ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 19 МАТЕМАТИКИ Выпуск 3
2012

В. М. Деундяк, Е. С. Чекунов (Ростов-на-Дону, ФГНУ НИИ «Спецвузавтоматика», ЮФУ). **О разработке алгоритмов для реализации списочного декодера Бернштейна.**

Стойкость кодовых криптосистем основана на сложности задачи декодирования случайного линейного кода [1]. В первой кодовой криптосистеме Мак-Элиса использовался бинарный код Гоппы $\mathcal{G}(L,g)$, где $g \in \mathbf{F}_{2^m}[x], L \subseteq \mathbf{F}_{2^m}$. В [3] представлены атаки на шифрограмму такой криптосистемы; чтобы противостоять атакам предлагается либо выбирать большие параметры кода, либо модифицировать криптографический протокол, используя списочный декодер Бернштейна [2]. Этот декодер кодов Гоппы позволяет при тех же параметрах кода исправлять большее количество ошибок, чем классический алгоритм Паттерсона. Это обстоятельство увеличивает стойкость модифицированной таким образом криптосистемы.

Важным этапом проектирования модифицированной криптосистемы является разработка алгоритмов для программной реализации списочного декодера Бернштейна, чему посвящена настоящая работа.

Рассмотрим поле рациональных функции $\mathbf{F}_{2^m}(x)$ с нормой

$$\forall a \in \mathbf{F}_{2^m}(x) : \|a\| = \begin{cases} 2^{\deg a}, & \text{если } a \neq 0; \\ 0, & \text{если } a = 0. \end{cases}$$

Пусть $\mathbf{F}_{2^m}[x](\subset \mathbf{F}_{2^m}(x))$ — кольцо полиномов над полем $\mathbf{F}_{2^m}, \Lambda_{n,\nu_n} \subset (\mathbf{F}_{2^m}[x])^n$ — n-мерная $\mathbf{F}_{2^m}[x]$-решетка с нормой ν_n, заданной следующим образом:

$$\forall \mathbf{a} = (a_1, a_2, \ldots, a_n) \in \Lambda_{n,\nu_n} : \nu_n(\mathbf{a}) = \max_i\{\|a_i\|\}. \tag{1}$$

В [4] получен алгоритм редуцирования базиса n-мерной $\mathbf{F}_q[x]$-решетки для степенной нормы в поле. В работе построен алгоритм 1, являющийся модификацией алгоритма из [4] для случая произвольной решетки Λ_{n,ν_n}. Кроме того, построен алгоритм 2 редуцирования базиса двумерной $\mathbf{F}_{2^m}[x]$-решетки $\Lambda_{2,\mu}$ с нормой

$$\forall \mathbf{a} = (a_1,\ a_2) \in \Lambda_{2,\mu} : \mu(\mathbf{a}) = \mu(a_1,\ a_2) = ||a_1^2 + xa_2^2||, \tag{2}$$

который работает значительно быстрее, чем алгоритм 1 для $\Lambda_{2,\mu}$. Алгоритм 3 получает на вход пришедшее по каналу слово z, многочлен Гоппы g и синдромный многочлен s. Обращаясь к алгоритму 2, этот алгоритм вычисляет натуральный параметр $\theta = \theta(z,g,s)$ и многочлен $\delta = \delta(s,g,h) \in \mathbf{F}_{2^m}[x]$. Алгоритм 4 получает на вход многочлены $h = x^{|L|} - x, \delta$, число θ и управляющие параметры $l, k \in \mathbf{N}$. Обращаясь к алгоритму 1, этот алгоритм вычисляет минимальный вектор φ некоторой специальной решетки $\tilde{\Lambda}_n$. Заключительный алгоритм 5 получает на вход полиномиальное представление минимального вектора φ и на основе его факторизации над полем $\mathbf{F}_{2^m}(x)$ формирует искомый список кодовых слов.

СПИСОК ЛИТЕРАТУРЫ

1. *Сидельников В. М.* Теория кодирования. М.: Физматлит, 2008.
2. *Bernstein D. J.* List decoding for binary Goppa codes. 2008. URL:http://cr.yp.to/papers.html#goppalist (дата обращения: 15.04.2012).
3. *Bernstein D. J.*, *Lange T.*, *Peters C.* Attacking and defending the McEliece cryptosystem. — Lecture Notes Comput. Sci., 2008, v. 5299, p. 31–46.
4. *Lenstra A. K.* Factoring multivariate polynomials over finite fields. — J. Comput. System Sci., 1985, v. 30, № 2, p. 235–248.