Построение этого семейства полностью продиктовано результатами работы [3], в которой получено описание ряда классов эквивалентности секретных ключей криптосистемы Мак-Элиса–Сидельникова.

Рассмотрим теперь задачу, связанную со стойкостью криптосистемы Мак-Элиса–Сидельникова. Однако здесь криптосистема Мак-Элиса–Сидельникова рассматривается не на всём ключевом пространстве, а только на полностью описанных в [3] классах эквивалентности.

Задача mcSRM

Вход: матрица $G = (H_1 \cdot R \| H_2 \cdot R) \cdot \Delta$, где H_1 и H_2 — невырожденные двоичные $(k \times k)$-матрицы, принадлежащие классу эквивалентности $[(H, HT^i_{\widetilde{\alpha}}, \Gamma)]$ для некоторой невырожденной $(k \times k)$-матрицы H, некоторой перестановочной $(2n \times 2n)$-матрицы Γ, некоторого числа $1 \leqslant i \leqslant k$ и некоторого вектора $\widetilde{\alpha}$; R — порождающая $(k \times n)$-матрица кода Рида–Маллера $RM(r, m)$; Δ — перестановочная $(2n \times 2n)$-матрица.

Найти: невырожденные матрицы H'_1 и H'_2 размера $(k \times k)$ и перестановочную $(2n \times 2n)$-матрицу Δ', такие, что $G \cdot \Delta' = (H'_1 R \| H'_2 R)$.

Справедливы следующие теоремы.

Теорема 1. Пусть существует набор машин Тьюринга $MTmcRMi$, каждая из которых решает соответствующую задачу mcRMi за полиномиальное время. Тогда существует машина Тьюринга $MTmcSRM$, которая решает задачу mcSRM за полиномиальное время.

Теорема 2. Пусть существует машина Тьюринга $MTmcRM$, которая решает задачу mcRM за полиномиальное время. Тогда существует семейство машин Тьюринга $MTmcRMi$, которые соответственно решают задачи mcRMi за полиномиальное время.

Теорема 3. Пусть существует машина Тьюринга $MTmcRM$, которая решает задачу mcRM за полиномиальное время. Тогда существует машина Тьюринга $MTmcSRM$, которая решает задачу mcSRM за полиномиальное время.

ЛИТЕРАТУРА

1. *McEliece R. J.* A public-key cryptosystem based on algebraic coding theory // DSN Prog. Rep., Jet Prop. Lab., California Inst. Technol. 1978. P. 114–116.
2. *Сидельников В. М.* Открытое шифрование на основе двоичных кодов Рида-Маллера // Дискретная математика. 1994. № 6(2). С. 3–20.
3. *Чижов И. В.* Ключевое пространство криптосистемы Мак-Элиса-Сидельникова // Дискретная математика. 2009. № 21(3). С. 132–158.

УДК 681.3

МОДЕЛЬ СИММЕТРИЧНОГО ШИФРА НА ОСНОВЕ НЕКОММУТАТИВНОЙ АЛГЕБРЫ ПОЛИНОМОВ

И. В. Широков

Пусть $\mathbb{F}$ — некоторое поле, $f(x), g(x)$ — элементы кольца $\mathbb{F}[x]$, $(f \circ g)(x) \equiv f(g(x))$ — композиция полиномов. Кольцо $\mathbb{F}[x]$ с дополнительной операцией композиции является некоммутативной алгеброй полиномов с тремя бинарными операциями $\{+, \cdot, \circ\}$.

Решение уравнения

$$(f \circ g)(x) = r(x) \bmod h(x), \quad f, g, h, r \in \mathbb{F}[x], \tag{1}$$

относительно неизвестного многочлена f или g сводится к поиску корней, принадлежащих основному полю $\mathbb{F}$, некоторых многочленов из кольца $\mathbb{F}[x]$, что не является трудной задачей.

Уравнение (1) естественным образом возникает в задаче определения группы алгебраических симметрий многочлена, которая в общем случае является подгруппой группы Галуа этого многочлена.

Свойства операции композиции многочленов позволяют предложить следующую модель криптосистемы. Открытыми параметрами криптосистемы являются множество различных многочленов $\{f_1(x), \ldots, f_n(x)\}$, $f_i(x) \in \mathbb{F}[x]$, степени $k \geqslant 2$ и некоторый неприводимый над $\mathbb{F}$ многочлен $h(x)$; секретным ключом является некоторая перестановка $\sigma \in S_n$. Открытый текст представляется многочленом $m(x) \in \mathbb{F}[x]$, шифртекстом будет следующий многочлен $c(x)$:

$$(f_{\sigma_n} \circ \cdots \circ f_{\sigma_1} \circ m)(x) = c(x) \bmod h(x). \tag{2}$$

Процесс шифрования заключается в вычислении по рекуррентной формуле:

$$c_0(x) = m(x); \quad c_i(x) = (f_{\sigma_i} \circ c_{i-1})(x) \bmod h(x),\ i = 1, \ldots, n; \quad c(x) = c_n(x).$$

Расшифрование заключается в последовательном решении систем вида (1) относительно неизвестных многочленов $c_{n-1}, \ldots, c_1, c_0 = m(x)$:

$$(f_{\sigma_i} \circ c_{i-1})(x) = c_i(x) \bmod h(x),\ i = n, \ldots, 1.$$

По мнению автора, при наличии пары «открытый текст – шифртекст» наиболее быстрый способ определить ключ — это полный перебор всего ключевого пространства мощности $n!$, т. е. выбор перестановки, шифрование и сравнение результата с шифртекстом.

Основой для такого вывода является следующее. Введем обозначение $f_\sigma = f_{\sigma_n} \circ \cdots \circ f_{\sigma_1}$; тогда уравнение (2) записывается в виде $f_\sigma \circ m = c \bmod h$. Заметим, что приводить по модулю $h(x)$ можно многочлен $m(x)$ и конечный результат композиции, а многочлен f_σ нельзя, так как если мы производим вычисления в фактор-кольце $\mathbb{F}[x]/(h(x))$, то композиция, в отличие от операции умножения, не является корректно определенной в фактор-кольце операцией. Для того чтобы найти коэффициенты многочлена f_σ, необходимо найти корни из поля F многочлена степени порядка $\exp(\exp n)$, что даже для небольших значений числа n невозможно. Попытаться как-то разделить исходную задачу на части также не представляется возможным.

По мнению автора, некоммутативная алгебра полиномов слабо изучена, но имеет при этом важные приложения. Это позволяет надеяться, что изучение этой алгебры и предлагаемой криптосистемы представляет некоторый научный интерес.