikhalev A. V., and Nechaev A. A.* Linear Recurring Sequences over Rings and Modules // J. Math. Sci. 1995. V. 76. No. 6. P. 2793–2915.
2. *Былков Д. Н.* Расстояние единственности семейства координатных последовательностей, полученных усложнением линейных рекуррент над кольцом Галуа //Прикладная дискретная математика. 2008. № 2. С. 5–7.